



Phishing & Education

Applying security principles during the pandemic

Isaiah James D. Puzon

Tuesday, October 12, 2021

“The fear of the Lord is the beginning of wisdom and the knowledge of the Holy One is understanding.”

– Proverbs 9:10





[screams internally]

(isaiah.puzon@cogia.edu.ph)-[~]
whoami

Employment

- Senior Offensive Security Engineer @ **Deltak Systems (Philippines), Ltd.** (Current)
- Global Security Professional @ **CMA-CGM** (Same as CEVA, now **resigned**)
- Senior Information Security Analyst @ **CEVA Logistics** (Same as CMA-CGM, now **resigned**)

Affiliations

- Red Team Member @ **Synack Red Team**
- CTF Team Member @ **[hsb] hackstreetboys & [TMHC] TheManyHatsClub**
- Sleepy Admin @ **[PITSF] Philippine IT Security Forums**
- Volunteer @ **Covenant of Grace Integrated Academy, Inc.**

Educational Background

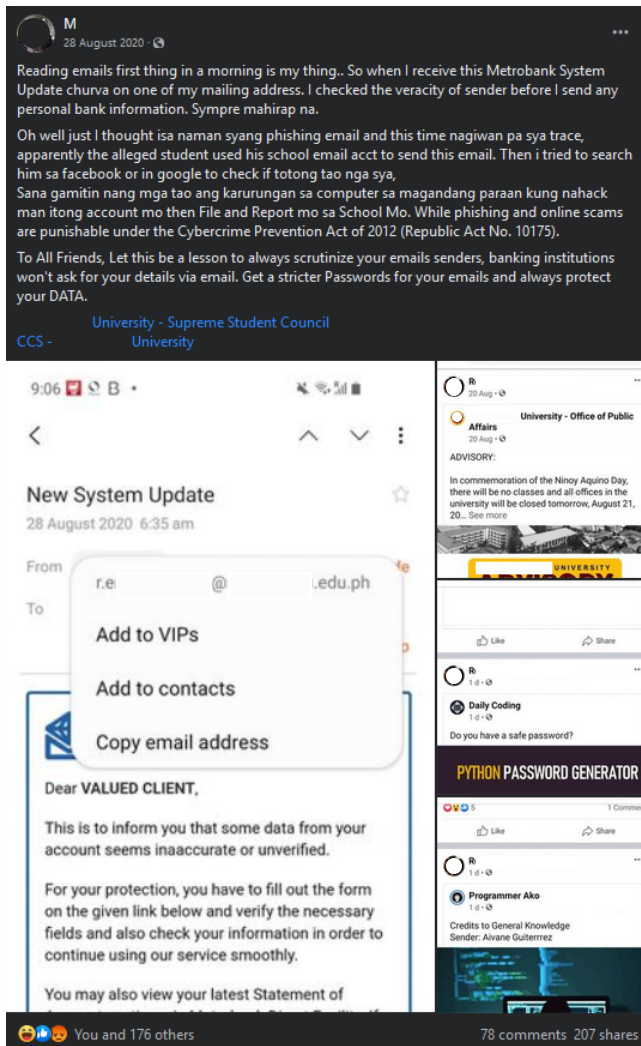
- BS Computer Engineering Alumni @ **FEU Institute of Technology**
- OSWE, OSCP, CCNA Cyber Ops, Security+, Linux+, CCNA R&S



Me as Derp



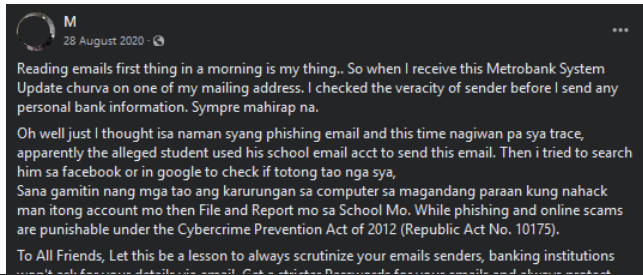
Current Situation



- Ordinary people are victims of Phishing
- Criminals steal the hard-earned money of working individuals within minutes
- This situation encompasses all industries: Healthcare, Education, Manufacturing, BPO, Banking, Finance, Logistics, Shipping, Military, Government, IT, etc.



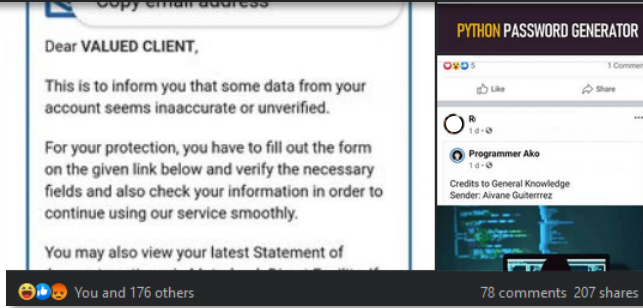
Current Situation



Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagiwan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if tolong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

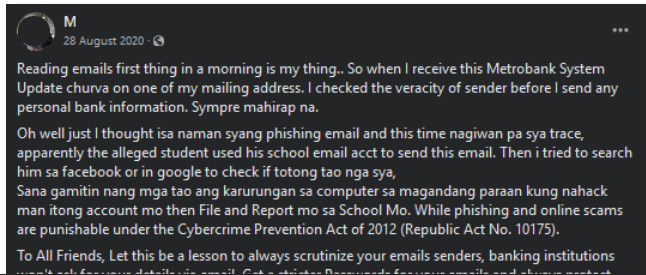
To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.



- Ordinary people are victims of Phishing
- Criminals steal the hard-earned money of working individuals within minutes
- This situation encompasses all industries: Healthcare, Education, Manufacturing, BPO, Banking, Finance, Logistics, Shipping, Military, Government, IT, etc.



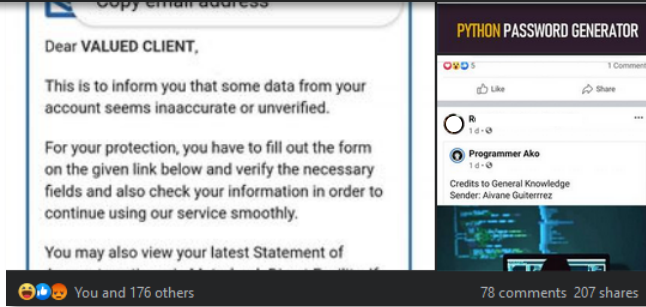
Current Situation



Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagiwan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if tolong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.

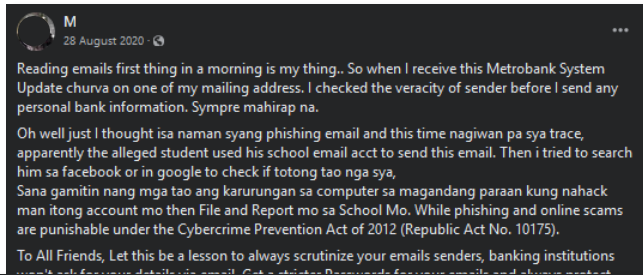


- Ordinary people are victims of Phishing
- Criminals steal the hard-earned money of working individuals within minutes
- This situation encompasses all industries: Healthcare, Education, Manufacturing, BPO, Banking, Finance, Logistics, Shipping, Military, Government, IT, etc.

The ORDINARY PERSON is under ATTACK



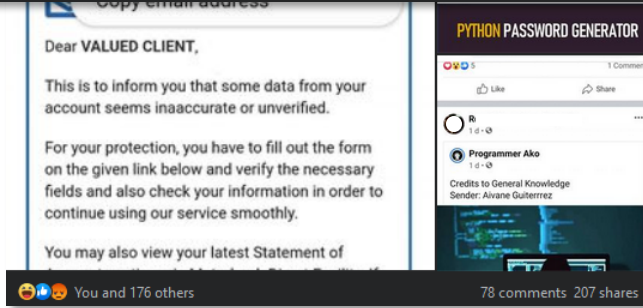
Current Situation



Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagiwan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if tolong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.



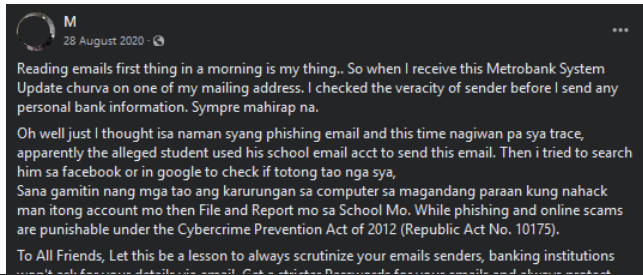
- Ordinary people are victims of Phishing
- Criminals steal the hard-earned money of working individuals within minutes
- This situation encompasses all industries: Healthcare, Education, Manufacturing, BPO, Banking, Finance, Logistics, Shipping, Military, Government, IT, etc.

The ORDINARY PERSON is under ATTACK

What can WE do?



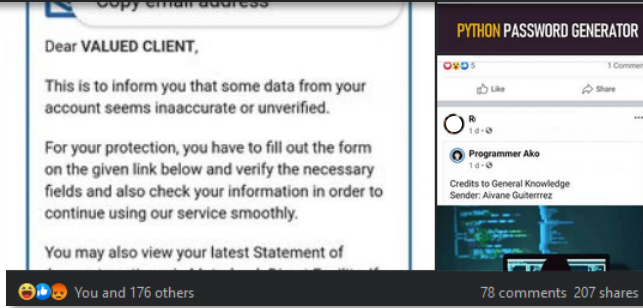
Current Situation



Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagiwan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if tolong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.



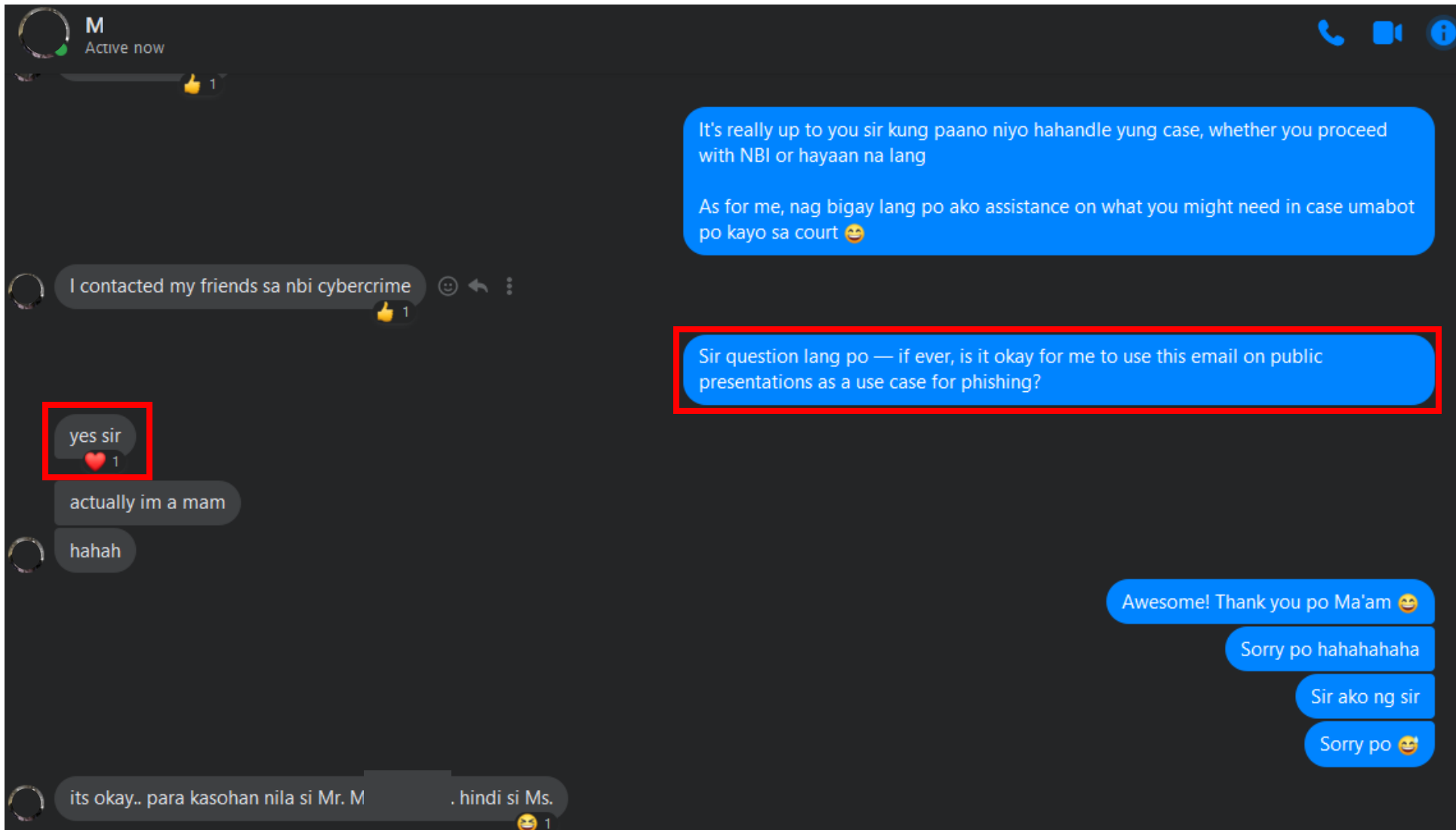
- Ordinary people are victims of Phishing
- Criminals steal the hard-earned money of working individuals within minutes
- This situation encompasses all industries: Healthcare, Education, Manufacturing, BPO, Banking, Finance, Logistics, Shipping, Military, Government, IT, etc.

The ORDINARY PERSON is under ATTACK

What can WE do?
How can we PROTECT them?



Complexity of Phishing



Disclaimer:

1. Express written approval has been given by the recipient of phishing to show the following slides
2. This is just gathering of facts of what happened during that specific day



Complexity of Phishing – The malicious email

The screenshot shows a Windows File Explorer window open to the directory `C:\Users\Administrator\Downloads\phishing`. The file list contains three items: `cmd.txt` (1 KB), `hash.txt` (2 KB), and `New System Update.eml` (28 KB). Two Notepad windows are open, displaying the results of a PowerShell command used to generate a SHA256 hash of the email file.

cmd.txt - Notepad

```
File Edit Format View Help
PS C:\Users\Administrator\Downloads\phishing> Get-FileHash -Algorithm SHA256 '.\New System Update.eml' | Out-String -Width 300 | Out-File hash.txt
PS C:\Users\Administrator\Downloads\phishing> cat .\hash.txt
```

Algorithm	Hash	Path
SHA256	79A10FD5855EFE6966CD22A5880BA81E9881BD1C244423B13EFC444DCDEB4ABA	C:\Users\Administrator\Downloads\phishing\New System Update.eml

hash.txt - Notepad

```
File Edit Format View Help
```

Algorithm	Hash	Path
SHA256	79A10FD5855EFE6966CD22A5880BA81E9881BD1C244423B13EFC444DCDEB4ABA	C:\Users\Administrator\Downloads\phishing\New System Update.eml



Complexity of Phishing – The malicious email

Fri 8/28/2020 06:35
MetroBank <r.e[REDACTED]@[REDACTED].edu.ph>
New System Update
To m[REDACTED]@yahoo.com



Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customerservice@metrobankcard.com

or call our 24-hour Customer Service hotline at 8700-700.

[VERIFY MY ACCOUNT](#)

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [REDACTED] University and its officials.



Complexity of Phishing – Email Body Analysis

The screenshot shows an email from MetroBank with the following details:

- Header:** From: MetroBank <[redacted]@[redacted].edu.ph> (highlighted with a red box and arrow pointing to a callout: "Mail appears to have been sent by a university student"). To: m[redacted]@yahoo.com. Date: Fri 8/28/2020 06:35 (highlighted with a red box and arrow pointing to a callout: "Mail was received on Friday, August 28, 2020 at 6:35 AM UTC+8").
- Body:** Metrobank logo, "Dear VALUED CLIENT," and a message about account data inaccuracies. It includes a "VERIFY MY ACCOUNT" button.
- Footer:** A disclaimer and a statement of views, both highlighted with a red box and arrow pointing to a callout: "Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [redacted] University and its officials."



Complexity of Phishing – Email Body Analysis

Fri 8/28/2020 06:35
MetroBank <r.e[REDACTED]@[REDACTED].edu.ph>
New System Update
To m[REDACTED]@yahoo.com



Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customerservice@metrobankcard.com

or call our 24-hour Customer Service hotline at 8700-700.

[VERIFY MY ACCOUNT](#)

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [REDACTED] University and its officials.

With a clear intent to **deceive** by impersonating Metrobank



Complexity of Phishing – Email Body Analysis

Fri 8/28/2020 06:35
MetroBank <r.e[redacted]@[redacted].edu.ph>
New System Update
To m[redacted]@yahoo.com



Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customer.service@metrobank.com

or call our 24-hour Customer Service hotline at 8700-700.

[https://donewellinsurance.com/
administrator/js/update/metrobank](https://donewellinsurance.com/administrator/js/update/metrobank)
Click or tap to follow link.

VERIFY MY ACCOUNT

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [redacted] University and its officials.

And concealing a malicious link
(Phishing Page)



Complexity of Phishing – Summary of Findings (Email Body Analysis)

Facts

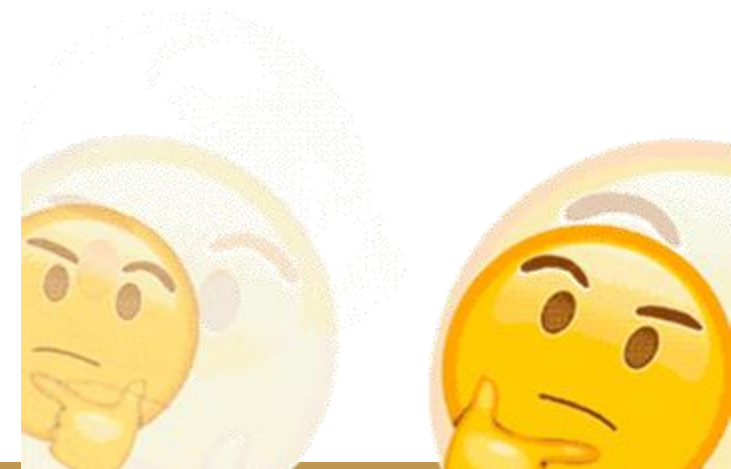
1. The mail was delivered on Friday, August 28, 2020 at 6:35 AM UTC+8
2. The received mail is malicious in nature
 - It intends to deceive recipients that the email came from Metrobank
 - It entices the recipients to click on “**VERIFY MY ACCOUNT**” which contains a concealed malicious link

Presumptions

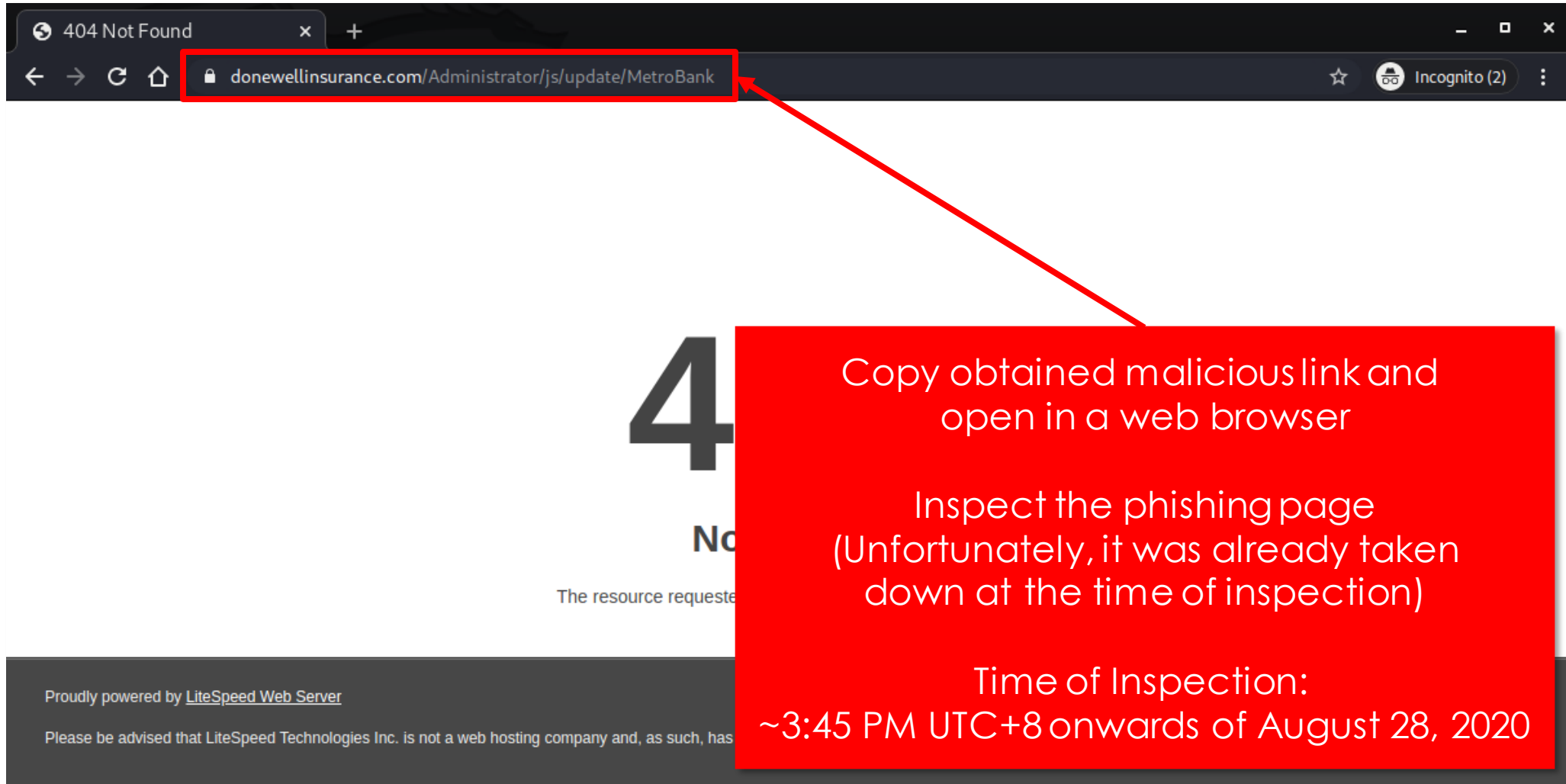
1. The mail was allegedly sent by a student of ***** University
 - The mail is sent from r.e*****@*****.***.edu.ph
 - The Disclaimer is automatically generated to notify recipients that its contents do not reflect the views of ***** University and its officials

Timeline of Events

1. 08-28-2020 at 6:35 AM UTC +8 (Malicious mail delivered)



Complexity of Phishing – Phishing Link Analysis



404 Not Found

donewellinsurance.com/Administrator/js/update/MetroBank

Incognito (2)

4
No
The resource request

Proudly powered by [LiteSpeed Web Server](#)

Please be advised that LiteSpeed Technologies Inc. is not a web hosting company and, as such, has

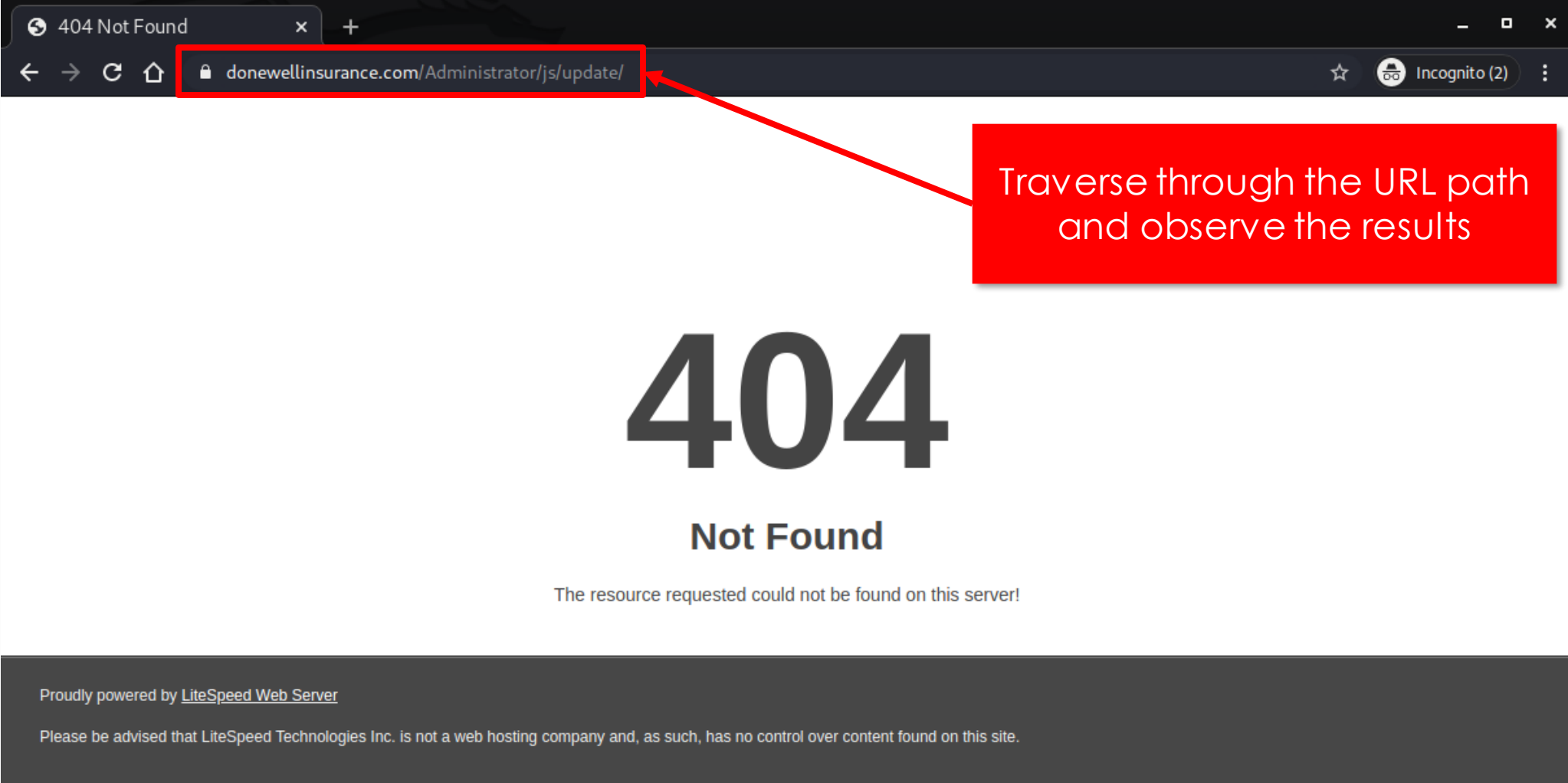
Copy obtained malicious link and open in a web browser

Inspect the phishing page (Unfortunately, it was already taken down at the time of inspection)

Time of Inspection:
~3:45 PM UTC+8 onwards of August 28, 2020



Complexity of Phishing – Phishing Link Analysis



The screenshot shows a web browser window with the address bar containing the URL `donewellinsurance.com/Administrator/js/update/`. The browser title is "404 Not Found". The main content area displays a large "404" and the text "Not Found" followed by "The resource requested could not be found on this server!". A red box highlights the URL in the address bar, and a red arrow points from a red text box to it. The text box contains the instruction: "Traverse through the URL path and observe the results".

Traverse through the URL path and observe the results

404
Not Found

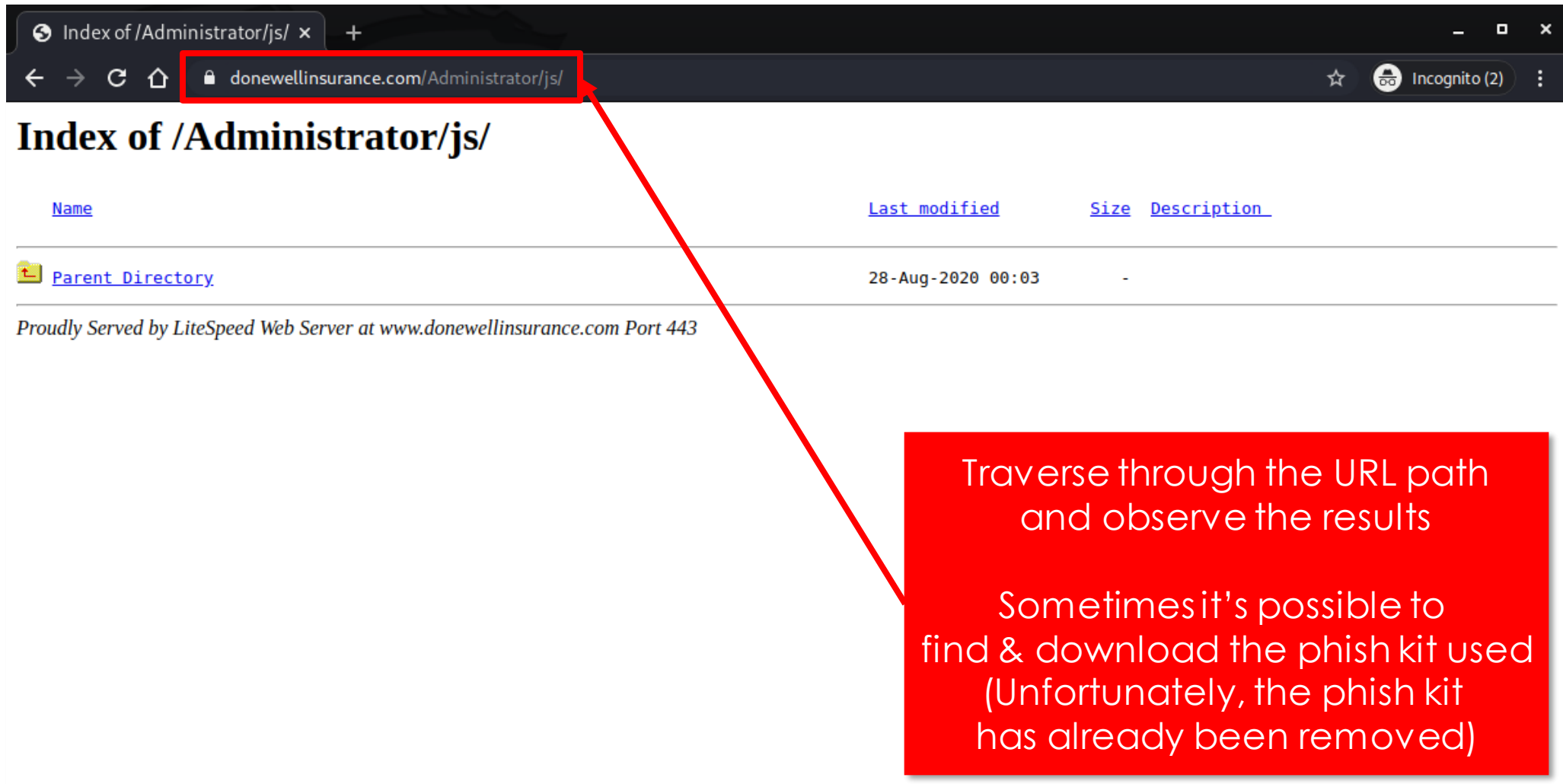
The resource requested could not be found on this server!

Proudly powered by [LiteSpeed Web Server](#)


Please be advised that LiteSpeed Technologies Inc. is not a web hosting company and, as such, has no control over content found on this site.



Complexity of Phishing – Phishing Link Analysis



Index of /Administrator/js/

Name	Last modified	Size	Description
 Parent Directory	28-Aug-2020 00:03	-	

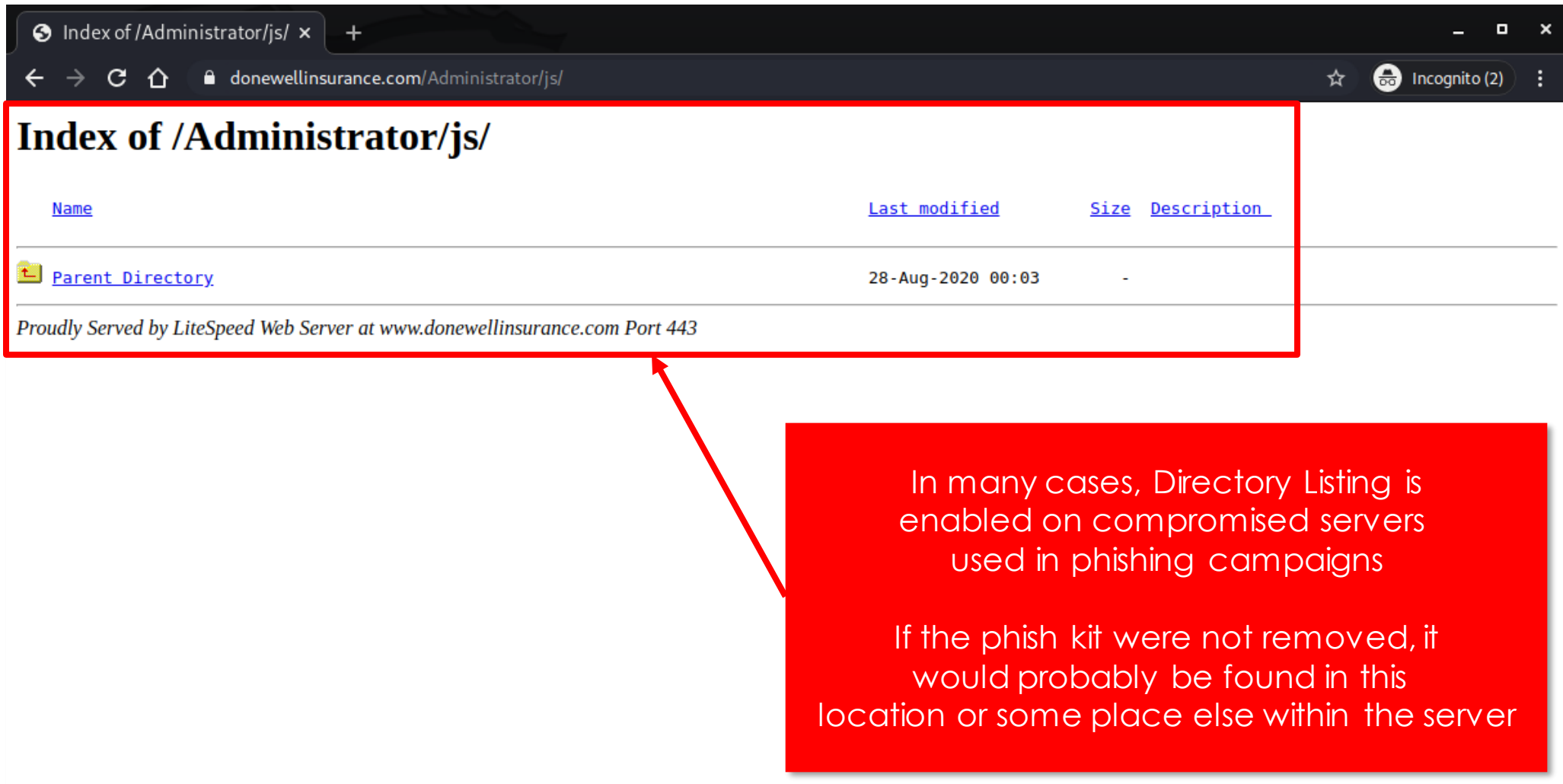
Proudly Served by LiteSpeed Web Server at www.donewellinsurance.com Port 443

Traverse through the URL path and observe the results


Sometimes it's possible to find & download the phish kit used (Unfortunately, the phish kit has already been removed)



Complexity of Phishing – Phishing Link Analysis



Index of /Administrator/js/

Name	Last modified	Size	Description
 Parent Directory	28-Aug-2020 00:03	-	

Proudly Served by LiteSpeed Web Server at www.donewellinsurance.com Port 443

In many cases, Directory Listing is enabled on compromised servers used in phishing campaigns

If the phish kit were not removed, it would probably be found in this location or some place else within the server



Complexity of Phishing – Phishing Link Analysis

Index of /Administrator/js/

donewellinsurance.com/Administrator/js/ Incognito (2)

Index of /Administrator/js/

Name	Last modified	Size	Description
Parent Directory	28-Aug-2020 00:03	-	

Proudly Served by LiteSpeed Web Server at www.donewellinsurance.com Port 443

The path to /Administrator/js/ was last modified on (Server Time): Friday, August 28, 2020 at 12:03 AM UTC+0



Complexity of Phishing – Phishing Link Analysis

Index of /Administrator/js/

donewellinsurance.com/Administrator/js/ Incognito (2)

Index of /Administrator/js/

Name	Last modified	Size	Description
Parent Directory	28-Aug-2020 00:03	-	

Proudly Served by LiteSpeed Web Server at www.donewellinsurance.com Port 443

Possible point of entry:
Exploitation of obsolete and vulnerable software



Complexity of Phishing – Phishing Link Analysis

EXPLOIT DATABASE

Litespeed Technologies - Web Server Remote Poison Null Byte

EDB-ID: 13850 **CVE:** 2010-2333 **Author:** KINGCOPE **Type:** REMOTE **Platform:** MULTIPLE **Date:** 2010-06-13

EDB Verified: ✓ **Exploit:** ⬇ / {} **Vulnerable App:** 📄

Litespeed Technologies Web Server Remote Poison null byte Zero-Day discovered and exploited by Kingcope in June 2010
google gives me over 9million hits

Example exploit session:

```
%nc 192.168.2.19 80
HEAD / HTTP/1.0

HTTP/1.0 200 OK
Date: Sun, 13 Jun 2010 00:10:38 GMT
Server: LiteSpeed <-- consider it 0wned
Accept-ranges: bytes
Connection: close
ETag: "6ff-4c12e288-a3ee"
Last-Modified: Sat, 12 Jun 2010 01:27:36 GMT
Content-Type: text/html
Content-Length: 1791
```

**Possible exploit used:
CVE-2010-2333
(<https://www.exploit-db.com/exploits/13850>)**



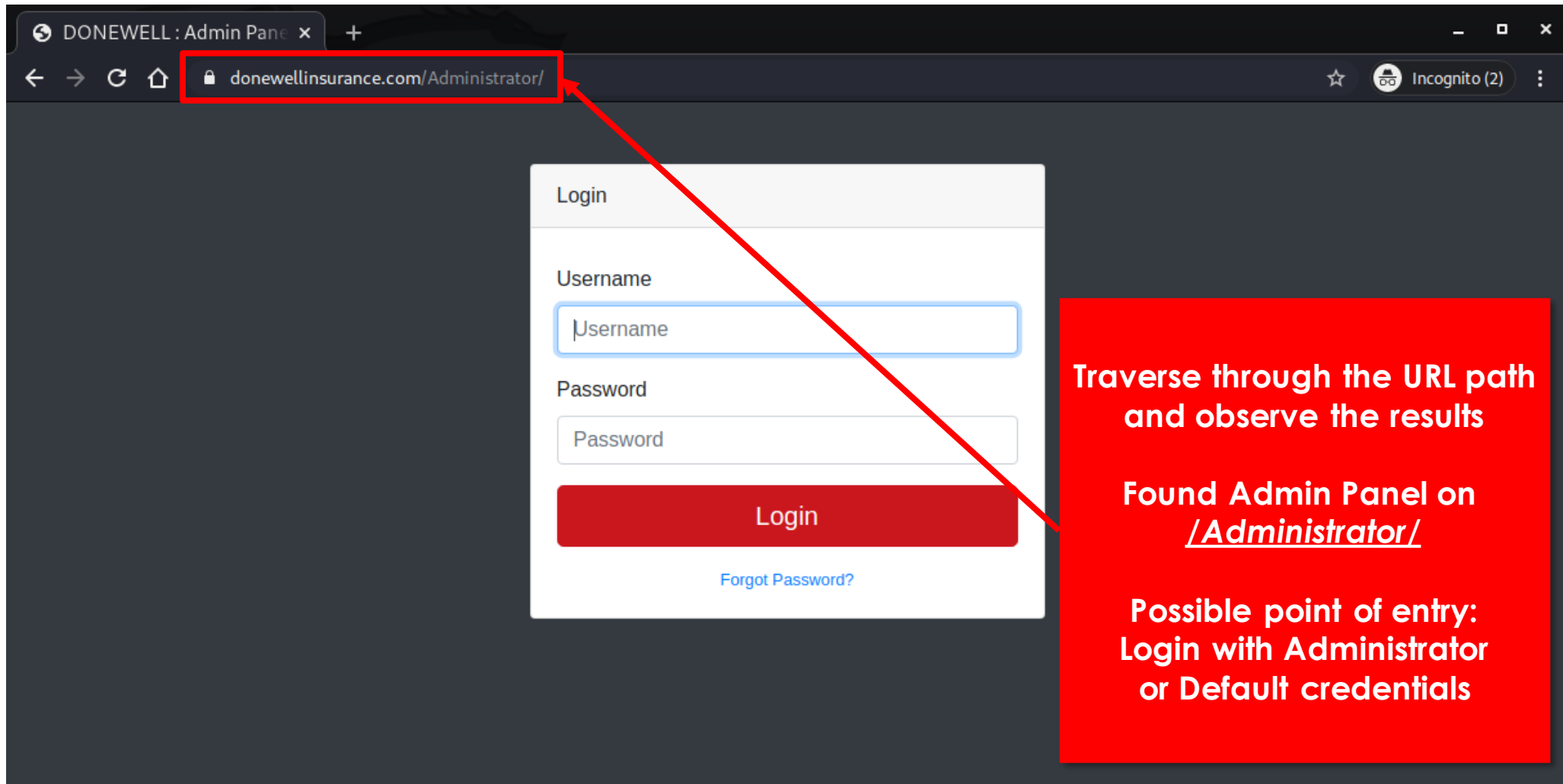
Complexity of Phishing – Phishing Link Analysis

```
Example exploit session:  
  
%nc 192.168.2.19 80  
HEAD / HTTP/1.0  
  
HTTP/1.0 200 OK  
Date: Sun, 13 Jun 2010 00:10:38 GMT  
Server: LiteSpeed <-- consider it 0wned  
Accept-Ranges: bytes  
Connection: close  
ETag: "6ff-4c12e288-a3ee"  
Last-Modified: Sat, 12 Jun 2010 01:27:36 GMT  
Content-Type: text/html  
Content-Length: 1791  
  
%fetch http://192.168.2.19/config.php  
config.php 0 B 0 Bps  
%cat config.php  
%/usr/local/bin/perl Litespeed.pl 192.168.2.19 config.php  
LiteSpeed Technologies Web Server Remote Source Code Disclosure Exploit  
By Kingcope  
June 2010  
  
Saving source code of config.php into 192.168.2.19-config.php  
Completed.  
Operation Completed :>.  
%cat 192.168.2.19-config.php  
<?php  
$db_secret="TOP SECRET PASSWORD";  
>  
%  
  
Exploit:  
  
#!/usr/bin/perl  
#  
#LiteSpeed Technologies Web Server Remote Source Code Disclosure zero-day Exploit  
#By Kingcope  
#Google search: ""Proudly Served by LiteSpeed Web Server""  
#June 2010  
#Thanks to TheDefaced for the idea, http://www.milw0rm.com/exploits/4556  
#
```

**Possible exploit used:
CVE-2010-2333
(<https://www.exploit-db.com/exploits/13850>)**



Complexity of Phishing – Phishing Link Analysis



The screenshot shows a web browser window with the following elements:

- Tab: DONEWELL : Admin Panel
- Address Bar: donewellinsurance.com/Administrator/ (highlighted with a red box)
- Page Title: Login
- Form Fields: Username (with placeholder text 'Username'), Password (with placeholder text 'Password')
- Buttons: Login (red), Forgot Password? (blue)

Traverse through the URL path and observe the results

Found Admin Panel on /Administrator/

Possible point of entry: Login with Administrator or Default credentials



Complexity of Phishing – Phishing Link Analysis

The image shows a screenshot of a phishing email from DoneWell Insurance. The email content includes a greeting 'Dear Customer', a notice about office hours, a phone number '0204332322', and a request to deposit payments into a Prudential Bank account with number '0092906670054'. A red callout box is overlaid on the right side of the screenshot, containing the text 'Default page of the site itself Presumptions' and a list of three points under the heading 'A threat actor:'. A red arrow points from the callout box to the browser address bar in the screenshot, which shows 'donewellinsurance.com'.

Default page of the site itself
Presumptions

A threat actor:

1. *Knowingly obtained Unauthorized Access on this web page*
2. *Uploaded a malicious phishing page / phish kit*
3. *Leveraged their access in this server on a phishing campaign*



Complexity of Phishing – Phishing Link Analysis

Donewell Insurance Company



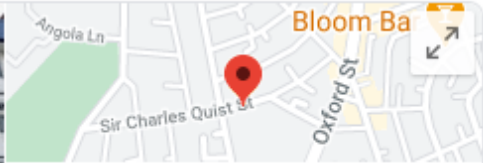
All Images Maps News Shopping More Settings Tools

About 3,560,000 results (0.56 seconds)

www.donewellinsurance.com ▾
Donewell Insurance
Your one-stop **insurance** shop · Bond Bonds **Donewells** Bond covers are: · Bond Electronic Equipment · Bond Money **Insurance** · Bond Bonds · Bond Electronic ...
[Company Profile](#) · [Find Agent or Branch](#) · [Branches](#) · [Management Team](#)

www.donewellinsurance.com > company-profile ▾
Company Profile - Donewell Insurance
DNEWELL INSURANCE COMPANY LIMITED is a private Limited Liability Company, owned by the Methodist church, Institutional Investors, Professional Trade ...

www.facebook.com > Places > Accra, Ghana ▾
Donewell Insurance - Home | Facebook
Donewell Insurance Insurance **Company** in Accra, Ghana · 13,476 people like this · 13,504



Donewell Insurance Company Limited

Website Directions Save

4.2 ★★★★★ 84 Google reviews

Insurance company in Accra, Ghana

Address: Sir Charles Quist St, Accra, Ghana



Complexity of Phishing – Phishing Link Analysis

Donewell Insurance Company

All Images Maps News Shopping More Settings Tools

About 3,560,000 results (0.56 seconds)

www.donewellinsurance.com

Donewell Insurance

Your one-stop **insurance** shop · Bond Bonds **Donewells** Bond covers are: · Bond Electronic Equipment · Bond Money **Insurance** · Bond Bonds · Bond Electronic ...

[Company Profile](#) · [Find Agent or Branch](#) · [Branches](#) · [Management Team](#)

www.donewellinsurance.com > [company-profile](#)

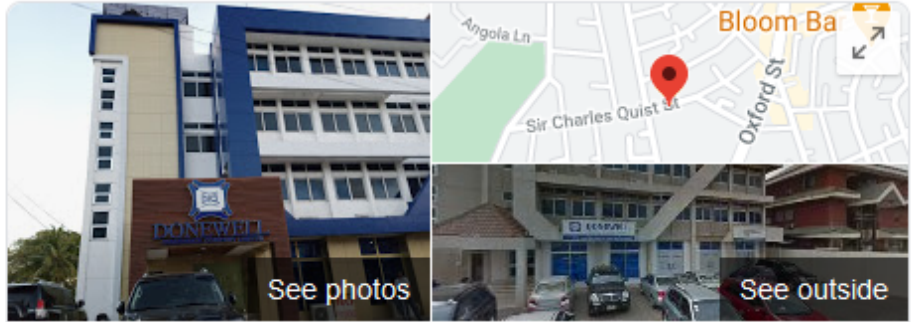
Company Profile - Donewell Insurance

DONEWELL INSURANCE COMPANY LIMITED is a private Limited Liability Company, owned by the Methodist church, Institutional Investors, Professional Trade ...

www.facebook.com > [Places](#) > [Accra, Ghana](#)

Donewell Insurance - Home | Facebook

Donewell Insurance Insurance **Company** in Accra, Ghana · 13,476 people like this · 13,504



Donewell Insurance Company Limited

[Website](#) [Directions](#) [Save](#)

4.2 ★★★★★ 84 Google reviews

Insurance company in Accra, Ghana


Address: Sir Charles Quist St, Accra, Ghana



Complexity of Phishing – Phishing Link Analysis

Time Zone Converter – Time Difference Calculator

Provides time zone conversions taking into account Daylight Saving Time (DST), local time zone and accepts present, past, or future

Sort By: 



Accra, Ghana
GMT (UTC +0)

Fri, 28 Aug 2020

00:03



Manila, Philippines
PHST (UTC +8)

Fri, 28 Aug 2020

08:03



Add another city or time zone...



Complexity of Phishing – Phishing Link Analysis

Index of /Administrator/js/

donewellinsurance.com/Administrator/js/ Incognito (2)

Index of /Administrator/js/

Name	Last modified	Size	Description
Parent Directory	28-Aug-2020 00:03	-	

Proudly Served by LiteSpeed Web Server at www.donewellinsurance.com Port 443

A change was made to /Administrator/js/ on
Philippine Time:
Friday, August 28, 2020 at 8:03 AM UTC+8



Complexity of Phishing – Summary of Findings (Email Body Analysis)

Facts

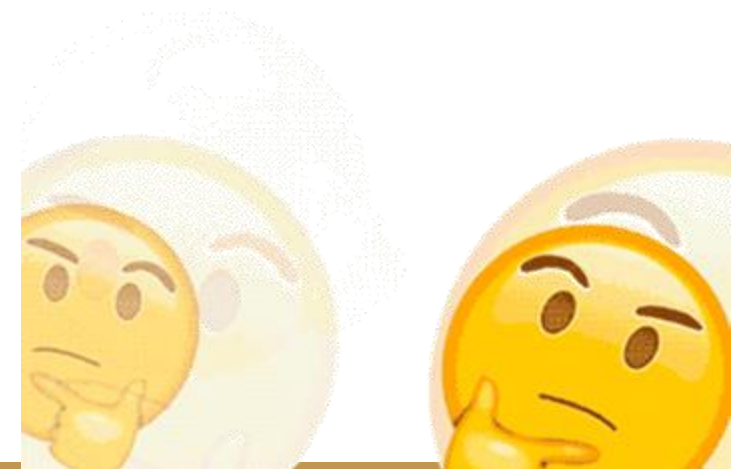
1. The mail was delivered on Friday, August 28, 2020 at 6:35 AM UTC+8
2. The received mail is malicious in nature
 - It intends to deceive recipients that the email came from Metrobank
 - It entices the recipients to click on “**VERIFY MY ACCOUNT**” which contains a concealed malicious link
3. **The domain donewellinsurance.com was used in this phishing campaign**
4. **A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

1. The mail was allegedly sent by a student of ***** University
 - The mail is sent from r.e*****@*****.***.edu.ph
 - The Disclaimer is automatically generated to notify recipients that its contents do not reflect the views of ***** University and its officials
2. **A threat actor compromised the domain donewellinsurance.com**
3. **Possible point of entry / mode of compromise**
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. 08-28-2020 at 6:35 AM UTC +8 (Malicious mail delivered)
2. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)



Complexity of Phishing – Email Header Analysis

The screenshot shows an email client window titled "New System Update - Message (HTML)". The sender is "MetroBank <r.e[REDACTED]@[REDACTED].edu.ph>" and the subject is "New System Update". The email body contains the Metrobank logo and the following text:

Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customerservice@metrobankcard.com or call our 24-hour Customer Service hotline at 8700-700.

[VERIFY MY ACCOUNT](#)

Below the main text, there are three paragraphs of smaller text:

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [REDACTED] University and its officials.

The screenshot shows the "Info" pane for the same email. The title is "New System Update". The pane contains the following options:

- Encrypt**: Encrypt this item. Set up restrictions for this item. For example, you may be able to restrict recipients from forwarding the email message to other people.
- Move to Folder**: Move item to a different folder. Move or copy this item to a different folder. Current Folder: Inbox.
- Resend or Recall**: Message Resend and Recall. Resend this email message or attempt to recall it from recipients.
- Properties**: Properties. Set and view advanced options and properties for this item. Size: 34 KB.

At the bottom of the pane, there are links for "Office Account", "Feedback", and "Options".



Complexity of Phishing – Email Header Analysis

The screenshot shows an email client window titled "New System Update - Message (HTML)". The "File" menu is highlighted in red. The email header shows it was received on "Fri 8/28/2020 06:35" from "MetroBank <r.e[REDACTED]@[REDACTED].edu.ph>" with the subject "New System Update". The email body features the Metrobank logo and a message addressed to a "VALUED CLIENT". The message text includes:

Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customerservice@metrobankcard.com or call our 24-hour Customer Service hotline at 8700-700.

[VERIFY MY ACCOUNT](#)

Below the main message, there are three paragraphs of smaller text:

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [REDACTED] University and its officials.

The screenshot shows the right-hand pane of the email client, titled "New System Update - Message (HTML)". It displays a list of actions for the selected email:

- Info**
- Save**
- Save As**
- Save Attachments**
- Print**
- Close**
- Office Account**
- Feedback**
- Options**

The main content area shows the following options:

- Encrypt this item**: Set up restrictions for this item. For example, you may be able to restrict recipients from forwarding the email message to other people.
- Move item to a different folder**: Move or copy this item to a different folder. Current Folder: Inbox
- Message Resend and Recall**: Resend this email message or attempt to recall it from recipients.
- Properties**: Set and view advanced options and properties for this item. Size: 34 KB



Complexity of Phishing – Email Header Analysis

The screenshot shows an email client window titled "New System Update - Message (HTML)". The "File" menu is highlighted in red. The email header shows the sender as "MetroBank <r.e[REDACTED]@[REDACTED].edu.ph>" and the subject as "New System Update". The email body contains the Metrobank logo and a message addressed to a "VALUED CLIENT". The message text includes:

Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary fields and also check your information in order to continue using our service smoothly.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you are not yet enrolled in Metrobank Direct, you may visit your Metrobank Branch for assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the terms and conditions and other details.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, you may email us at customerservice@metrobankcard.com or call our 24-hour Customer Service hotline at 8700-700.

[VERIFY MY ACCOUNT](#)

Below the main message, there are three disclaimer sections:

Have a hassle-free experience every time you use your card for your online purchases. To proceed with an internet transaction, you need to either input a One-Time-Password (OTP) which you will receive via SMS or email, or answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your mobile number and email address as well as those of your supplementary cardholders. To update your mobile number or email address on our records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [REDACTED] University and its officials.

The screenshot shows the right-hand pane of the email client, titled "New System Update - Message (HTML)". The pane contains a list of actions for the selected email item:

- Info
- Save
- Save As
- Save Attachments
- Print
- Close
- Encrypt this item
- Move item to a different folder
- Message Resend and Recall
- Properties (highlighted in red)

The "Properties" option is highlighted with a red box. Below it, the text reads: "Set and view advanced options and properties for this item." and "Size: 34 KB".



Complexity of Phishing – Email Header Analysis

File Message Help Tell me what you want to do

Delete Archive Reply Reply Forward Move to: ? To Manager Team Email Done Reply & Delete Create New

Delete Respond Quick Steps

Fri 8/28/2020 06:35 MetroBank <r.e.@[redacted].edu.ph> New System Update To m.[redacted]@yahoo.com

Metrobank

Dear VALUED CLIENT,

This is to inform you that some data from your account seems inaccurate or unverified.

For your protection, you have to fill out the form on the given link below and verify the necessary details.

You may also view your latest Statement of Account anytime via Metrobank Direct Facility. If you need assistance and other details.

Thank you for using SOA facility. Please visit our website at www.metrobankcard.com for the latest information.

This is a system-generated email. Please DO NOT REPLY to this. For inquiries and other concerns, please contact our 24-hour Customer Service hotline at 8700-700.

Have a hassle-free experience every time you use your card for your online transactions. Please ensure you answer a few security questions which will appear on your transaction screen.

Ensure the timely receipt of your OTP via SMS or email by keeping us updated with your contact details. If you need records, call our 24-hour Customer Service Hotline at 8-700-700 or 1800-1888-5775.

DISCLAIMER: This message is for the designated recipient only and may contain confidential and/or privileged information. If you have received it in error, please delete it and advise the sender immediately. You should not copy or use it for any other purpose, nor disclose its contents to any other person.

DISCLAIMER: This e-mail and any attachments may contain confidential and/or proprietary information intended for the use of the named recipient/s only. If you are not the intended recipient, any unauthorized disclosure, copying, dissemination or use of any of the information is strictly prohibited. Please notify the sender and immediately delete this e-mail from your system.

Views and opinions expressed in this e-mail are those of the sender. They do not necessarily reflect the views of [redacted] University and its officials.

Properties

Settings: Importance Normal, Sensitivity Normal, Do not AutoArchive this item

Security: Encrypt message contents and attachments, Add digital signature to outgoing message, Request S/MIME receipt for this message

Tracking options: Request a delivery receipt for this message, Request a read receipt for this message

Delivery options: Have replies sent to, Expires after None 00:00

Contacts..., Categories None

Internet headers: Received: from 10.253.62.152 by atlas106.free.mail.gq1.yahoo.com with HTTP; Thu, 27 Aug 2020 22:35:20 +0000; Return-Path: <r.e.@[redacted].edu.ph>; Received: from 40.107.131.129 (EHLO APC01-SG2-obe.outbound.protection.outlook.com) by 10.253.62.152 with SMTPS; Thu, 27 Aug 2020 22:35:20 +0000

Copy Internet headers to Notepad



Complexity of Phishing – Email Header Analysis

X-Forefront-Antispam-Report:
CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:
NLI;SFV:NSPM;H:HK0PR02MB2865.apcprd02.prod.outlook.com;PTR:;CAT:NONE;SFS:(346002)(366004)(376002)(396003)(136003)(39850400004)(6486002)(7116003)(316002)(786003)(8676002)(6916009)(9686003)(15974865002)(83080400001)(8936002)(15650500001)(5660300002)(66574015)(83380400001)(33656002)(18074004)(2906002)(66946007)(186003)(16526019)(166002)(26005)(3480700007)(86362001)(478600001)(33964004)(52116002)(956004)(52536014)(6496006)(66476007)(66556008)(57042006);DIR:OUT;SFP:1102;
X-MS-Exchange-Antispam-MessageData:

yOp3S1/opc+LZ787K1yZkGQvSuaasyORuywt
rNyZpFQ8EXTL98dBtGzbt2xiO C7BDZ9khpj99R/r2iv Q6802
eVTsVy14yviDoxl/jaRV2KjCi/3KHv6yDrr3vndRX4Ydtjm6l
KyGtIuiB59jOfQcUjvYkfkQdAYvB1V Gwqnp6mqZkhYR3Hi
YYJ51cAyW7EPeP17ol695upv RkwyFgjsBvXLeFzlxhO M1a
pHahhM6V eBkOfkl2sBRZB4CVDYKGT8DQej5eok1SGP+
RLKJlORHEQ xrek4h+JJCIDt8M2tX41v qi2nXC d7+86WpuN
46AM+Wev nr67B4D GwF8Aqhw P80+vQflfkQwYN S83
k+hRO IIZy zmx7S1fQhdN6pNtbvRaiZOVj0Wvx SkZQ+7r6
N4V 3tfjAte08v7vRfoHoOk0 1jJu+G9Ge0ZH20BBKrsJdJZA
VyiGiyCa0HyShsX7ID GVCZJNHH98bC3PWdL y1A GurOm r
RCgKudZzeJh8g0WboC vwkYA1jTGQ3VkyQOZYPSxyOk2f
Cy0ocF shiBgTrPyQkifDIVFhJe19hyAVSi6Tcq52QKpBwC
yrlbN3NOoFJIrgooovfDZ32qhuKfx+iR3v8NHH+EytTF3py
uhp5/cAPzoUTUdeLmufQkfh04s5X9A==

X-OriginatorOrg: *****@****.edu.ph
X-MS-Exchange-CrossTenant-NetWork-Message-Id:
fbf2ca38-fd55-436b-d4d9-08d84ad978d7

X-MS-Exchange-CrossTenant-AuthSource:
HK0PR02MB2865.apcprd02.prod.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27
Aug 2020 22:35:17.2632
(UTC)

X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-
96d7-17f29e16cb16

X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName:
SbWDtj/YNwqtPcqnp7ry6eQmQIOFW7coJ7JfyItrN Y6M
NEbv ezfa4vJ+BFZxlyxVGzNxa+pi+GPLMH+mfa+F2hor
ID93V m+mqNNQWBFpCoLw8Jp9d022A ONrPtoF

X-MS-Exchange-Transport-
CrossTenantHeadersStamped: HK0PR02MB3057
Content-Length: 19551

From: "MetroBank" <r.e*****@*****.edu.ph>
To: m*****@yahoo.com
Date: 27 Aug 2020 22:35:16 +0000
Subject: New System Update
Content-Type: multipart/alternative;
boundary = --boundary_5207_32343822-bb55-489c-a2f2-
1cb55229337b
X-ClientProxiedBy:
MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) To
HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
Message-ID:

<HK0PR02MB2865CA6172E4053B117B1CB493550@HK0PR02
MB2865.apcprd02.prod.outlook.com>
MIME-Version: 1.0

X-MS-Exchange-MessageSentRepresentingType: 1
Received: from EC2AMAZ-59M1G4T (54.89.76.235) by
MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) with Microsoft SMTP Server
(version=TLS1_0,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id
15.20.3326.19 via Frontend Transport; Thu, 27 Aug 2020
22:35:16 +0000

X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: bfb2ca38-fd55-436b-
d4d9-08d84ad978d7
X-MS-TrafficTypeDiagnostic: HK0PR02MB3057:
X-Microsoft-Antispam-PRV5:

<HK0PR02MB3057814CAF98268E3FB77DE493550
@HK0PR02MB3057.apcprd02.prod.outlook.com>
X-MS-Ob-TLC-OOBClassifiers: OLM:7691;
X-MS-Exchange-SenderADCheck: 1
X-Microsoft-Antispam: BCL0;
X-Microsoft-Antispam-Message-Info:

wIih2oxFVx0uqxy CdFtPBRJ5i7Jq4eN4P Bfv4X/hXfbx
u9kv am7EUuuDXhXwB/II1+sRwTO9UP2M7dPMU6XzuEO/Ux61
oXL4t3v bay 5nSA XKXmAX0LeRes9T5I81pn4nd6i8itPwKmm3I8g
vQ8HmbZ+kuM3xdp69QaFY+Mt0tCfPcrCFpE3W7D/LSI8P/8
V7SfmwDF8dDjonYfUgoYhZQchogy Y02teKE+Q5eNczcTOpeS+/
o/mhXYq1GQIPT1BnYwEz1.fpg4vmEmemxVhEzta3s0c6HhcVza
k2EY9h52wngO LZ7epas020cf2d4BPnQAZuEJfQGDb7D Wlby/x
Zsm1wc+FGLpeD05Jm476e9tD GodP3/ABRei3II+AY0SQUeR4R
D8Uc7Avmuhzv6k3kyAQnAwHb4DUeGLV PEDCDFrG9lkIG
TEA 74Aeja6zmmWlGjMILU6yndTPR1tGg9y9yK54gx1pOD7D
X7Jn5k0bzYrkauKsGp5ruD680 KM1QYCRadRbyvFK1Q==

ARC-Message-Signature: i=1; a=rsa-sha256;
c=relaxed/relaxed; d=microsoft.com;
s=arcselector9901;
h=From:Date:Subject:Message-ID:Content-Type:MIME-
Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3O01iR7SNx01kr1nY1txa5GzdSefOocWpSxOFpw=;

b=H5wDTRdULUMRG5E5Ru+/VeE24Oc3pAl16B4sqAPcu2IEsc9
U8Jf+ZcVfcm122xhLphpoETtDUkNaD/haByLV0kGqENP16tJg
crpF5kDQmuUzAQO1t+ns/1g/Y7y7ZxGN9epYHP3KWAL4MZU
AWURVu913Pnfy+vY5JZXArA7V03gwkQ4TNUMdW+CcgFToRs
b251TycHT2dex5tZ/h/5eGcGMD9bIH5t0ixSf/ytA8+yX9egTrX
nrkZ497UBPInnMQBSBgCe9aj5tjpuK9v0rZxj/bxG85Dhe/IVgh
IOfbxhH7WFx032NfMA6Lkjd7QeBqxMpHmv2C4BgFfifuz6Q==
ARC-Authentication-Results: i=1; mx.microsoft.com 1;
spf=pass
smtp.mailfrom=*****@****.edu.ph; dmarc=pass
action=none
header.from=*****@****.edu.ph; dkim=pass
header.d=*****@****.edu.ph;
arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=****eduph.onmicrosoft.com; s=selector2-****eduph-
onmicrosoft.com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-
Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3O01iR7SNx01kr1nY1txa5GzdSefOocWpSxOFpw=;

b=RzyjYmSzt1SYeb+wRfAJL+ubrD6K8DUneT8uwrxSIQgPoX
jEDeOAxL1qSeywVlvrh61YXR7k5pSLmkCB3XV2qCBghv089Ky
vO8m0BgY4cvXPg3Q8TxYVIEIDPOEi+LctCuybO3fXArUE42E1
BTTD9lkP89WSCb9N597rcIQj4=
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
by HK0PR02MB3057.apcprd02.prod.outlook.com
(2603:1096:203:60::15) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.3326.23; Thu, 27 Aug
2020 22:35:17 +0000
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551]) by
HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551%3]) with mapi id
15.20.3326.019; Thu, 27 Aug 2020
22:35:17 +0000

Received: from 10.253.62.152
by atlas106.free.mail.gq1.yahoo.com with HTTP; Thu, 27 Aug 2020 22:35:20
+0000
Return-Path: <r.e*****@*****.edu.ph>
Received: from 40.107.131.129 (EHLO APC01-SG2-
obe.outbound.protection.outlook.com)
by 10.253.62.152 with SMTPS; Thu, 27 Aug 2020 22:35:20 +0000
X-Originating-IP: [40.107.131.129]
Received-SPF: pass (domain of *****@****.edu.ph designates
40.107.131.129 as permitted sender)
Authentication-Results: atlas106.free.mail.gq1.yahoo.com;
dkim=pass header.i=*****@****eduph.onmicrosoft.com header.s=selector2-
****eduph-onmicrosoft-com;
spf=pass smtp.mailfrom=*****@****.edu.ph;
dmarc=unknown
X-Apparently-To: m*****@yahoo.com; Thu, 27 Aug 2020
22:35:20 +0000
X-YMailISG: dZoOSyGwLDuaGRLRXLozvXn0nyD7V93xf9wvz8loG5kh8P

X.Q5jdXsUsQhUKCySYGNL9VQMDhNEUUDyAcAfxaaYMur6nrhqwWl0wzGe
aObmqBkff95PDbcPtj_n5fEKKI4K705Vz_cjCYFIT73gp36_G14AWfqIBY1Y
o5wRCSSsTHmccHsSq41uZqJfe_t9WQ6RvA6i56D1Qeple777E.C11Lfl1f9
ANsWQY8kvI6VHCYT1vWkA86sWqxQ_IA5_I50xJ_BppCffrD2C288md.or7JO
MizbrxN4S7vM0tbs53BUoywC9XDNIuYccPzvpCqBhs8RlwrIaw0Z70djqQC
xMC9sPPFknCR7Jn_e2NRBeCi7kZ9AsgPLOI.U28EvgGp3EtHQ1_IU2UPC_a

5ZA_x_WGWR54XhNDRPOx3hY9uCMckxi8wv7hwzmkC80rVQWARi.OXqPKRKY
SvzPh2hi5Q1G3RIhbSAOe0nAYNsG2jAMBjP_RAC7cpoghtCVcb1TEdE.Jwc
XTwYn1T7LMLRLMbyIq2PtBk2n5dy7fghMjfiNzykiMrZeytFONF07JMd9jYZ
.3qihbg_EfuulLFqn5tfdSrbOoVjujm7QglFiYqQ26uUAHI94m6tM27jWSP
8anwRmA_4RAwPqth6R2BYP3xBjvY8O9se2vsKojzVjFQEHTErZOAYg91bB
8h3Sj39.JdvGOIR7rInIcZe9Bbc6U9A8a22huBH90xwBri1N66FXlYZczf
vQldVkv5Fndz2pg1YZMxhC7_nXpHC9oPqByRpJ6Gj.9DAs_8Fa9IsHhYH3iPg
faKePbXOLgbmkDQXNT0VbiPhfXkGzfpByTjHhAJvuFqUqmb1OqWMMXNfhrl
h_Oy9grgmkc23h7ktnJDYOWjKAAGawjOvOfksLsYGIuzGQoJDFpwiOHxFeA.
owu4n6NDdQlCmRGmRdyzBDV_EtNgwFWyZ8zuTSPXe1Rf28Q957EzQ8alfnx
TrA bZN50Wuuuq uDfjTjHPKQOXfXA f2KwDqskAVfQDF7y7z1p2btD.ZF5S5Yb
4a5UtyF4jUrZxlvouA2a00GYBdRau7pFSna0A1uTnZxMdcB.dX7wbmBF1M
EsKQukb.ivdievg6kr_kkaw4tFZ3GuVKf9ge1GpBUv0JKRI_OCIxy.QiFr
JZW2J5F.U0iwMblfYKdc4r5TWWms7BH2HEJrfCkt2c2f27dM5r7
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com;
cv=none;

b=RRMeC660NNWqY/yipRsh6ZVxGg3/pTP24FYCYHOI9fd0Lb9yS6NUEI9/WU6
NUbv0Uis2zDK3QKE7Rro/WO08wniQ911RCCR+drFV2db84B2HCW0s4Qx7a1
u7IMoY09Aifv3WjT1TmOgqJRF8A0beToZkxjT5vZH9Q4+XpXqOgePete57
SGBmVbzHXQNNIn29QvB0RG/n2u4a+DwQXhff/11Mpdw1u6j9K7sM8Mi
O1ssN0gk82mncvFOsQIPaul3ly7rG42n8z0Nu06Pm9ziC6ByBHM6biKlmeif
AQrTY+VfIGHm5SBgPUawTE+Fl2y+cvHUxOg==



Complexity of Phishing – Email Header Analysis

X-Forefront-Antispam-Report:
CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:
NLI;SFV:NSPM;H:HK0PR02MB2865.apcprd02.prod.outlook.com;PTR:;CAT:NONE;SFS:(346002)(366004)(376002)(396003)(136003)(39850400004)(6486002)(7116003)(316002)(786003)(8676002)(6916009)(9686003)(15974865002)(83080400001)(8936002)(15650500001)(5660300002)(66574015)(83380400001)(33656002)(18074004)(2906002)(66946007)(186003)(16526019)(166002)(26005)(3480700007)(86362001)(478600001)(33964004)(52116002)(956004)(52536014)(6496006)(66476007)(66556008)(57042006);DIR:OUT;SFP:1102;

X-MS-Exchange-AntiSpam-MessageData:
y0p3S1/opc+LZ787K1yZkQGvSuaasyORuywrt
rNy zPFQ8EXTL98dBtGzbt2xiO C7BD29khpj99R/r2iv Q6802
eV Tsvy 14yviDox1/jaRV2KjCi/3KHv6yDrr3vndRX4Ydtjm6l
KyGtIuiB59jOfQcUjvfkfQdAYvB1Vgwnp6mqZkhYR3Hi
YYJ51CaYw7EPeP17ol695upv RKWYFgsjBvXlefZlxhO M1a
pHahhM6V eBkOfkl2sBRZ4CVDYKGT8DQej5eok1SGP+
RLKJlORHE Qxrek4h+JJCIDt8M2tX41v qiznXC d7+86WpuN
46A M +Wew nrR67B4D GwF8Aqhw P80+VQflfkQwYN S83
k+hRO IIZy zmx7S1fQhdN6pNtbvRaiZ0Vj0Wvx SkZQ+7r6
N4V 3tjfAte08v7vRfoHoOk0 1jIu+G9Ge0ZH20BBKrsUdJZA
VyiGiyCa0HyShsX7ID GVCZJNH898C3PWdlY 1A GurOm R
RCyKudZzeJh8g0WboCvkwYA1jTGQ3VkyQOZYPSxyOk2f
Cj0ocFshIBgTrPyQkifDIVFhJe19hyAVsI6Tcq52QKpBwgC
yrlbN3NOoFJIrgoovfFdZ3zqhuKfx+ir3v8NHh+EytTF3py

X-OriginatorOrg: *****@****.edu.ph
X-MS-Exchange-CrossTenant-NetWork-Message-Id:
fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-Exchange-CrossTenant-AUTHSource:
HK0PR02MB2865.apcprd02.prod.outlook.com
X-MS-Exchange-CrossTenant-AUTHAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27
Aug 2020 22:35:17.2632
(UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-
96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName:
SbWDTjY Nw qtpCqy np7ry6eQmQOFWcoJ7JfY ItrN Y6M
NEbv ezfa4vJ+BFZxlyxVGzNxa+pi+GPLMH+mfa+F2hor
I9D3V m+qNNQWBFpCoLw8Jp9d0Z2A O NRPtoF
X-MS-Exchange-Transport-
CrossTenantHeadersStamped: HK0PR02MB3057

From: "MetroBank" <r.e*****@*****.edu.ph>
To: m*****@yahoo.com
Date: 27 Aug 2020 22:35:16 +0000
Subject: New System Update

Content-Type: multipart/mixed;
boundary="--boundary_5207_32343822-bb55-489c-a2f2-1cb55229337b
X-ClientProxiedBy:
MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) To
HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
Message-ID:

<HK0PR02MB2865CA6172E4053B117B1CB933550@HK0PR02MB2865.apcprd02.prod.outlook.com>
MIME-Version: 1.0

X-MS-Exchange-Message-Content-Representation:
Received: from EC2AMAZ-59M1G4T (54.89.76.235) by
MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) with Microsoft SMTP Server
(version=TLS1_0,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id
15.20.3326.19 via Frontend Transport; Thu, 27 Aug 2020
22:35:16 +0000
X-Originating-IP: [54.89.76.235]

X-MS-Exchange-Organization: HK0PR02MB3057;
X-MS-OFFICE365-FILTERING-CORRELATION-ID: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-Microsoft-Exchange-Organization: HK0PR02MB3057;
X-Microsoft-Antispam-PRV S:
<HK0PR02MB305714CAF9826E83FB77DE493550

@HK0PR02MB3057.apcprd02.prod.outlook.com>
X-MS-OB-TLC-OOBCLASSIFIERS: OLM:7691;
X-MS-Exchange-SenderADCheck: 1
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:
wIih2oxFVx0uqxy CdFtPBRJ5i7Jq4eN4P Bfv4X/hXfbx
u9kv am7EU uuDXhXw B/II1+sRwTo9UP2M7dPMU6XzuEO/Uxg61
oXL4t3v bay 5nSA XKXmAX0LeRes9T5I81pn4nd6i8itPw Kmm3I8g
v Q8HmbZ+kuM3xdp69QaFY+MtoCfPcrCFPe3W7D/LSI8P/8
V7Sfmw DF8dDjonY fUgoYhZ0chogy YO2teKE+Q5eNczcTOpeS+/o
mhXYq1GQ IPT1BnYwEz1.fpg4vmEmemxVhEtza3s0c6H hcVza
k2Eiy9h52wng O LZr7epas020 cf2d4BP NQAZUJEfIqGDb7D WlbyX
Zsm1wc+FGLpeD O5Jm476e9tD GodP3/ABRei3II+AYOSQUEr4R
D8Uc7A vmmuhzv63kwyAQnAwWbH4DUeGLV PEDCDFrG9lkIG
TEA 74Aeja6zmmWlGjMILUj6nDTPR1TfGg9y9yK54gxY1pOD7D
X7Jn5k0bzYrkauKsGp5ruD680 KM1QYCRadRbyvFK1Q==

ARC-Message-Signature: i=1; a=rsa-sha256;
c=relaxed/relaxed; d=microsoft.com;
s=arcselector9901;
h=From:Date:Subject:Message-ID:Content-Type:MIME-
Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3O01iR7SNx01kr1nY1txa5GzdSefOocWpSxOfPpw=;

b=H5wDTRdULUMRG5E5Ru+/VeE24Oc3pAl16B4sqAPCu2IEsc9
U8Jf+ZcVfcm122xhLphpoETtDUkNaD/haByLV0kGqENP16tJg
crpF5kDQmuUzAQOIt+ns/1g/Y7y7ZxGN9epYHP3KWAL4MZU
AWURVu913Pnfy+vY5JZXArA7V03gwKQ4TNUMdW+CcGFTORs
b251TycHT2dex5tZ/h/5eGcGMD9bIH5t0ixSf/yTA8+yX9egTrX
nrDKZ497UBPInnMQBSBgCe9aj5tjpuK9vORzXj/bxG85Dhe/IVgh

ARC-Authentication-Results: i=1; mx.microsoft.com 1;
spf=pass
smtp.mailfrom=*****@****.edu.ph; dmarc=pass
action=none
header.from=*****@****.edu.ph; dkim=pass
header.d=*****@****.edu.ph;
arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=*****@****.edu.ph; s=selector2-***@****.edu.ph;
onmicrosoft.com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-
Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3O01iR7SNx01kr1nY1txa5GzdSefOocWpSxOfPpw=;

b=RzyjYmSzt1SYeb+wRfAJL+ubrD6K8DUneT8uwrxSIQgPoX
jEDeOAxL1qSeywVlv rh61YXR7k5pSnlmKCB3XV2qCBghv089Ky
vO8m0BgY4cvXPg3Q8TxyVIEIDPOEi+LctCuybO3fXArUE42E1
BTTD9lkP89WScb9N597rcIQj4=
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
by HK0PR02MB3057.apcprd02.prod.outlook.com
(2603:1096:203:60::15) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.3326.23; Thu, 27 Aug
2020 22:35:17 +0000

Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551]) by
HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551%3]) with mapi id
15.20.3326.019; Thu, 27 Aug 2020
22:35:17 +0000

Received: from 10.253.62.152
by atlas106.free.mail.gq1.yahoo.com with HTTP; Thu, 27 Aug 2020 22:35:20
+0000
Return-Path: <r.e*****@*****.edu.ph>
Received: from 40.107.131.129 (EHLO APC01-SG2-
obe.outbound.protection.outlook.com)
by 10.253.62.152 with SMTPS; Thu, 27 Aug 2020 22:35:20 +0000
X-Originating-IP: [40.107.131.129]
Received-SPF: pass (domain of *****@****.edu.ph designates
40.107.131.129 as permitted sender)
Authentication-Results: atlas106.free.mail.gq1.yahoo.com;
dkim=pass header.i=*****@****.edu.ph header.s=selector2-
@*.edu.ph onmicrosoft.com;
spf=pass smtp.mailfrom=*****@****.edu.ph;
dmarc=unknown
X-Apparently-To: m*****@yahoo.com; Thu, 27 Aug 2020
22:35:20 +0000
X-MailSize: dZoO SYgWLDuaGRLRXLxvLnOnyD7V93xf9wvz8loG5khl8P

X-Q5jdXsUsQ hUKCySYGNL9VQMDhNEUUDUyAcAfxaaYMur6nrhqw Wl0wzZe
aObmQbKbf95PDbcPtj_n5FEKKI4K705Vz_cjCYFIT73gp36_G14AWfqIBY1Y
o5wRCSSsTvmccHsSq41uzJqf_t9WQ6RvA6i50D1Qeple777E.C11Lft1f9
ANsWQY8Hv16VHCYT1vWka86sWqxQ_IA5_I50xJ_BppCfrrDc288md.or7JO
MizbrxNv4S7vM0tbs53BUoywC9XDNIuYccPzvpCqBhs8Wrlwaz0W9djQC
xMC9sPFFknCR7Jn_e2NRBeCi7kz9AsgPLOI.U28EVG6p3EtHQ1_IU2UPC_a

5ZA_x_WGWR54XhNDRPOx3hY9uCMckxi8wv7hwzmkC80rVQWARi.OxqPKRkZy
SvzPh2hi5Q1G3RlhbSAOe0nAYnsG2jAMBjP_RAC7cpoghtCVcb1TEdE.Jwc
XTwYN1T7LMLRLMbyIq2tPbK2nSdy7fghMjflNzykiMrZEytcFONF07JM d9jYZ
.3qihbg_EfuULfqn5tfdSrbO OvjujM7QglFiYqQ26uUAHl94m6tM27jWSP
8anwRmA_4RAwPqth6R2BYP3xBjvY8O9se2vsKojzVjFQEHTErZOAYg91bB
8h3Sj39.JdvGOIR7rInCze9Bbc6UT9AK8a22huBH90xwBR11N6FXIYZczf
vQldVksVfndz2pg1Y ZMXhC7_nXpHc9oPQByRpJ6Gj.9DAs_8Fa9IsH YH3iPg
faKePbxO LgbmkDQXNTOVbiPhfXkGzfpBytjHhaJvuFqUqmb1OqWMMXNfhrl
h_Oy5grgmkc23h7kNJDYOWjKAAGawjovOfksLSyGIuzGQoJDFpwiOHxFeA.
owu4n6NDdQlCmRGmRdyzBDV_EtNgFWyZ8zuTSPXe1Rf28Q957EzQ8alfnx
TrA BzN50Wuuuq uDFgTjHPKQXQfXA f2KwDqskAVfQDF7Y7z1p2btD.ZF5BSYb
4a5UtyF4jUrZVxlvouA2a0GYBdRau7pFSna0A1uTnXzMcDb.dX7wbmBF1M
EsKQubk.Ivdielg6n6kr_kkaw4tFZ3GuVKcf9ge1GpBUv0JKR1_OCIXY.QiFr
JZW2J5FvOiwMblfYKdc4r5TWWms7BH2HEJrfCkt2c2f27dM5r7
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com;
cv=none;

b=RRMeC660NNWqY/yipRsh6ZVxGg3/pTP24FYCYHOI9fd0Lb9yS6NUEI9/WU6
NUbv0Uis2zDKE3QkE7Rro/WO08wniQ911RCCR+drFV2db84B2HcWos4Qx7a1
u7IMoY09Aifv3wJT1TmOggJRF8A0beToZkxjT5vZH9Q4+XpXqO0gePete57
SGBmVbzHxQNOINIz9QvB0RG/n2w4a+DwQXhff/11MP2nd1u6j9K7sMB8I
O1ssN0gk82mncvFOsQIPaul3ly7rG42n8z0nuO6Pm9ziC6byBHM6biKlmeif
AQrTY+VfIGHm5SBgPUawTE+Fl2y+cVHUxOg==



Complexity of Phishing – Email Header Analysis

Mail Header Analyzer (MHA) Home

Subject: New System Update
 Message-ID: <HK0PR02MB2865CA6172E4053B117B1CB493550@HK0PR02MB2865.apcprd02.prod.outlook.com>
 Creation time (Date): 27 Aug 2020 22:35:16 +0000
 From: "MetroBank" <r.e*****@*****.edu.ph>
 To: m*****@yahoo.com

Total Delay is: 4 sec

Delay in seconds.

Hop	From	By	With	Time (UTC)	D
1	EC2AMAZ-59M1G4T (54.89.76.235)	MN2PR12CA0021.namprd12.prod.outlook.com (2603:10b6:208:a8::34)	Microsoft SMTP Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA)	08/27/2020 10:35:16 PM	0
2	HK0PR02MB2865.apcprd02.prod.outlook.com ([fe80::2804:771c:f26c:f551])	HK0PR02MB2865.apcprd02.prod.outlook.com ([fe80::2804:771c:f26c:f551%3])	mapi	08/27/2020 10:35:17 PM	1
3	HK0PR02MB2865.apcprd02.prod.outlook.com (2603:1096:203:37::22)	HK0PR02MB3057.apcprd02.prod.outlook.com (2603:1096:203:60::15)	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	08/27/2020 10:35:17 PM	0
4	40.107.131.129 (EHLO APC01-SG2-obe.outbound.protection.outlook.com)	10.253.62.152	SMTPs	08/27/2020 10:35:20 PM	3
5	10.253.62.152	atlas106.free.mail.gq1.yahoo.com	HTTP	08/27/2020 10:35:20 PM	*

Security Headers

Received-SPF	pass (domain of *****.edu.ph designates 40.107.131.129 as permitted sender)
Authentication-Results	atlas106.free.mail.gq1.yahoo.com; dkim=pass header.i=@*****.edu.ph; dmarc=pass action=none header.from=*****.edu.ph; dkim=pass header.d=*****.edu.ph; arc=none
ARC-Authentication-Results	i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=*****.edu.ph; dmarc=pass action=none header.from=*****.edu.ph; dkim=pass header.d=*****.edu.ph; arc=none
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=*****.edu.ph; s=selector2-*****.edu.ph; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-Bh=YpPL3OO1iR7SNx01kr1nY1xa5GzdSeI0ocWpSxOFpw=; b=RzyjYmSZt1SYeb+wRfAJL-ubrD6K8DUneT8uwwrxSIQgPoXjEDe0AxL1qSeywVlvrh61YXR7k5psNLmkCB3XV2qCBghv089KvYv08m0BgY4cvXPg3Q8TxYVIEIDPOEI+LctC

X-headers

Vincent Yiu @vysecurity

Red / Blue Team Tip: If you're still reading e-mail message headers using Notepad, you're doing it wrong. Check out Message Header Analyzer: mha.azurewebsites.net

It'll save your eyes 🤖 #cyber #redteam #blueteam #suspiciousemails

2:38 AM · Sep 9, 2021 · Twitter Web App

52 Retweets 1 Quote Tweet 229 Likes

References:

- <https://twitter.com/vysecurity/status/1435673942589521922>
- <https://github.com/cyberdefenders/email-header-analyzer>
- <https://mha.azurewebsites.net/>



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-TrafficTypeDiagnostic: HK0PR02MB3057:
X-Microsoft-Antispam-PRVS:
<HK0PR02MB3057814CAF98268E3FB77DE493550@HK0PR02MB3057.apcprd02.prod.outlook.com>
X-MS-Obb-TLC-00BClassifiers: OLM:7691;
X-MS-Exchange-SenderADCheck: 1
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:

wIih2oxFVx0uqxyCdFtPBRJ5i7Jq4eN4PBfv4X/hXfBxU9kvam7EUuuDXhXwB/II1+sRwT09UP2M7dPMU6XzuE0/Ux61oXL4t3vbay5nSAXKXmAX0LeRes9T5I81pn4nD6i8itPwKmm3I8gvQ8HmbZ
+kuM3xDp69QaFY++Mt0tCfPcrRCfP3E3W7D/LSI8P/8V75fwmDF8dDjonYfUgoYhZ0chogyY02teKE+Q5eNczcT0peS
+/o/mhXYq1GQ1PT1BnYwEz1IfpG4vmEmemxVhEtza3s0c6HhcVZak2EiY9h52wngOLZr7epas020cF2d4BPNQAZUJEfIqGDb7DWLb/xZsm1wc+FgrLpeD05Jm476e9tDGodP3/ABRei3II
+AY0SQuEr4RD8Uc7Avmmuhzv63kwyAQnAwVHb4DUIeGLVPEDCDFrG9l1k1GT7EA74Aeja6zmnWIGjM1LU6ynDTPRrItG9y9/yKS4gxY1p0D7DX7Jn5k0bzYrkauKsGp5ruD680KM1QYCRadRbyvFK1Q==
X-Forefront-Antispam-Report:
  CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:NL1;SFV:NSPM;H:HK0PR02MB2865.apcprd02.prod.outlook.com;PTR:;CAT:NONE;SFS:(346002)(366004)(376002)
(396003)(136003)(39850400004)(6486002)(7116003)(316002)(786003)(8676002)(6916009)(9686003)(15974865002)(83080400001)(8936002)(15650500001)(5660300002)
(66574015)(83380400001)(33656002)(18074004)(2906002)(66946007)(186003)(33656002)(16526019)(166002)(26005)(3480700007)(86362001)(478600001)(33964004)(52116002)(956004)
(52536014)(6496006)(66476007)(66556008)(57042006);DIR:OUT;SFP:1102;
X-MS-Exchange-AntiSpam-MessageData:
  y0p3S1/opc
+LZ787KIyzKGVsuaasyORuywtrNyzPfQ8EXTL98dBtGzbt2xi0C7BDZ9khip99R/r2ivQ680ZeVtSvy14yviDoxI/aRV2KjCi/3KHv6yDrr3vndRX4Ydtjm6lKygiuiB59j0fQcUvkvfekQdAYvB1VGwqN6
mqZkhYR3HiYY/51CaYw7EPEp17o1695upvRKWYFgsjBvXLeFzLxhOM1apHahhM6lVeBk0fk12sBRZB4CVDYKGT8DQeJ5eok1SGP+RLKJL0RHEQxrek4h+JJCLDt8M2tX41vqi2nXCd7+86WpuN46AM
+WevnrR67B4DGwF8AqhwP80+vQfLfkKQwYNS83k+rH0ILZyZmx7S1fQHdN6pNtbvRaiZ0VjWxvSkZQ+7r6N4V3tFjAte08v7vRfoHo0kv1iJu
+G9GeoZH0BBKrsUdJZAVyiG1YCa0HyShsX7IDGVCZJNHH98bC3PwDl/y1AGur0MrRCgKudZzEJh8g0WboCvkwYA1jTGQ3VkyQ0ZYPSxyOk2fCyoocFshiBgTrPyQkiFdIVFhJe19hyAVsI6Tcq52QKpBwgCy
r1bN3N0oFJIRgoovFFdZ32qhuKfx+iR3v8NHH+EytTF3pyuhp5/cAPZo0tUdeLmufQKfhs04s5X9A==
X-OriginatorOrg: ██████████.edu.ph
X-MS-Exchange-CrossTenant-Network-Message-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-Exchange-CrossTenant-AuthSource: HK0PR02MB2865.apcprd02.prod.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27 Aug 2020 22:35:17.2632
(UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName: SbWdtj/YNwqtPcqvn7ry6eQvmq10FW7coJ7JFyItrNY6MNEbVezfa4vJ+BFzxlyoxVGzNxa+pI+GPLMH+mfA+F2horI9D3Vm
+mQNNQWBFpCoLw8JpJ9d0Z2AONrPtoF
X-MS-Exchange-Transport-CrossTenantHeadersStamped: HK0PR02MB3057
Content-Length: 19551
```

PRE-ANALYSIS NOTES

Mail Headers can contain non-standard headers which vary depending on the mail server & mail client that the mail passed through

- An email from Gmail to Yahoo will have different headers than an email from Outlook to Gmail
- Consider the mail client & mail server that was used during analysis
- In case an unfamiliar mail header is encountered, use Google to understand what it does
- Headers that begin with **X-*** are added by software (e.g.: Mail Gateway, Mail Client, Mail Server, etc.)
- **ALWAYS** consider and understand the **CONTEXT**

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
X-Originating-IP: [54.89.76.235]
X-MS-Exchange-CrossTenant-AuthSource: HK0PR02MB3057
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27 Aug 2020 22:35:17.2632
(UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName: SbWdtj/YNwqtPcqvn7ry6eQvmq10FW7coJ7JFyItrNY6MNEbVezfa4vJ+BFzxlyoxVGzNxa+pI+GPLMH+mfaf+2horI9D3Vm
+mQNNQWBFPcolW8JpJ9d0Z2AONrPtoF
X-MS-Exchange-Transport-CrossTenantHeadersStamped: HK0PR02MB3057
```

PRE-ANALYSIS NOTES

Mail Headers can contain non-standard headers which vary depending on the mail server & mail client that the mail passed through

- An email from Gmail to Yahoo will have different headers than an email from Outlook to Gmail
- Consider the mail client & mail server that was used during analysis
- In case an unfamiliar mail header is encountered, use Google to understand what it does
- Headers that begin with **X-*** are added by software (e.g.: Mail Gateway, Mail Client, Mail Server, etc.)
- **ALWAYS** consider and understand the **CONTEXT**

OBSERVATIONS

X-MS-Exchange-CrossTenant-*

- Mail headers primarily used by Office 365

X-OriginatorOrg

- *****@***.edu.ph

X-Originating-IP

- 54.89.76.235

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-TrafficTypeDiagnostic: HK0PR02MB3057:
X-Microsoft-Antispam-PRVS:
<HK0PR02MB3057814CAF98268E3FB77DE493550@HK0PR02MB3057.apcprd02.prod.outlook.com>
X-MS-Exchange-Organization: OLM:7691;
X-MS-Exchange-SenderADCheck: 1
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:

wIih2oxFVx0uqyxCdFtPBRJ5i7Jq4eN4PBfv4X/hXfBxU9kvam7EUuuDXhXwB/II1+sRwT09UP2M7dPMU6XzuE0/Ux61oXL4t3vbay5nSAXKXmAX0LeRes9T5I81pn4nD6i8itPwKmm3I8vQ8HmbZ
+kuM3xDp69QaFY++Mt0tCfPcrRCrCFE3W7D/LSI8P/8V75fwmDF8dDjonYfUgoYhZ0chogyY02teKE+Q5eNczcT0peS
+/o/mhXYq1GQ1PT1BnYwEz1IfpG4vmEmemxVhEtza3s0c6HhcVZak2EiY9h52wngOLZr7epas020cF2d4BPNQAZuJfEIQgdB7DWLb/xZsm1wc+FgrLpeD05Jm476e9tDGodP3/ABRei3II
+Y0SQuEn4RD8Lc7Aymubzvb63kwyA0pWVh4DUtEGLVPEDCFE691k1GTEA740a3a6zmpWTq3M1U6vndTPRtT+G9v9/yK54gyY1a0D7DX7Jn5k0hzYckauKsGp5nuD680KM10YCRadBhvyEK10==
X-Forefront-Antispam-Report:
  CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:HK0PR02MB2865.apcprd02.prod.outlook.com;PTR:;CAT:NONE;SFS:(346002)(366004)(376002)
(396003)(136003)(39850400004)(6486002)(7116003)(316002)(786003)(8676002)(6916009)(9686003)(15974865002)(83080400001)(8936002)(15650500001)(5660300002)
(66574015)(83380400001)(33656002)(18074004)(2906002)(66946007)(186003)(33656001)(16526019)(166002)(26005)(3480700007)(86362001)(478600001)(33964004)(52116002)(956004)
(52536014)(6496006)(66476007)(66556008)(57042006);DIR:OUT;SFP:1102;
X-MS-Exchange-Organization:
  y0p3S1/opc
+LZ787KIyzKGVsuaasyORuywtrNyzPfQ8EXTL98dBtGzbt2xi0C7BDZ9khip99R/r2ivQ680ZevTsvy14yviDoxI/aRV2KjCi/3KHv6yDrr3vndRX4Ydtjm6lKygiuiB59j0fQcUvkvfekQdAYvB1VGwqnP6
mqZkhYR3HiYY/51CaYw7EPEp17o1695upvRKWYFgsjBvXLeFzLxhOM1apHahhM61VeBk0fk12sBRZB4CVDYKGT8DQej5eok1SGP+RLKJ10RHEQxrek4h+JJC1Dt8M2tX41vqi2nXCd7+86WpuN46AM
+WevnrR67B4DgwF8AqhwP80+vQfLfkQwYNS83k+rH0ILZyZmx7S1fQHdN6pNtbvRaiZ0Vj0WxvSkZQ+7r6N4V3tFjAte08v7vRfoHo0kv1i3u
+G9GeoZH20BBKrsudJZAVyiG1YCa0HyShsX7IDGVZCJNHH98bC3PwDl/y1AGur0MrRCgKudZzEJh8g0WboCvkwYA1jTGQ3VkyQ0ZYPSxyOk2fCy0ocFshiBgTrPyQkifDIVFhJe19hyAVsI6Tcq52QKpBwgCy
r1bN3N0oFJIrgoovFFdZ32qhuKfx+iR3v8NHH+EytTF3pyuhp5/cAPZo0UtUdeLmufQKfhs04s5X9A==
X-OriginatorOrg:
X-MS-Exchange-CrossTenant-Message-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-Exchange-CrossTenant-Network-Message-Id: bebf77b2-2746-4203-96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-AuthSource: HK0PR02MB2865.apcprd02.prod.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27 Aug 2020 22:35:17.2632
(UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName: SbWdtj/YNwqtPcqvn7ry6eQvmq10FW7coJ7JFyItrNY6MNEbVezfa4vJ+BFzxlyoxVGzNxa+pI+GPLMH+mfA+F2horI9D3Vm
+mQNNQWBFPcolW8JpJ9d0Z2AONrPtoF
X-MS-Exchange-Transport-CrossTenantHeadersStamped: HK0PR02MB3057
Content-Length: 19551
```

PRE-ANALYSIS NOTES

Mail Headers can contain non-standard headers which vary depending on the mail server & mail client that the mail passed through

- An email from Gmail to Yahoo will have different headers than an email from Outlook to Gmail
- Consider the mail client & mail server that was used during analysis
- In case an unfamiliar mail header is encountered, use Google to understand what it does
- Headers that begin with **X-*** are added by software (e.g.: Mail Gateway, Mail Client, Mail Server, etc.)
- **ALWAYS** consider and understand the **CONTEXT**

OBSERVATIONS

X-MS-Exchange-CrossTenant-*

- Mail headers primarily used by Office 365

X-OriginatorOrg

- *****@***.edu.ph

X-Originating-IP

- 54.89.76.235

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis



NOTES

contain non-standard headers
ing on the mail server & mail
passed through
mail to Yahoo will have different
email from Outlook to Gmail
client & mail server that was used

ilar mail header is encountered, use
and what it does
in with **X-*** are added by software
(e.g., Mail Client, Mail Server, etc.)
and understand the **CONTEXT**

ssTenant-*

primarily used by Office 365

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

The screenshot shows an email client interface. At the top, the article title is "Anti-spam message headers in Microsoft 365". Below the title, there is a date and time "01/22/2021 • 11 minutes to read" and several profile icons. A blue banner with an information icon and the word "Important" is present. The main text of the article reads: "The improved Microsoft 365 security center is now available in public preview. This new experience brings Defender for Endpoint, Defender for Office, 365 Microsoft 365 Defender, and more into the Microsoft 365 security center. Learn what's new. This topic might apply to both Microsoft Defender for Office 365 and Microsoft 365 Defender. Refer to the Applies To section and look for specific call outs in this article where there might be differences." Below this, a paragraph states: "In all Microsoft 365 organizations, Exchange Online Protection (EOP) scans all incoming messages for spam, malware, and other threats. The results of these scans are added to the following header fields in messages:" followed by a bulleted list of three headers: "X-Forefront-Antispam-Report", "X-Microsoft-Antispam", and "Authentication-results". The first item in the list is highlighted with a red box. The email client's status bar at the bottom shows "Windows (CRLF)", "Ln 101, Col 1", and "120%".

NOTES

contain non-standard headers
ing on the mail server & mail
passed through
mail to Yahoo will have different
email from Outlook to Gmail
client & mail server that was used

ilar mail header is encountered, use
t and what it does
in with **X-*** are added by software
(ay, Mail Client, Mail Server, etc.)
and understand the **CONTEXT**

ssTenant-*

primarily used by Office 365

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

Anti-spam message headers in Microsoft 365

01/22/2021 • 11 minutes to read

X-Forefront-Antispam-Report message header fields

Important

The improved Microsoft Endpoint, Defender for Cloud, and Microsoft Defender for Office 365. This topic might apply to you. and look for specific callouts.

In all Microsoft 365 organizations, there are many phishing threats. The results of these threats are listed below.

- X-Forefront-Antispam-Report**
- X-Microsoft-Antispam: Contains additional information about bulk mail and phishing.
- Authentication-results: Contains information about SPF, DKIM, and DMARC (email authentication) results.

Note

The X-Forefront-Antispam-Report header contains many different fields and values. Fields that aren't described in the table are used exclusively by the Microsoft anti-spam team for diagnostic purposes.

...CTRY:;LANG:hr;SCL:1;SRV:;IPV:NLI;SFV:NSPM;PTR:;CAT:NONE;SFTY:;...

The individual fields and values are described in the following table.

Windows (CRLF) | Ln 101, Col 1 | 120%

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

The screenshot displays an email header analysis interface. On the left, a sidebar lists various protection categories: **Anti-s**, **Importa**, **The improv**, **Endpoint, I**, **This topic**, **and look fo**, **In all Microsc**, **threats. The r**, **X-Foref**, **X-Micro**, and **Authen**. The main content area is titled "The category of protection policy, applied to the message:" and lists the following categories:

- **BULK**: Bulk
- **DIMP**: Domain Impersonation
- **GIMP**: Mailbox intelligence based impersonation
- **HPHSH** or **HPHISH**: High confidence phishing
- **HSPM**: High confidence spam
- **MALW**: Malware
- **PHSH**: Phishing
- **SPM**: Spam
- **SPOOF**: Spoofing
- **UIMP**: User Impersonation
- **AMP**: Anti-malware
- **SAP**: Safe attachments
- **OSPM**: Outbound spam

Below the list, a text block states: "An inbound message may be flagged by multiple forms of protection and multiple detection scans. Policies have different priorities, and the policy with the highest priority is applied first. For more information, see [What policy applies when multiple protection methods and detection scans run on your email.](#)"

The interface also shows filtering options:

- CIP**: [IP address] The connecting IP address. You can use this IP address in the IP Allow List or the IP Block List. For more information, see [Configure connection filtering.](#)
- CTRY** The source country as determined by the connecting IP address, which may not be the same as the originating sending IP address.

On the right side of the screenshot, there are partial views of other sections: "Standard headers", "Id and value", and "table are".



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-TrafficTypeDiagnostic: HK0PR02MB3057:
X-Microsoft-Antispam-PRVS:
<HK0PR02MB3057814CAF98268E3FB77DE493550@HK0PR02MB3057.apcprd02.prod.outlook.com>
X-MS-Exchange-Organization: OLM:7691;
X-MS-Exchange-SenderADCheck: 1
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:

wIih2oxFVxuqyxCdFtPBRJ5i7Jq4eN4PBfv4X/hXfBxU9kvam7EUuuDXhXwB/II1+sRwT09UP2M7dPMU6XzuE0/Ux61oXL4t3vbay5nSAXKXmAX0LeRes9T5I81pn4nD6i8itPwKmm3I8gvQ8HmbZ
+kuM3xDp69QaFY++Mt0tCfPcrRCfP3E3W7D/LSI8P/8V75fmmwDF8dDjonYfUgoYhZ0chogyY02teKE+Q5eNczcT0peS
+/o/mhXYq1GQ1PT1BnYwEz1IfpG4vmEmemxVhEtza3s0c6HhcVZak2EiY9h52wngOLZr7epas020cF2d4BPNQAZuJfEfqGD67DwLb/xZsm1wc+FgrLpeD05Jm476e9tDGodP3/ABRei3II
+AY0SQuEn4RD8Uc7Aymuhzvb63kwyA0pWVh4DUtEGLVPEDCFE691k1GTEA740a3a6zmpWTq3M1U6vndTPRtT+G9v9/yK54gyY1a0D7DX7Jn5k0hzYckauKsGp5nuD680KM10YCRadBhvyEK10==
X-Forefront-Antispam-Report:
  CIP:255.255.255.255;CTRY:;LANG:en;SCL:1;SRV:;IPV:NL;SFV:NSPM;H:HK0PR02MB2865.apcprd02.prod.outlook.com;PTR:;CAT:NONE;SFS:(346002)(366004)(376002)
(396003)(136003)(39850400004)(6486002)(7116003)(316002)(786003)(8676002)(6916009)(9686003)(15974865002)(83080400001)(8936002)(15650500001)(5660300002)
(66574015)(83380400001)(33656002)(18074004)(2906002)(66946007)(186003)(33656002)(16526019)(166002)(26005)(3480700007)(86362001)(478600001)(33964004)(52116002)(956004)
(52536014)(6496006)(66476007)(66556008)(57042006);DIR:OUT;SFP:1102;
X-MS-Exchange-Organization: y0p3S1/opc
+LZ787KIyzKGVsuasayORuywtrNyzPfQ8EXTL98dBtGzbt2xi0C7BDZ9khp199R/r2ivQ680ZevTsvy14yviDoxI/aRV2KjCi/3KHv6yDrr3vndRX4Ydtjm61KygiuiB59j0fQcUvkvfQdAYvB1VGwqnP6
mqZkhYR3HiYY/51CaYw7EPEp17o1695SupvRKWYFgsjBvXLeFzLxhOM1apHahhM61VeBk0fk12sBRZB4CVDYKGT8DQej5eok1SGP+RLKJ10RHEQxrek4h+JJC1Dt8M2tX41vqi2nXCd7+86WpuN46AM
+WevnrR67B4DGwF8AqhwP80+vQfLfkQwYNS83k+rH0ILZyZmx7S1fQHdN6pNtbvRaiZ0VjWxvSkZQ+7r6N4V3tFjAte08v7vRfoHo0kv1i3u
+G9GeoZH0BBKrsudJZAVyiG1YCa0HyShsX7IDGVCZJNHH98bC3PwDL/y1AGur0MrRCgKudZzEJh8g0WboCvkwYA1jTGQ3VkyQ0ZYPSxyOk2fCy0ocFshiBgTrPyQikfDIVFhJe19hyAVsI6Tcq52QKpBwgCy
r1bN3N0oFJIrgoovFFdZ32qhuKfx+iR3v8NHH+EytTF3pyuhp5/cAPZo0UtUdeLmufQKfhs04s5X9A==
X-OriginatorOrg: *****.***.edu.ph
X-MS-Exchange-CrossTenant-Message-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
X-MS-Exchange-CrossTenant-AuthSource: HK0PR02MB2865.apcprd02.prod.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Internal
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 27 Aug 2020 22:35:17.2632
(UTC)
X-MS-Exchange-CrossTenant-FromEntityHeader: Hosted
X-MS-Exchange-CrossTenant-Id: bebf77b2-2746-4203-96d7-17f29e16cb16
X-MS-Exchange-CrossTenant-MailboxType: HOSTED
X-MS-Exchange-CrossTenant-UserPrincipalName: SbWdtj/YNwqtPcqvn7ry6eQvmq10FW7coJ7JFyItrNY6MNEbVezfa4vJ+BFzlyoxVGzNxa+pI+GPLMH+mfa+F2horI9D3Vm
+mQNNQWBFPcoLw8JpJ9d0Z2A0NRPtoF
X-MS-Exchange-Transport-CrossTenantHeadersStamped: HK0PR02MB3057
Content-Length: 19551
```

PRE-ANALYSIS NOTES

Mail Headers can contain non-standard headers which vary depending on the mail server & mail client that the mail passed through

- An email from Gmail to Yahoo will have different headers than an email from Outlook to Gmail
- Consider the mail client & mail server that was used during analysis
- In case an unfamiliar mail header is encountered, use Google to understand what it does
- Headers that begin with **X-*** are added by software (e.g.: Mail Gateway, Mail Client, Mail Server, etc.)
- **ALWAYS** consider and understand the **CONTEXT**

OBSERVATIONS

X-MS-Exchange-CrossTenant-*

- Mail headers primarily used by Office 365

X-OriginatorOrg

- *****.***.edu.ph

X-Originating-IP

- 54.89.76.235

X-Forefront-Antispam-Report:

- **CIP:** 255.255.255.255
- **H:** HK0PR02MB2865.apcprd02.prod.outlook.com
- **PTR:** NULL
- **CAT:** NONE

CIP: Connecting IP Address

H: HELO/EHLO string of the connecting mail server

PTR: Reverse DNS lookup of the connecting IP Address

CAT: Category applied to the Message

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

OBSERVATIONS

```
Untitled - Notepad
File Edit Format View Help
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pA116B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphoETtDUKNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzAQ011t
+ns/1g/Y7y7ZxGN9epYHP3KWAL4MZUAWURVu913Pnfy+vY5JZXXrA7V03gwKQ4TNUMdW
+CcgFToRsb251TycHT2dex5tZ/h/5eGcGMD9bIH5t0igxSf/ytA8+yX9egTnXnrdKZ497UBP1nnMQBSBgCe9aj5tjpuK9voRzXJ/bxG85Dhe/IVgh10fbxhH7WFx032NfMA6LKjd7QeBqxMpHmv2C4BgFF1fu
z6Q==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass
smtp.mailfrom=[REDACTED].edu.ph; dmarc=pass action=none
header.from=[REDACTED].edu.ph; dkim=pass header.d=[REDACTED].edu.ph;
arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=tsueduph.onmicrosoft.com; s=selector2-tsueduph-onmicrosoft-com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=RzyjYmSzt1S5Yeb+wRfAJL+ubrD6K8DUneT8uwrwXSIQgPoXjEde0AxL1qSeywV1vrh61YXR7k5psNlMkCB3XV2qCBghv089Kyv08m0BgY4cvXPg3Q8TxYVIEIDPOEi
+LctCUyb03fXArUE42E1BTTD91kP89WSCb9N597rcIQj4=
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com (2603:1096:203:37::22)
by HK0PR02MB3057.apcprd02.prod.outlook.com (2603:1096:203:60::15) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3326.23; Thu, 27 Aug
2020 22:35:17 +0000
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551]) by HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551%3]) with mapi id 15.20.3326.019; Thu, 27 Aug 2020
22:35:17 +0000
From: "MetroBank" <r*****@[REDACTED].edu.ph>
To: m*****@yahoo.com
Date: 27 Aug 2020 22:35:16 +0000
Subject: New System Update
Content-Type: multipart/alternative;
boundary=-boundary_5207_32343822-bb55-489c-a2f2-1cb55229337b
X-ClientProxiedBy: MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) To HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
Message-ID:
<HK0PR02MB2865CA6172E4053B117B1CB493550@HK0PR02MB2865.apcprd02.prod.outlook.com>
MIME-Version: 1.0
X-MS-Exchange-MessageSentRepresentingType: 1
Received: from EC2AMAZ-59M1G4T (54.89.76.235) by MN2PR12CA0021.namprd12.prod.outlook.com (2603:10b6:208:a8::34) with Microsoft SMTP Server (version=TLS1_0,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id 15.20.3326.19 via Frontend Transport; Thu, 27 Aug 2020 22:35:16 +0000
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
Windows (CRLF) Ln 1, Col 1 120%
```

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pAl16B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphpoETtDUkNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzAQ011t
+ns/1g/Y7y7ZxGN9epYHP3KWAL4MZUAWURVu913Pnfy+vY5JZXXrA7V03gwKQ4TNUMdW
+CcgFToRsb251TycHT2dex5tZ/h/5eGcGMD9bIH5t0igxSf/ytA8+yX9egTnXnrdKZ497UBP1nnMQBSBgCe9aj5tjpuK9voRzXJ/bxG85Dhe/IVgh10fbxhH7WFx032NfMA6LKjd7QeBqxMpHmv2C4BgFF1fu
z6Q==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass
smtp.mailfrom=[REDACTED].edu.ph; dmarc=pass action=none
header.from=[REDACTED].edu.ph; dkim=pass header.d=[REDACTED].edu.ph;
arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=tsueduph.onmicrosoft.com; s=selector2-tsueduph-onmicrosoft-com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=RzyjYmSZt1S5eb+wRfAJL+ubrD6K8DUneT8uwrwXSIQgPoXjEDeOAxL1qSeywV1vrh61YXR7k5psNlMkCB3XV2qCBghv089Kyv08m0BgYcvXPg3Q8TxYVIEIDPOEi
+LctCUyb03FXArUE42E1BTTD91kP89WSCb9N597rcIQj4=
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com (2603:1096:203:37::22)
by HK0PR02MB3057.apcprd02.prod.outlook.com (2603:1096:203:60::15) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3326.23; Thu, 27 Aug
2020 22:35:17 +0000
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551]) by HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f5513]) with mapi id 15.20.3326.019; Thu, 27 Aug 2020
22:35:17 +0000
From: "MetroBank" <r*****@[REDACTED].edu.ph>
To: m*****@yahoo.com
Date: 27 Aug 2020 22:35:16 +0000
Subject: New System Update
Content-Type: multipart/alternative;
boundary="--boundary_5207_32343822-bb55-489c-a2f2-1cb55229337b
X-ClientProxiedBy: MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) To HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
Message-ID:
<HK0PR02MB2865CA6172E4053B117B1CB493550@HK0PR02MB2865.apcprd02.prod.outlook.com>
MIME-Version: 1.0
X-MS-Exchange-Message-Auth-AsynchronousType: 1
Received: from EC2AMAZ-59M1G4T (54.89.76.235) by MN2PR12CA0021.namprd12.prod.outlook.com (2603:10b6:208:a8::34) with Microsoft SMTP Server (version=TLS1_0,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id 15.20.3326.19 via Frontend Transport; Thu, 27 Aug 2020 22:35:16 +0000
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
Windows (CRLF) Ln 1, Col 1 120%
```

OBSERVATIONS

Received

- from EC2AMAZ-59M1G4T (54.89.76.235)
- Thu, 27 Aug 2020 22:35:16 +0000

From

- Name: "MetroBank"
- Email: <r*****@*****.***.edu.ph>

To

- m*****@yahoo.com

Date

- 27 Aug 2020 22:35:16 +0000

Subject

- New System Update

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pA116B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphpoETtDUkNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzAQ011t
+ns/1g/Y7y7ZxGN9epY
+CcgFToRsb251TycHT2
z6Q==
ARC-Authentication-
smtp.mailfrom=
header.from=
arc=none
DKIM-Signature: v=1
d=tsueduph.onmicr
h=From:Date:Subjec
bh=YpPL3001iR7SNx0
b=RzyjYmSZt1SYeb+w
+LctCUyb03FXArUE42E
Received: from HK0P
by HK0PR02MB3057.a
Microsoft SMTP Ser
cipher=TLS_ECDHE_R
2020 22:35:17 +000
Received: from HK0P
([fe80::2804:771c:
([fe80::2804:771c:
22:35:17+0000
From: "MetroBank" <
To: m*****@
Date: 27 Aug 2020 2
Subject: New System
Content-Type: multi
boundary=--boundar
X-ClientProxiedBy:
(2603:10b6:208:a8:
(2603:1096:203:37:
Message-ID:
<HK0PR02MB2865CA61
MIME-Version: 1.0
X-MS-Exchange-Message-
Received: from EC2A
cipher=TLS_ECDHE_RS
X-Originating-IP: [
X-MS-PublicTraffic
X-MS-Office365-Filt
Windows (CRLF) Ln 1, Col 1 120%
```

OBSERVATIONS

Received

- from EC2AMAZ-59M1G4T (54.89.76.235)

Time Zone Converter – Time Difference Calculator

Provides time zone conversions taking into account Daylight Saving Time (DST), local time zone and accepts present, past, or future dates.

Sort By: -- Custom --

UTC, Time Zone (UTC +0)	Thu, 27 Aug 2020	22:35		
Manila, Philippines PHST (UTC +8)	Fri, 28 Aug 2020	06:35		

+ Add another city or time zone...

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Summary of Findings (Email Header Analysis)

Facts

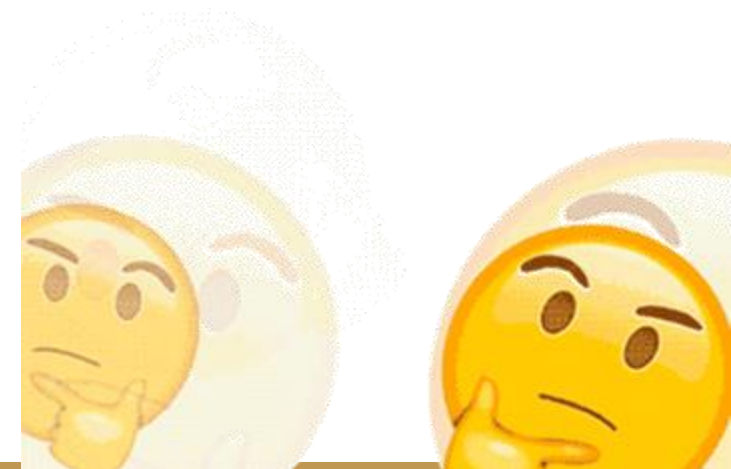
1. The malicious mail came from an Office 365 tenant
2. The originating host is *****.***.edu.ph
3. The originating IP address is 54.89.76.235
4. The malicious mail was **NOT** categorized by Office 365
5. The malicious mail was delivered to the recipient at exactly 27 Aug 2020 22:35:16 +0000

Presumptions

1. N/A

Timeline of Events

1. 08-28-2020 at 6:35 AM UTC +8 (Malicious mail delivered)



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
File Edit Format View Help
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pAl16B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphoETtDUkNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzAQ011t
+ns/1g/Y7y7ZxGN9epYHP3KWAL4MZUAWURVu913Pnfy+vY5JZXXrA7V03gwKQ4TNUMdW
+CcgFToRsb251TycHT2dex5tZ/h/5eGcGMD9bIH5t0igxSf/ytA8+yX9egTnXnrdKZ497UBP1nnMQBSBgCe9aj5tjpuK9v0RzXJ/bxG85Dhe/IVgh10fbxhH7WFx032NfMA6LKjd7QeBqxMpHmv2C4BgFF1fu
760--
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass
smtp.mailfrom=[REDACTED].edu.ph; dmarc=pass action=none
header.from=[REDACTED].edu.ph; dkim=pass header.d=[REDACTED].edu.ph;
arc=none
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=tsueduph.onmicrosoft.com; s=selector2-tsueduph-onmicrosoft-com;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWpSx0Fpw=;
b=RzyjYmSzt1S5eb+wRfAJL+ubrD6K8DUneT8uwrwxSIQgPoXjEde0AxL1qSeywV1vrh61YXR7k5psNlMkCB3XV2qCBghv089Kyv08m0BgY4cYvXPg3Q8TxYVIEIDPOEi
+LctCUyb03FXArUE42E1BTDD91kP89WSCb9N597rcIQj4=
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com (2603:10b6:208:a8::34)
by HK0PR02MB3057.apcprd02.prod.outlook.com (2603:1096:203:60::15) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3326.23; Thu, 27 Aug
2020 22:35:17 +0000
Received: from HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551]) by HK0PR02MB2865.apcprd02.prod.outlook.com
([fe80::2804:771c:f26c:f551%3]) with mapi id 15.20.3326.019; Thu, 27 Aug 2020
22:35:17 +0000
From: "MetroBank" <[REDACTED]@[REDACTED].edu.ph>
To: m*****@yahoo.com
Date: 27 Aug 2020 22:35:16 +0000
Subject: New System Update
Content-Type: multipart/alternative;
boundary=-boundary_5207_32343822-bb55-489c-a2f2-1cb55229337b
X-ClientProxiedBy: MN2PR12CA0021.namprd12.prod.outlook.com
(2603:10b6:208:a8::34) To HK0PR02MB2865.apcprd02.prod.outlook.com
(2603:1096:203:37::22)
Message-ID:
<HK0PR02MB2865CA6172E4053B117B1CB493550@HK0PR02MB2865.apcprd02.prod.outlook.com>
MIME-Version: 1.0
X-MS-Exchange-MessageSentRepresentingType: 1
Received: from EC2AMAZ-59M1G4T (54.89.76.235) by MN2PR12CA0021.namprd12.prod.outlook.com (2603:10b6:208:a8::34) with Microsoft SMTP Server (version=TLS1_0,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id 15.20.3326.19 via Frontend Transport; Thu, 27 Aug 2020 22:35:16 +0000
X-Originating-IP: [54.89.76.235]
X-MS-PublicTrafficType: Email
X-MS-Office365-Filtering-Correlation-Id: fbf2ca38-fd55-436b-d4d9-08d84ad978d7
Windows (CRLF) Ln 1, Col 1 120%
```

OBSERVATIONS

ARC-Authentication-Results

- smtp.mailfrom=*****.[REDACTED].edu.ph
- dmarc=pass action=none
- header.from=*****.[REDACTED].edu.ph
- dkim=pass header.d=*****.[REDACTED].edu.ph
- arc=none

DKIM-Signature

- d=***eduph.onmicrosoft.com
- s=selector2-***eduph.onmicrosoft.com

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Internet Engineering Task Force (IETF)
Request for Comments: 8617
Category: Experimental
ISSN: 2070-1721

K. Andersen
LinkedIn
B. Long, Ed.
Google
S. Blank, Ed.
Valimail
M. Kucherawy, Ed.
TDP
July 2019

The Authenticated Received Chain (ARC) Protocol

Abstract

The Authenticated Received Chain (ARC) protocol provides an
authenticated "chain of custody" for a message, allowing each entity
that handles the message to see what entities handled it before and
what the message's authentication assessment was at each step in the
handling.

ARC allows Internet Mail Handlers to attach assertions of message
authentication assessment to individual messages. As messages
traverse ARC-enabled Internet Mail Handlers, additional ARC
assertions can be attached to messages to form ordered sets of ARC
assertions that represent the authentication assessment at each step
of the message-handling paths.

ARC-enabled Internet Mail Handlers can process sets of ARC assertions
to inform message disposition decisions, identify Internet Mail
Handlers that might break existing authentication mechanisms, and
convey original authentication assessments across trust boundaries.
```

OBSERVATIONS

ARC-Authentication-Results

- smtp.mailfrom=*****@***.edu.ph
- dmarc=pass action=none
- header.from=*****@***.edu.ph
- dkim=pass header.d=*****@***.edu.ph
- arc=none

DKIM-Signature

- d=***@eduph.onmicrosoft.com
- s=selector2-***@eduph.onmicrosoft.com

easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
Received: from 10.253.62.152
by atlas106.free.mail.gq1.yahoo.com with HTTP; Thu, 27 Aug 2020 22:35:20 +0000
Return-Path: <r*****@*****.edu.ph>
Received: from 40.107.131.129 (EHLO APC01-SG2-obe.outbound.protection.outlook.com)
by 10.253.62.152 with SMTPs; Thu, 27 Aug 2020 22:35:20 +0000
X-Originating-Ip: [40.107.131.129]
Received-SPF: pass (domain of *****.edu.ph designates 40.107.131.129 as permitted sender)
Authentication-Results: atlas106.free.mail.gq1.yahoo.com;
dkim=pass header.i=@*****.eduph.onmicrosoft.com header.s=selector2-*****.eduph-onmicrosoft-com;
spf=pass smtp.mailfrom=*****.edu.ph;
dmarc=unknown
X-Apparently-To: m*****@yahoo.com; Thu, 27 Aug 2020 22:35:20 +0000
X-MS-Exchange-Organization: *****
X-Q5jcDXsUsQhUKCySYGNL9VQMDhNEUUDUyACaFxaaIyMUr6nrhqwWl0wzGe
aObMqBkff95PDbcPtj_n5FEKKI4K705Vz_qJCYF1TT3gp36_G14AWfQIBY1Y
o5wRCS5sTHmccHsSq4IuZqJfe_t9WQ6RvA6i56D1Qep1e777E.C11LtF1f9
AnSwQY8kvI6VHCYT1vwKa86sWqxQ_IA5_I50xJ_BppCffrDC288md.or7j0_
MizbrxNV457vM0txbs53BUoywC9VXDNIuYCCpZvpCqBhs8WrIwazt0W9dJQC
xMC9sPPFknCR7Jn_e2NRBeCi7kz9AsgPLOI.U28EVGGp3EtHQ1_IU2UPC_a
5ZAx_WGWr54XhNDRPOx3hY9uCMckxi8wv7hwzmkC80rVQWArI.OXqPKRKzy
SvzPh2hi5Q1G3R1hbSA0e0nAYNsG2jAMBjP_RAC7cpoghtCVCBb1TEdE.Jwc
XTwYN1T7LMRLMbyIq2tPbK2nSdy7fghMjFInzykIMrZEytcFOF07JMd9jYZ
.3qihbg_EfuulFqn5tfdSrb00vju7m7Qg1FiYqQ26uUAHI94m6tM27jWSP
8anwRmA_4RAwPqth6R2BYP3xBjvY809se2vsKojzViJfQEHTErZ0AyUg91bB
8h3Sj39.JdVGOIR7r1NICze9BbC6UT9AK8a22huBH90xwBrI1NB6FXIYZcZF
vQldVksVfndz2pg1YZMXhC7_nXpHC9oPQByRj6Gj.9DAs_8Fa9IsHYH3iPg
faKePbX0LgmbkDQXNT0VbiPhfXxkGzfpFbYtjHhaJvuFqUqmb10qWmXNfhr1
h_Oy5rgxmkc23h7ktNJDY0WjKAAGawjoV0fksLsYGIuzGQoJdFpwi0Hxfea.
owu4n6NDDqLcMRGmRdyzBDV_EtNGvFWYz8zuTSPXe1Rf28Q957VEzQ8alfnx
TrAbZN50WuwuQuDfgJTHpKQOXfXAf2KwDqsKAVfQDF7Y7z1p2btD.ZFSBSYb
4a5VutyF4jUrZVxIvouA2a00GYBdRau7pFSna0A1uTnZXMcdb.dX7wbmBF1M
EsKQub.iVdievgn6kr_kkaw4tFZ3GuVKcF9ge1gBPuv0JKR1_OCixY.Q1Fr
JZW12J3sFu0iwmblfYYkdc4rr5TWwms7BH2HEJRFcKt2cF27dM5r7
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;
b=RRMeC660NNWqY/yPinRsh6ZVgXg3/pTP24fYCYHOI9fd0Lb9ys6NUE19/WU6NUbV0Uis2zDKE3QkE7Rro/W008wniQ911RCCR
+drFZVdb84B2HcW0s4Qx7a1u7IM0y09AIfv3wjT1TmOgqJRF8A0beT0zKjxT5vZH9Q4+XpXqk00gePete57SGBmVbzHxQN0NInz9QoVB0RG/n2wu4a
+DwQHxf/f/1IMPtd1u6j9K75m8Mi01ssN0g0k2mncnVf0sQIPaul31y7r642n8z0Nu06Pm9z1C6byBHMv16biKIrneiFAQrTY+Vf/IGHm55BgpUawtE+F12y+cVHUxOg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
s=arcselector9901;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWp5Xofpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pA116B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphpoETtDUKNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzA0Q11t
```

OBSERVATIONS

ARC-Authentication-Results

- smtp.mailfrom=*****.edu.ph
- dmarc=pass action=none
- header.from=*****.edu.ph
- dkim=pass header.d=*****.edu.ph
- arc=none

DKIM-Signature

- d=**eduph.onmicrosoft.com
- s=selector2-***eduph.onmicrosoft.com

X-Apparently-To

- m*****@yahoo.com

Authentication-Results

- dkim=pass
- spf=pass
- dmarc=unknown

Received-SPF

- Pass (*****.edu.ph designates 40.107.131.129 as permitted sender)

X-Originating-Ip

- 40.107.131.129

Reply-To

- r*****@*****.edu.ph

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis

Anti-spam message headers in Microsoft 365

01/22/2021 • 11 minutes to read • [Profile Icons] +15

Important

The improved [Microsoft 365 security center](#) is now available in public preview. This new experience brings Defender for Endpoint, Defender for Office, 365 Microsoft 365 Defender, and more into the Microsoft 365 security center. [Learn what's new.](#) This topic might apply to both Microsoft Defender for Office 365 and Microsoft 365 Defender. Refer to the **Applies To** section and look for specific call outs in this article where there might be differences.

In all Microsoft 365 organizations, Exchange Online Protection (EOP) scans all incoming messages for spam, malware, and other threats. The results of these scans are added to the following header fields in messages:

- **X-Forefront-Antispam-Report:** Contains information about the message and about how it was processed.
- **X-Microsoft-Antispam:** Contains additional information about bulk mail and phishing.
- **Authentication-results:** Contains information about SPF, DKIM, and DMARC (email authentication) results.

Windows (CRLF) Ln 59, Col 20 120%

results
*****@***.edu.ph
on=None
*****@***.edu.ph
r.d=*****@***.edu.ph

microsoft.com
uph.onmicrosoft.com

phoo.com

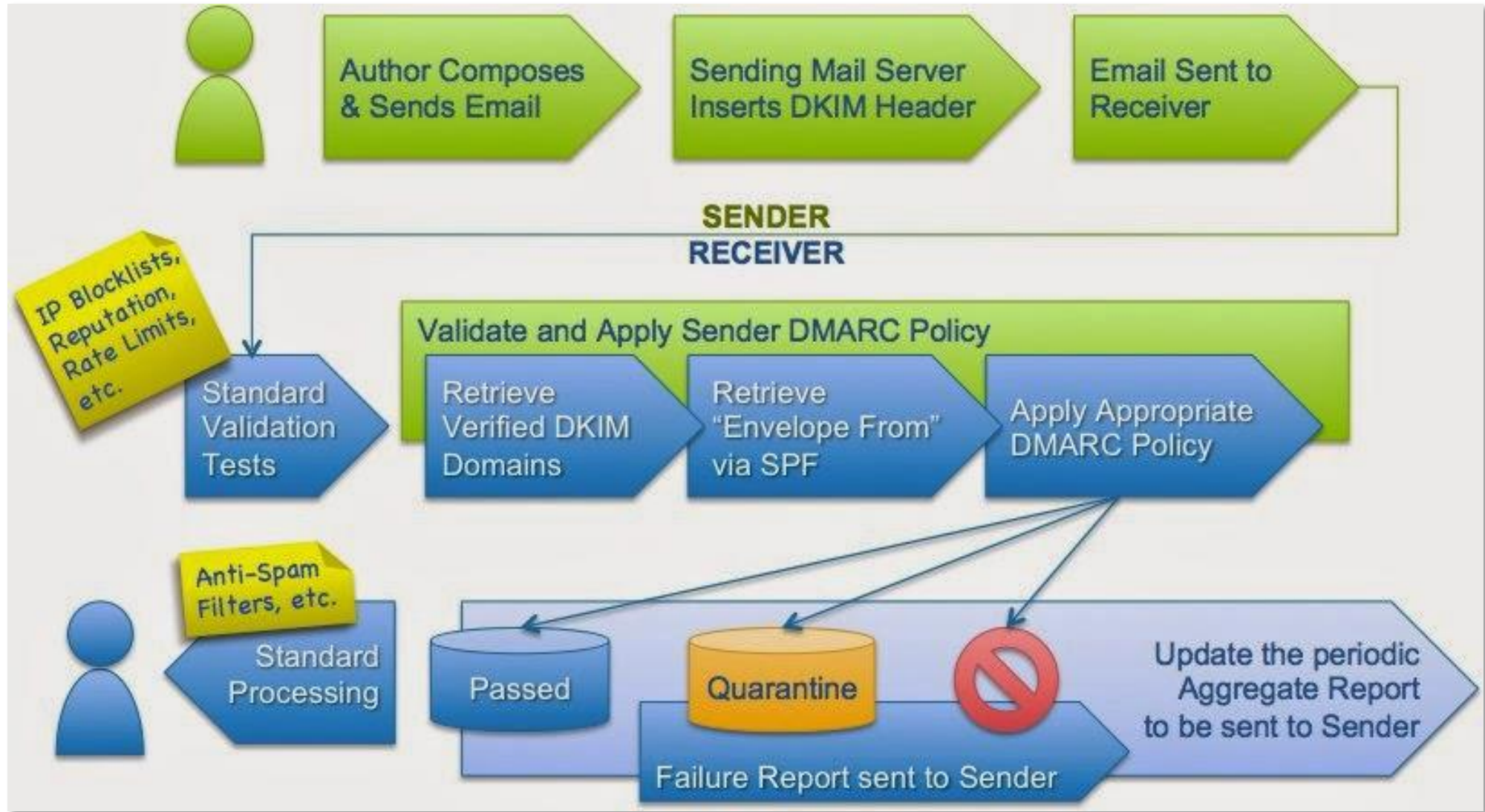
du.ph designates 40.107.131.129 as
)

*****@***.edu.ph

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Email Header Analysis



Reference: <https://www.endpoint.com/blog/2014/04/15/spf-dkim-and-dmarc-brief-explanation>

Complexity of Phishing – Email Header Analysis

```
Untitled - Notepad
Received: from 10.253.62.152
by atlas106.free.mail.gq1.yahoo.com with HTTP; Thu, 27 Aug 2020 22:35:20 +0000
Return-Path: <r*****@*****.edu.ph>
Received: from 40.107.131.129 (EHLO APC01-SG2-obe.outbound.protection.outlook.com)
by 10.253.62.152 with SMTPs; Thu, 27 Aug 2020 22:35:20 +0000
X-Originating-Ip: [40.107.131.129]
Received-SPF: pass (domain of *****.edu.ph designates 40.107.131.129 as permitted sender)
Authentication-Results: atlas106.free.mail.gq1.yahoo.com;
dkim=pass header.i=@*****.eduph.onmicrosoft.com header.s=selector2-*****.eduph-onmicrosoft-com;
spf=pass smtp.mailfrom=*****.edu.ph;
dmarc=unknown
X-Apparently-To: m*****@yahoo.com; Thu, 27 Aug 2020 22:35:20 +0000
X-MS-Exchange-Organization: *****
X-Q5jcDXsUsQhUKCySYGNL9VQMDhNEUUDUyACaFxaaIyMUr6nrhqwW10wzGe
aObMqBkff95PDbcPtj_n5FEKKI4K705Vz_qJCYF1TT3gp36_G14AwfQIBY1Y
o5wRCS5sTHmccHsSq4IuZqJfe_t9WQ6RvA6i56D1Qep1e777E.C11LtF1f9
AnSwQY8kvI6VHCYT1vwKa86sWqxQ_IA5_I50xJ_BppCffrDC288md.or7j0_
MizbrxNV457vM0txbs53BUoywC9VXDNIuYCCpZvpCqBhs8WrIwazt0W9dJQC
xMC9sPPFknCR7Jn_e2NRBeCi7kz9AsgPLOI.U28EVGGp3EtHQ1_IU2UPC_a
5ZAx_WGWr54XhNDRPOx3hY9uCMCKxi8wv7hwzmkC80rVQWArI.OXqPKRKzy
SvzPh2hi5Q1G3R1hbSA0e0nAYNsG2jAMBjP_RAC7cpoghtCVCBb1TEdE.Jwc
XTwYN1T7LMRLMbyIq2tPbK2nSdy7fghMjFInzykIMrZEytcFOF07JMd9jYZ
.3qihbg_EfuulFqn5tfdSrb00vju7m7Qg1FiYqQ26uUAHI94m6tM27jWSP
8anwRmA_4RAwPqth6R2BYP3xBjvY809se2vsKojzViJfQEHTErZ0AyUg91bB
8h3Sj39.JdVGOIR7r1NICze9BbC6UT9AK8a22huBH90xwBrI1NB6FXIYZcZF
vQldVksVfndz2pg1YZMXhC7_nXpHC9oPQByRj6Gj.9DAs_8Fa9IsHYH3iPg
faKePbX0LgmbkDQXNT0VbiPhfXxkGzfpFbYtjHhaJvuFqUqmb10qWmXNfhr1
h_Oy5rgxmkc23h7ktNJDY0WjKAAGawjoV0fksLsYGIuzGQoJdFpwi0Hxfea.
owu4n6NDDqLcMRGmRdyzBDV_EtNGvFWYz8zuTSPXe1Rf28Q957VEzQ8alfnx
TrAbZN50WuwuQuDfgJTHpKQOXfXAf2KwDqsKAVfQDF7Y7z1p2btD.ZFSBSYb
4a5VutyF4jUrZVxIvouA2a00GYBdRau7pFSna0A1uTnZXMcdb.dX7wbmBF1M
EsKQqb.iVdievgn6kr_kkaw4tFZ3GuVKcF9ge1gBPuv0JKR1_OCiXY.Q1Fr
JZW12J3sFu0iwMblfYYkdc4rr5TWwms7BH2HEJRFcKt2cF27dM5r7
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;
b=RRMeC660NNWqY/yPinRsh6ZVgXg3/pTP24fYCYHOI9fd0Lb9ys6NUE19/WU6NUbV0Uis2zDKE3QkE7Rro/W008wniQ911RCCR
+drFZVdb84B2HcW0s4Qx7a1u7IM0y09AIfv3wjT1TmOgqJRF8A0beT0zKjxT5vZH9Q4+XpXqk00gePete57SGBmVbzHxQNONInz9QoVB0RG/n2wu4a
+DwQHxf/f/1IMPtd1u6j9K75m8Mi01ssN0g0k2mncnVf0sQIPaul31y7r642n8z0Nu06Pm9ziC6byBHMv16biKIrneiFAQrTY+Vf/IGHm55BgpUawtE+Fl2y+cVHUxOg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
s=arcselector9901;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
bh=YpPL3001iR7SNx01kr1nY1txa5GzdSef0ocWp5Xofpw=;
b=H5WdTRdULUMRgE5Ru+/VeE240c3pA116B4sqApCu2IEsc9U81Jf+ZcVfCm122xhLphpoETtDUKNaD/haByLV0kGqENPI6tUgcrpF5kDQmuUzA0Q11t
```

OBSERVATIONS

ARC-Authentication-Results

- smtp.mailfrom=*****.edu.ph
- dmarc=pass action=none
- header.from=*****.edu.ph
- dkim=pass header.d=*****.edu.ph
- arc=none

DKIM-Signature

- d=**eduph.onmicrosoft.com
- s=selector2-***eduph.onmicrosoft.com

X-Apparently-To

- m*****@yahoo.com

Authentication-Results

- dkim=pass
- spf=pass
- dmarc=unknown

Received-SPF

- Pass (*****.edu.ph designates 40.107.131.129 as permitted sender)

X-Originating-Ip

- 40.107.131.129

Reply-To

- r*****@*****.edu.ph

Easiest way to analyze is by reading the headers bottom-up



Complexity of Phishing – Summary of Findings (Email Header Analysis)

Facts

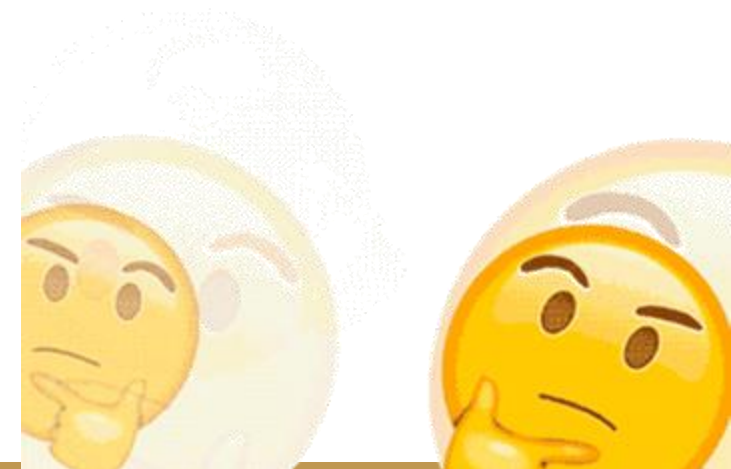
1. The malicious mail came from an Office 365 tenant
2. The originating host is *****.***.edu.ph
3. The originating IP address is 54.89.76.235
4. The malicious mail was **NOT** categorized by Office 365
5. The malicious mail was delivered to the recipient at exactly 27 Aug 2020 22:35:16 +0000
6. The malicious mail **passed** all 3 standard security protocol checks (SPF, DKIM, DMARC)
7. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph

Presumptions

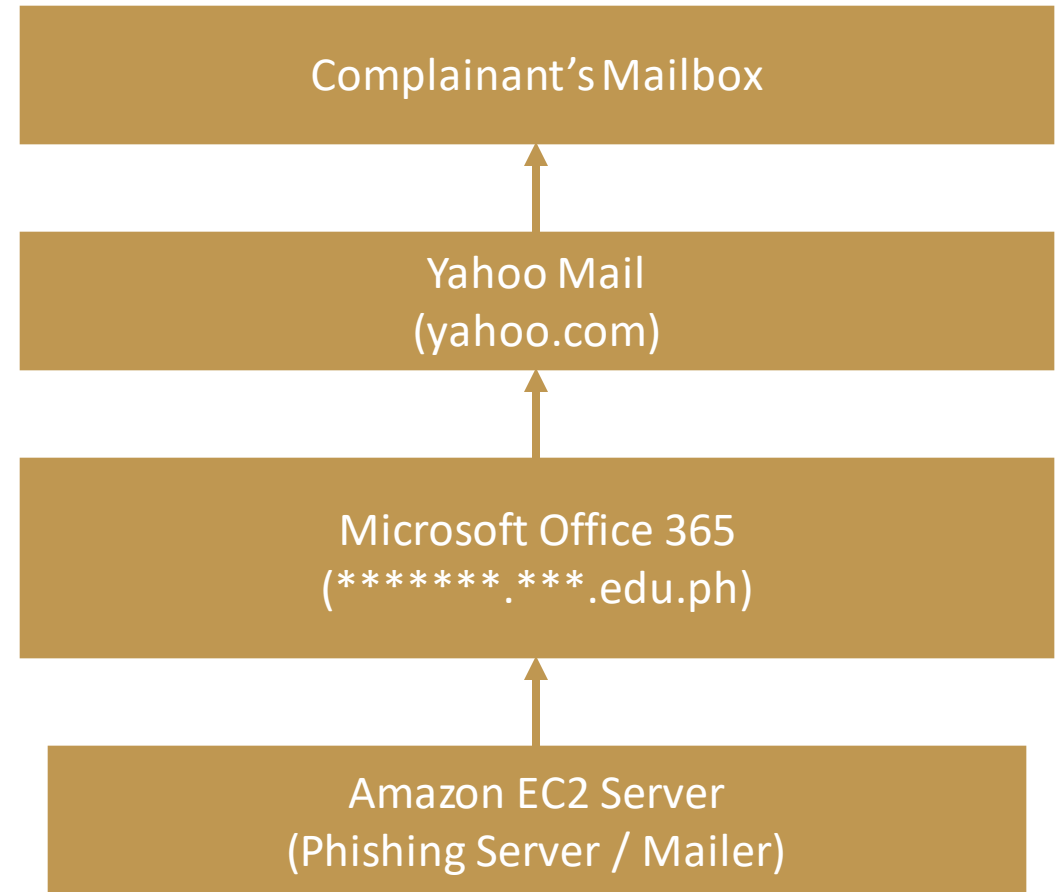
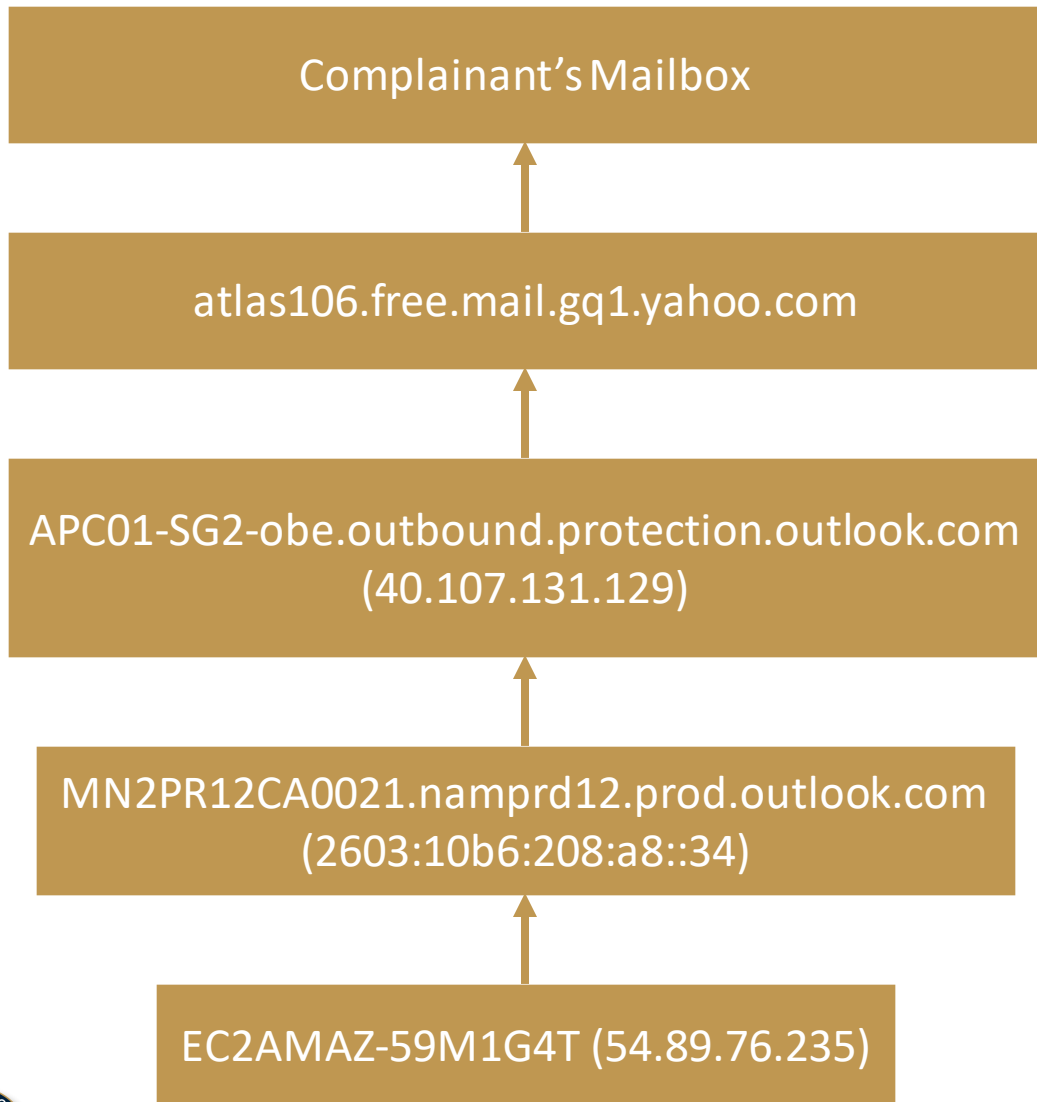
1. N/A

Timeline of Events

1. 08-28-2020 at 6:35 AM UTC +8 (Malicious mail delivered)



Complexity of Phishing – Mail Flow



Complexity of Phishing – Summary of Findings (Email Content Analysis)

Facts

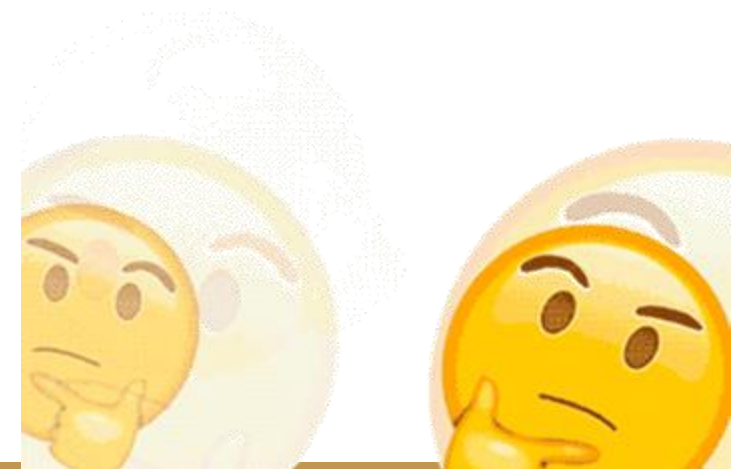
1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. **08-28-2020 at 6:35 AM UTC +8 (Malicious mail delivered)**
2. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)



Complexity of Phishing – Social Media Analysis

28 August 2020 · [Profile]

Hello po Good afternoon po Sa inyong Lahat.

Sana Lahat po ng mga nasend po ng Email About po sa Metrobank update from this Email r. [Profile]@ [Profile].edu.ph HINDI po ako yung nag send ng email o phishing email. Nagamit po yung student account chineck ko po dun sa mga history po ng login kanina pong 3AM po ng umaga.

Hindi ko po magagawang mag send ng email or phishing email sa mga tao.Opo IT student po ako pero hindi ko po magagawa o gamitin ang computer knowledge ko sa masama lalo na po sa ganung bagay.

Sent Items

From	Subject	Date
jrdinglasan@yahoo.com	New System Update	Thu 7:32 PM
lee_gervacio@yahoo.com	New System Update	Thu 7:32 PM
cooishakebeets@yahoo.com	New System Update	Thu 7:31 PM
marynakyama@yahoo.com	New System Update	Thu 7:31 PM
agreyes123@yahoo.com	New System Update	Thu 7:31 PM
kraguino5555@yahoo.com	New System Update	Thu 7:31 PM
en_upa@yahoo.com	New System Update	Thu 7:31 PM

New System Update

To: sarahbeth_c@yahoo.com

Metrobank Update

Dear Valued Client,

Our system has detected some error to your transaction.

If this was you, kindly disregard this message. Otherwise, please proceed to verification.

You can verify your account at <https://personal.metrobankdirect.com/>

These communication channels are available to you 24 hours a day, 7 days a week.

Thank you for banking online with us!

The MetroBank Banking Team

Important: Please save this message for future reference

Metrobank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 8768-1000 and email address customerservice@metrobank.com.ph

Metrobank, Inc. © 2020. All Rights Reserved.

Today at 9:45:11 AM +08 Ha Noi, VN Office 365 Exchange Online ✓ Successful sign-in

Today at 4:24:06 AM +08 Astrakhanskaya Oblast', RU Office 365 Exchange Online ✓ Successful sign-in

Today at 3:24:34 AM +08 Tirane, AL Office 365 Exchange Online ✓ Successful sign-in

Location Tirane, AL

IP [What is this?](#) 79.106.5.53

App Office 365 Exchange Online

Account [Profile]@student.tsu.edu.ph

Look unfamiliar? Secure your account

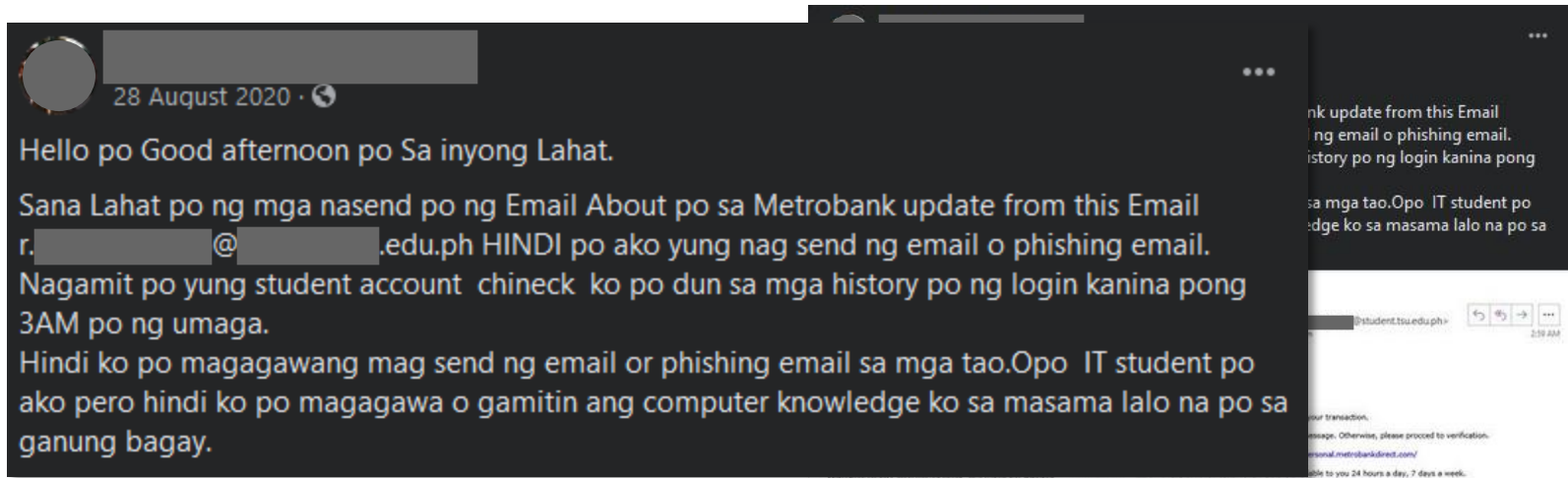
Today at 2:09:52 AM +08 Al Qahirah, EG Office 365 ✓ Successful sign-in

Today at 2:09:49 AM +08 Al Qahirah, EG Office 365 Exchange Online ✓ Successful sign-in

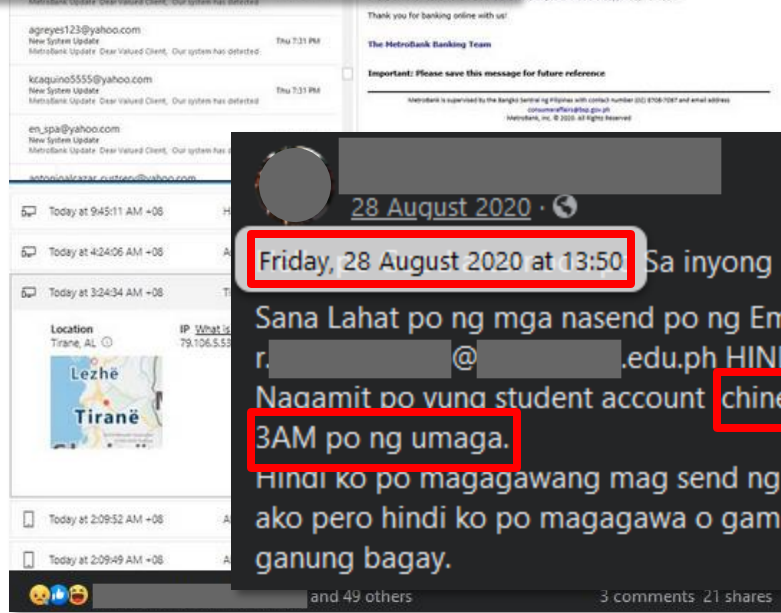
and 49 others 3 comments 21 shares



Complexity of Phishing – Social Media Analysis



A screenshot of a Facebook post from August 28, 2020. The post is in Tagalog and discusses a phishing email from Metrobank. The text reads: "Hello po Good afternoon po Sa inyong Lahat. Sana Lahat po ng mga nasend po ng Email About po sa Metrobank update from this Email r. [redacted]@ [redacted].edu.ph HINDI po ako yung nag send ng email o phishing email. Nagamit po yung student account chineck ko po dun sa mga history po ng login kanina pong 3AM po ng umaga. Hindi ko po magagawang mag send ng email or phishing email sa mga tao.Opo IT student po ako pero hindi ko po magagawa o gamitin ang computer knowledge ko sa masama lalo na po sa ganung bagay." The post includes a small image of a Metrobank system update email and a map of Tiranë, Albania.



This block contains two screenshots. The top one shows an email from Metrobank with the subject "New System Update" and the body text: "Metrobank Update: Dear Valued Client, Our system has detected...". The bottom screenshot shows a Facebook post from August 28, 2020, at 13:50. The text of the post is: "Sa inyong Lahat. Sana Lahat po ng mga nasend po ng Email About po sa Metrobank update from this Email r. [redacted]@ [redacted].edu.ph HINDI po ako vuna naa send na email o phishing email. Nagamit po vuna student account chineck ko po dun sa mga history po ng login kanina pong 3AM po ng umaga. Hindi ko po magagawang mag send ng email or phishing email sa mga tao.Opo IT student po ako pero hindi ko po magagawa o gamitin ang computer knowledge ko sa masama lalo na po sa ganung bagay." The post has 3 comments and 21 shares.



Complexity of Phishing – Summary of Findings (Email Content & Social Media Analysis)

Facts

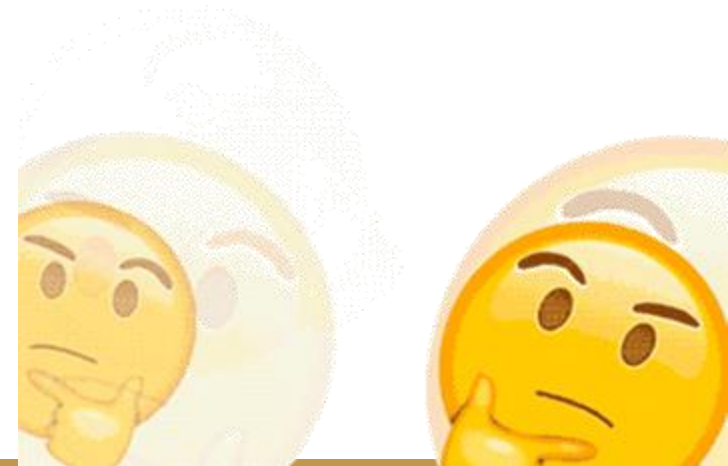
1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. **08-28-2020 at ~3:00 AM UTC +8 (The defendant checked their student mail)**
2. **08-28-2020 at 6:35 AM UTC+8 (Malicious mail delivered to complainant)**
3. **08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)**
4. **08-28-2020 at 1:50 PM UTC+8 (Facebook post by the defendant)**



Complexity of Phishing – Social Media Analysis

The screenshot shows an email inbox on the left and a selected phishing email on the right. The inbox lists several emails from 'jrdinglasan@yahoo.com' to 'antonioalcazar_custserv@yahoo.com', all with the subject 'New System Update' and the body 'MetroBank Update Dear Valued Client, Our system has detected'. The selected email is from 'R [redacted] <r.[redacted]@[redacted].edu.ph>' to 'sarahbeth_c@yahoo.com' at 2:59 AM. The body of the phishing email reads: 'MetroBank Update', 'Dear Valued Client,', 'Our system has detected some error to your transaction.', 'If this was you, kindly this regard this message. Otherwise, please procced to verification.', 'You can verify your account at <https://personal.metrobankdirect.com/>', 'These communication channels are available to you 24 hours a day, 7 days a week.', 'Thank you for banking online with us!', 'The MetroBank Banking Team', and 'Important: Please save this message for future reference'. At the bottom, it states 'MetroBank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 8708-7087 and email address consumeraffairs@bsp.gov.ph MetroBank, inc. © 2020. All Rights Reserved'.

From	Subject	Time
jrdinglasan@yahoo.com	New System Update	Thu 7:32 PM
lee_gervacio@yahoo.com	New System Update	Thu 7:32 PM
coolshakebeets@yahoo.com	New System Update	Thu 7:31 PM
marlynnakayama@yahoo.com	New System Update	Thu 7:31 PM
agreyes123@yahoo.com	New System Update	Thu 7:31 PM
kcaquino5555@yahoo.com	New System Update	Thu 7:31 PM
en_spa@yahoo.com	New System Update	Thu 7:31 PM
antonioalcazar_custserv@yahoo.com	New System Update	Thu 7:31 PM

New System Update

R [redacted] <r.[redacted]@[redacted].edu.ph>
To sarahbeth_c@yahoo.com 2:59 AM

MetroBank Update

Dear **Valued Client**,

Our system has detected some error to your transaction.

If this was you, kindly this regard this message. Otherwise, please procced to verification.

You can verify your account at <https://personal.metrobankdirect.com/>

These communication channels are available to you 24 hours a day, 7 days a week.

Thank you for banking online with us!

The MetroBank Banking Team

Important: Please save this message for future reference

MetroBank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 8708-7087 and email address consumeraffairs@bsp.gov.ph
MetroBank, inc. © 2020. All Rights Reserved



Complexity of Phishing – Social Media Analysis

Sent Items By Date ↑

Sender	Subject	Time
jrdinglasan@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:32 PM
lee_gervacio@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:32 PM
coolshakebeets@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM
marlynnakayama@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM
agreyes123@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM
kcaquino5555@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM
en_spa@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM
antonioalcazar_custserv@yahoo.com	New System Update MetroBank Update Dear Valued Client, Our system has detected	Thu 7:31 PM

New System Update

R [redacted] <r.[redacted]@[redacted].edu.ph>
To sarahbeth_c@yahoo.com 2:59 AM

MetroBank Update

Dear **Valued Client**,

Our system has detected some error to your transaction.

If this was you, kindly this regard this message. Otherwise, please procced to verification.

You can verify your account at <https://personal.metrobankdirect.com/>

These communication channels are available to you 24 hours a day, 7 days a week.

Thank you for banking online with us!

The MetroBank Banking Team

Important: Please save this message for future reference

MetroBank is supervised by the Bangko Sentral ng Pilipinas with contact number (02) 8708-7087 and email address consumeraffairs@bsp.gov.ph
MetroBank, Inc. © 2020. All Rights Reserved



Complexity of Phishing – Summary of Findings (Email Content & Social Media Analysis)

Facts

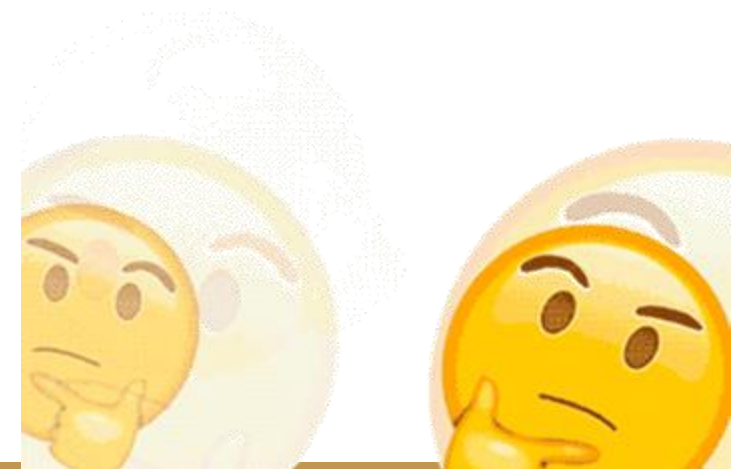
1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions


1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. **08-27-2020 at 7:31 PM UTC +8 (Phishing Email sent to multiple recipients)**
2. **08-28-2020 at 2:59 AM UTC +8 (Phishing Email sent to “sarahbeth_c@yahoo.com”)**
3. 08-28-2020 at ~3:00 AM UTC +8 (The defendant checked their student mail)
4. **08-28-2020 at 6:35 AM UTC+8 (Malicious mail delivered to complainant)**
5. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)
6. 08-28-2020 at 1:50 PM UTC+8 (Facebook post by the defendant)



Complexity of Phishing – Social Media Analysis

Today at 9:45:11 AM +08	Ha Noi, VN ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▼
Today at 4:24:06 AM +08	Astrakhanskaya Oblast', RU ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▼
Today at 3:24:34 AM +08	Tirane, AL ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▲
Location Tirane, AL ⓘ				
IP What is this? 79.106.5.53				
App Office 365 Exchange Online				
Account r.██████████@██████████.edu.ph				
				
Look unfamiliar? Secure your account				
Today at 2:09:52 AM +08	Al Qahirah, EG ⓘ	Office 365	✓ Successful sign-in	▼
Today at 2:09:49 AM +08	Al Qahirah, EG ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▼
Today at 2:09:44 AM +08	Al Qahirah, EG ⓘ	O365 Suite UX	✓ Successful sign-in	▼
Yesterday at 9:56:48 PM +08	Val-De-Marne, FR ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▼
Yesterday at 9:50:11 PM +08	Rio De Janeiro, BR ⓘ	Office 365 Exchange Online	✓ Successful sign-in	▼



Complexity of Phishing – Summary of Findings (Email Content & Social Media Analysis)

Facts

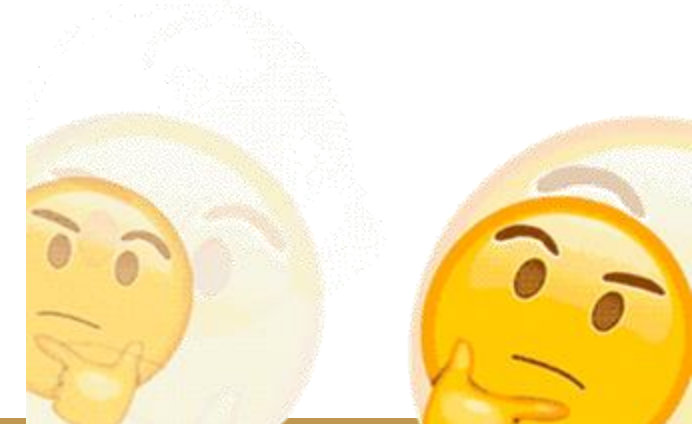
1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator


Timeline of Events

1. 08-27-2020 at 7:31 PM UTC +8 (Phishing Email sent to multiple recipients)
2. 08-27-2020 at 9:50 PM UTC +8 (Suspicious login to defendant's student email from Brazil)
3. 08-27-2020 at 9:56 PM UTC +8 (Suspicious login to defendant's student email from France)
4. 08-28-2020 at 2:09 AM UTC +8 (Suspicious login to defendant's student email from Egypt)
5. 08-28-2020 at 2:59 AM UTC +8 (Phishing Email sent to "sarahbeth_c@yahoo.com")
6. 08-28-2020 at ~3:00 AM UTC +8 (The defendant checked their student mail)
7. 08-28-2020 at 3:24 AM UTC +8 (Suspicious login to defendant's student email from Albania)
8. 08-28-2020 at 4:24 AM UTC +8 (Suspicious login to defendant's student email from Russia)
9. 08-28-2020 at 6:35 AM UTC +8 UTC+8 (Malicious mail delivered to complainant)
10. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)
11. 08-28-2020 at 9:45 AM UTC +8 (Suspicious login to defendant's student email from Vietnam)
12. 08-28-2020 at 1:50 PM UTC+8 (Facebook post by the defendant)



Complexity of Phishing – Social Media Analysis


R [redacted]
Hello po sir M [redacted]
Hindi po ako yung nag send ng email po sainyo
Hindi ko po magagawa yung bagay na po yon chineck ko po history of devices ko po na nag online o nag bukas ng school account ko po ... See more



Like · Reply · 21 w

→ A Arshinov Makhno replied · 28 replies

R [redacted]
Hello po sir M [redacted]
Hindi po ako yung nag send ng email po sainyo
Hindi ko po magagawa yung bagay na po yon chineck ko po history of devices ko po na nag online o nag bukas ng school account ko po ... See more



Like · Reply · 21 w

Friday, 28 August 2020 at 13:19 replied · 28 replies



Complexity of Phishing – Social Media Analysis

The screenshot displays the 'My Sign-Ins' page in a web browser. The page lists recent sign-in activities with columns for time, location, app, and account status. Two sets of logins are highlighted with red boxes:

Time	Location	App	Status
Today at 12:00:34 PM +08	Pangasinan, PH	Microsoft Forms	Successful sign-in
Today at 9:45:11 AM +08	Ha Noi, VN	Office 365 Exchange Online	Successful sign-in
Today at 4:24:06 AM +08	Astrakhanskaya Oblast', RU	Office 365 Exchange Online	Successful sign-in
Today at 3:24:34 AM +08	Tirane, AL	Office 365 Exchange Online	Successful sign-in
Today at 2:09:52 AM +08	Al Qahirah, EG	Office 365	Successful sign-in
Today at 2:09:49 AM +08	Al Qahirah, EG	Office 365 Exchange Online	Successful sign-in
Today at 2:09:44 AM +08	Al Qahirah, EG	O365 Suite UX	Successful sign-in
Yesterday at 9:56:48 PM +08	Vai-De-Marne, FR	Office 365 Exchange Online	Successful sign-in

The location details for the highlighted logins include a map of Tirane, AL, and a link to 'Look unfamiliar? Secure your account'. A video call window titled 'Meeting in "General"' is visible on the right, showing a participant with a crown. The system tray at the bottom right shows the time as 1:19 PM.



Complexity of Phishing – Summary of Findings (Email Content & Social Media Analysis)

Facts

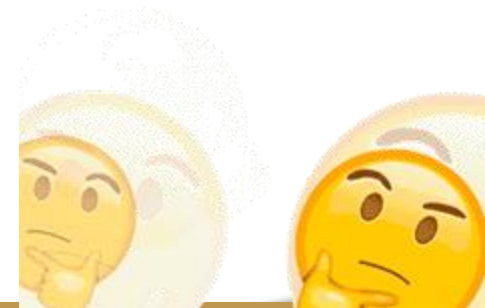
1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

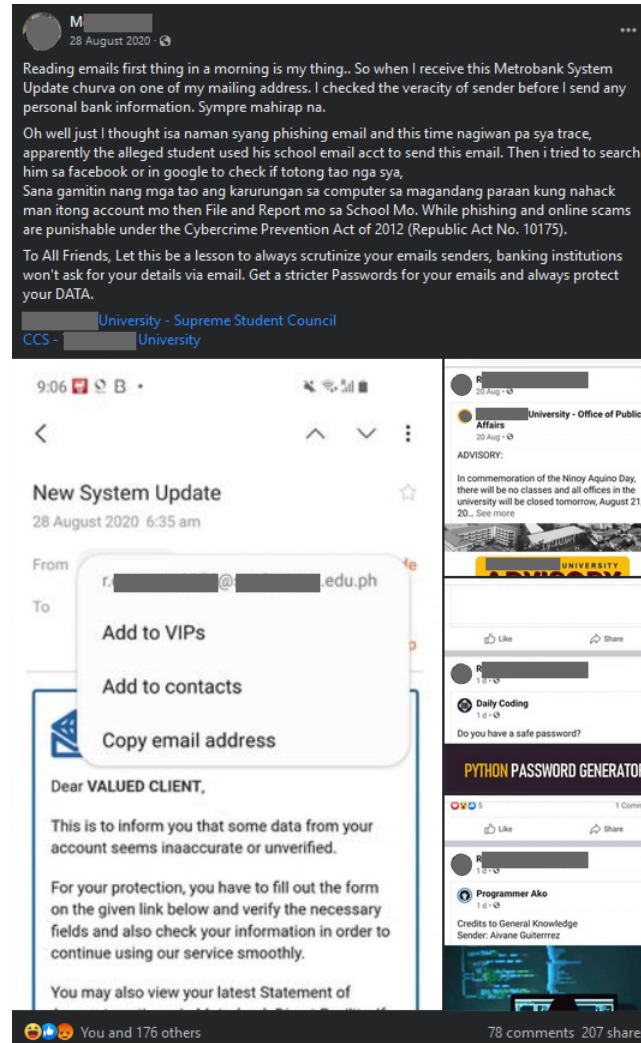
1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. 08-27-2020 at 7:31 PM UTC +8 (Phishing Email sent to multiple recipients)
2. 08-27-2020 at 9:50 PM UTC +8 (Suspicious login to defendant's student email from Brazil)
3. 08-27-2020 at 9:56 PM UTC +8 (Suspicious login to defendant's student email from France)
4. 08-28-2020 at 2:09 AM UTC +8 (Suspicious login to defendant's student email from Egypt)
5. 08-28-2020 at 2:59 AM UTC +8 (Phishing Email sent to "sarahbeth_c@yahoo.com")
6. 08-28-2020 at ~3:00 AM UTC +8 (The defendant checked their student mail)
7. 08-28-2020 at 3:24 AM UTC +8 (Suspicious login to defendant's student email from Albania)
8. 08-28-2020 at 4:24 AM UTC +8 (Suspicious login to defendant's student email from Russia)
9. 08-28-2020 at 6:35 AM UTC+8 (Malicious mail delivered to complainant)
10. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)
11. 08-28-2020 at 9:45 AM UTC +8 (Suspicious login to defendant's student email from Vietnam)
12. **08-28-2020 at 12:00 NN UTC +8 (Login to defendant's student email from Philippines)**
13. **08-28-2020 at 1:19 PM UTC+8 (Facebook comment by the defendant to complainant's post)**
14. 08-28-2020 at 1:50 PM UTC+8 (Facebook post by the defendant)



Complexity of Phishing – Social Media Analysis



Complexity of Phishing – Social Media Analysis

M [redacted]
28 August 2020 · 🌐

Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagihan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if totong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

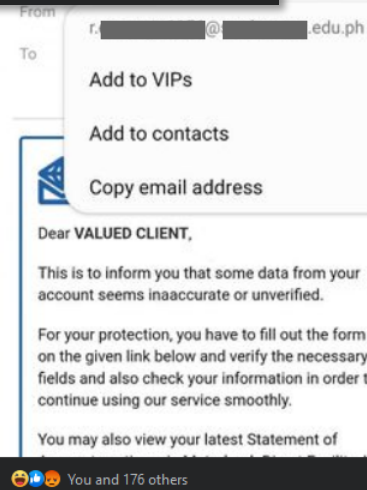
To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.

ny thing.. So when I receive this Metrobank System
ss. I checked the veracity of sender before I send any
p na.

shing email and this time nagihan pa sya trace,
ool email acct to send this email. Then i tried to search
itong tao nga sya,
in sa computer sa magandang paraan kung nahack
rt mo sa School Mo. While phishing and online scams
ention Act of 2012 (Republic Act No. 10175).

s scrutinize your emails senders, banking institutions
tricter Passwords for your emails and always protect

ouncil



M [redacted]
28 August 2020 · 🌐

Friday, 28 August 2020 at 09:36

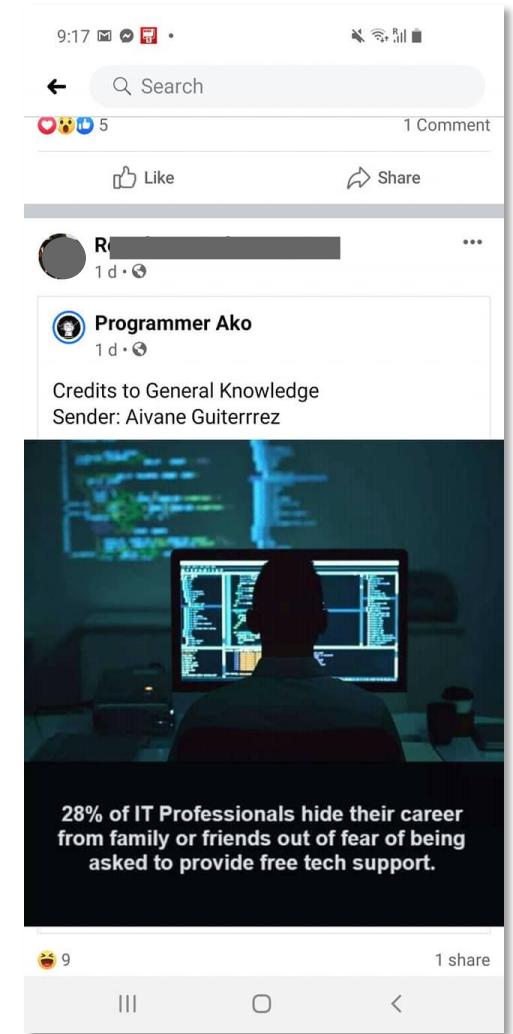
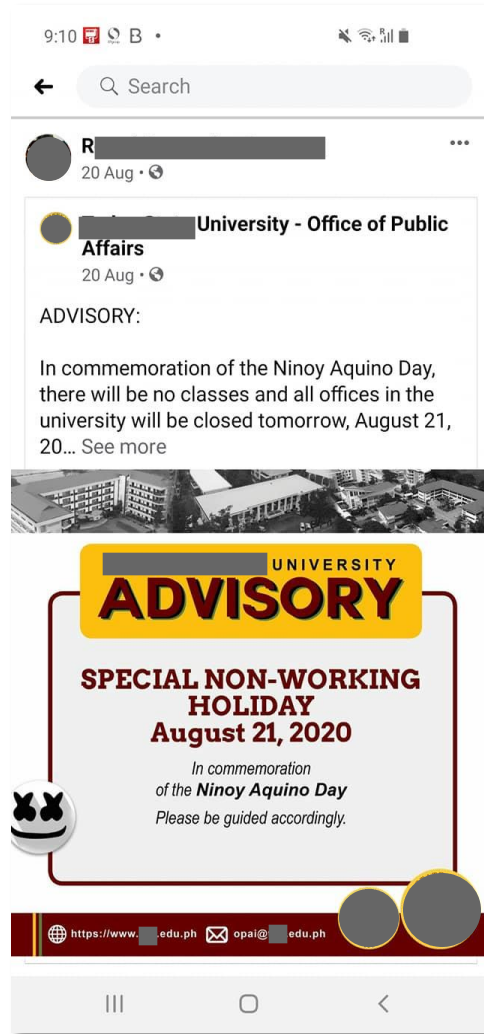
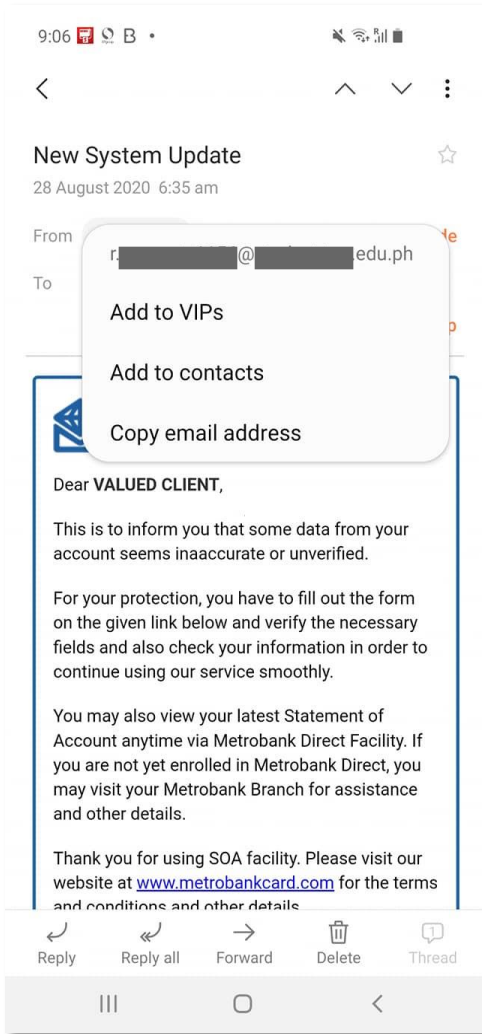
Reading emails first thing in a morning is my thing.. So when I receive this Metrobank System Update churva on one of my mailing address. I checked the veracity of sender before I send any personal bank information. Sympre mahirap na.

Oh well just I thought isa naman syang phishing email and this time nagihan pa sya trace, apparently the alleged student used his school email acct to send this email. Then i tried to search him sa facebook or in google to check if totong tao nga sya, Sana gamitin nang mga tao ang karunungan sa computer sa magandang paraan kung nahack man itong account mo then File and Report mo sa School Mo. While phishing and online scams are punishable under the Cybercrime Prevention Act of 2012 (Republic Act No. 10175).

To All Friends, Let this be a lesson to always scrutinize your emails senders, banking institutions won't ask for your details via email. Get a stricter Passwords for your emails and always protect your DATA.



Complexity of Phishing – Social Media Analysis



Complexity of Phishing – Summary of Findings (Email Content & Social Media Analysis)

Facts

1. The malicious mail came from r*****@*****.***.edu.ph who is a **user** from *****.***.edu.ph
2. The mail was delivered on **Friday, August 28, 2020 at 6:35 AM UTC+8**
3. The received mail is **malicious** in nature
 - It intends to **deceive** recipients that the email came from **Metrobank**
 - It entices the recipients to **click** on **“VERIFY MY ACCOUNT”** which contains a **concealed malicious link**
4. The domain donewellinsurance.com was used in this phishing campaign
5. A change was made to the directory <https://donewellinsurance.com/Administrator/js/> on **Friday, August 28, 2020 at 8:03 AM UTC+8**

Presumptions

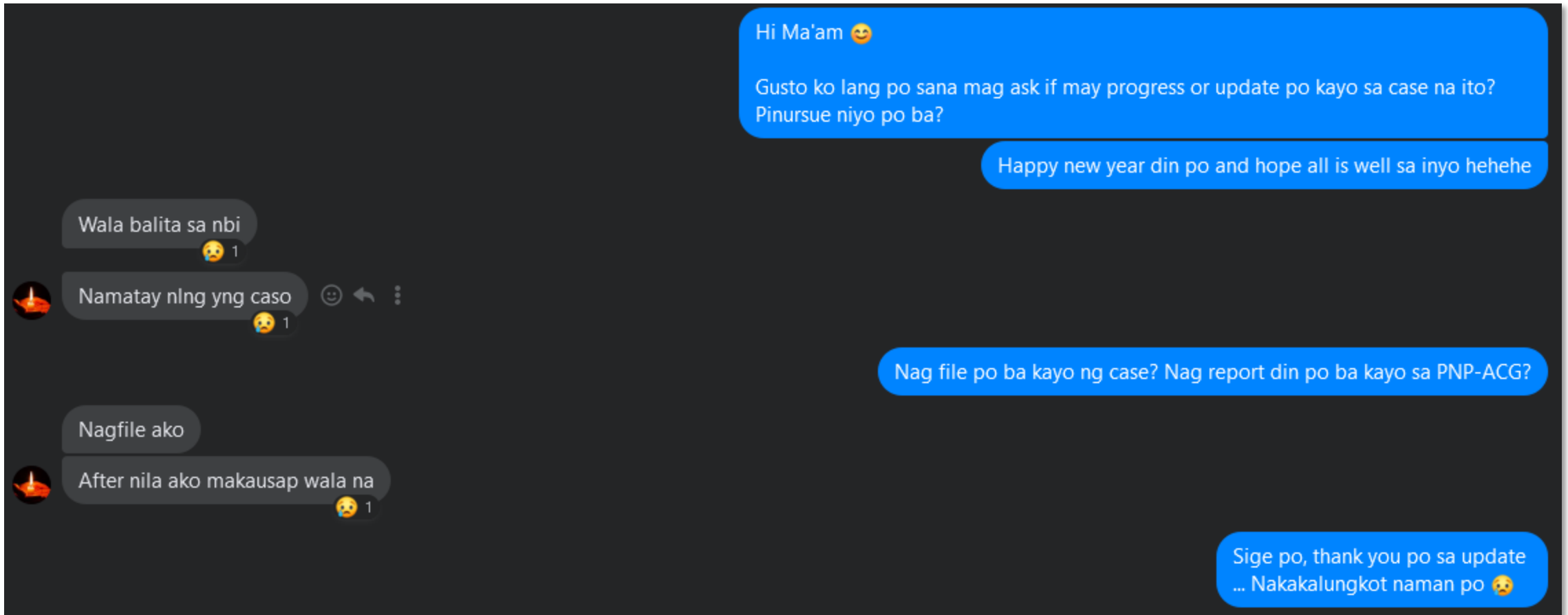
1. A threat actor compromised the domain donewellinsurance.com
2. Possible point of entry / mode of compromise
 - Exploitation of a remote information disclosure vulnerability (CVE-2010-2333)
 - Identified Administrator / Default Credentials
 - Login through the Admin Panel as Administrator

Timeline of Events

1. 08-27-2020 at 7:31 PM UTC +8 (Phishing Email sent to multiple recipients)
2. 08-27-2020 at 9:50 PM UTC +8 (Suspicious login to defendant's student email from Brazil)
3. 08-27-2020 at 9:56 PM UTC +8 (Suspicious login to defendant's student email from France)
4. 08-28-2020 at 2:09 AM UTC +8 (Suspicious login to defendant's student email from Egypt)
5. 08-28-2020 at 2:59 AM UTC +8 (Phishing Email sent to "sarahbeth_c@yahoo.com")
6. **08-28-2020 at ~3:00 AM UTC +8 (The defendant checked their student mail)**
7. 08-28-2020 at 3:24 AM UTC +8 (Suspicious login to defendant's student email from Albania)
8. 08-28-2020 at 4:24 AM UTC +8 (Suspicious login to defendant's student email from Russia)
9. **08-28-2020 at 6:35 AM UTC+8 (Malicious mail delivered to complainant)**
10. 08-28-2020 at 8:03 AM UTC +8 (Modification on <https://donewellinsurance.com/Administrator/js/>)
11. **08-28-2020 at 9:36 AM UTC +8 (Facebook post by the complainant)**
12. 08-28-2020 at 9:45 AM UTC +8 (Suspicious login to defendant's student email from Vietnam)
13. **08-28-2020 at 12:00 NN UTC +8 (Login to defendant's student email from Philippines)**
14. **08-28-2020 at 1:19 PM UTC +8 (Facebook comment by the defendant to complainant's post)**
15. **08-28-2020 at 1:50 PM UTC+8 (Facebook post by the defendant)**

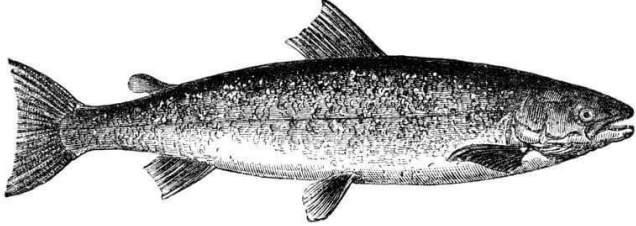


Complexity of Phishing – Current Status



Reality of our Current Situation

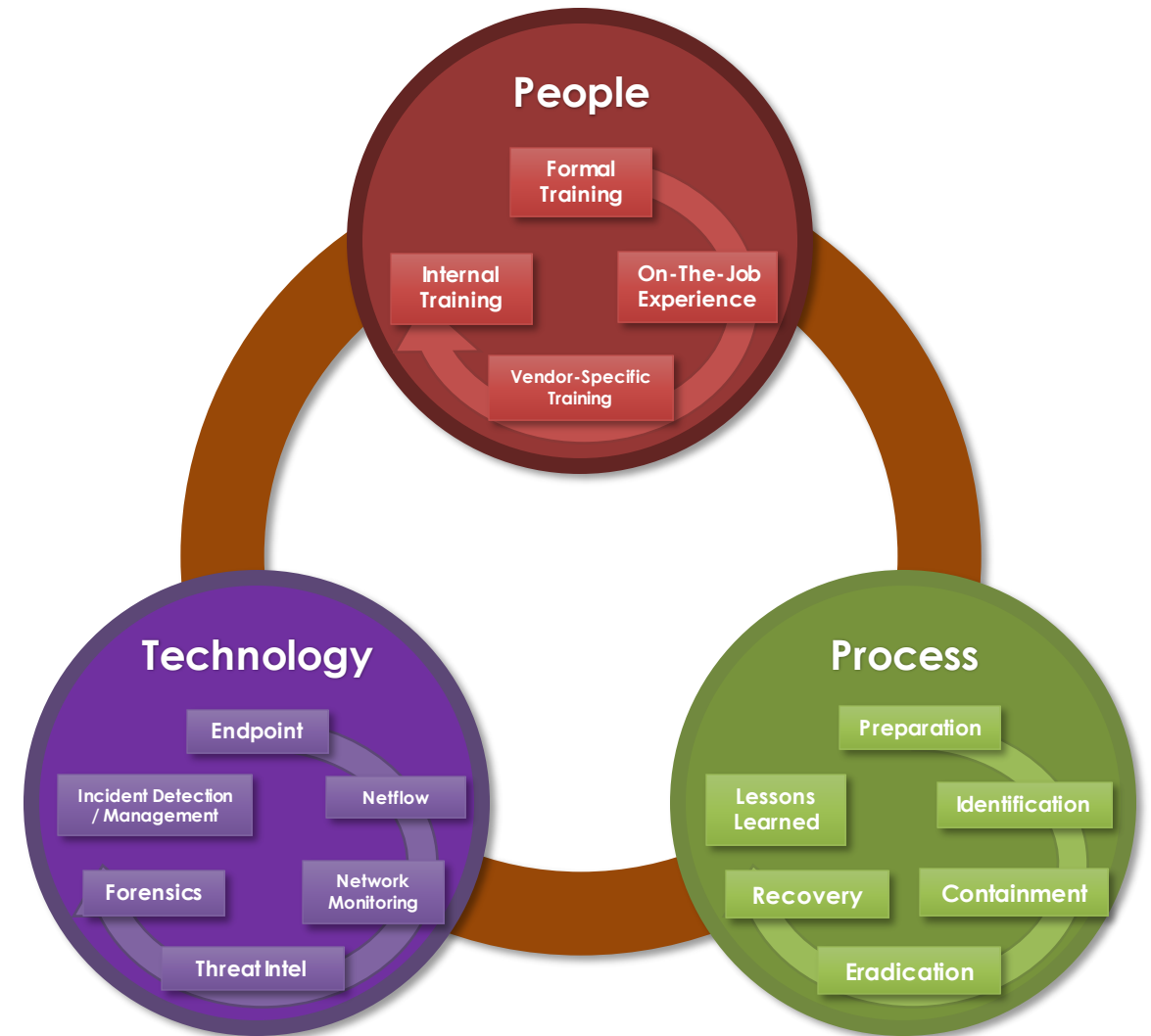
Security by optimism and prayer



Expert

Hoping Nobody Hacks You

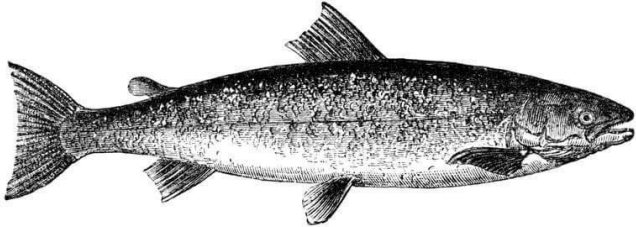
ORLY? @ThePracticalDev



Reference: <https://sibertor.com/wp-content/uploads/2016/07/building-world-class-security-operations-center-roadmap-35907.pdf>

Reality of our Current Situation

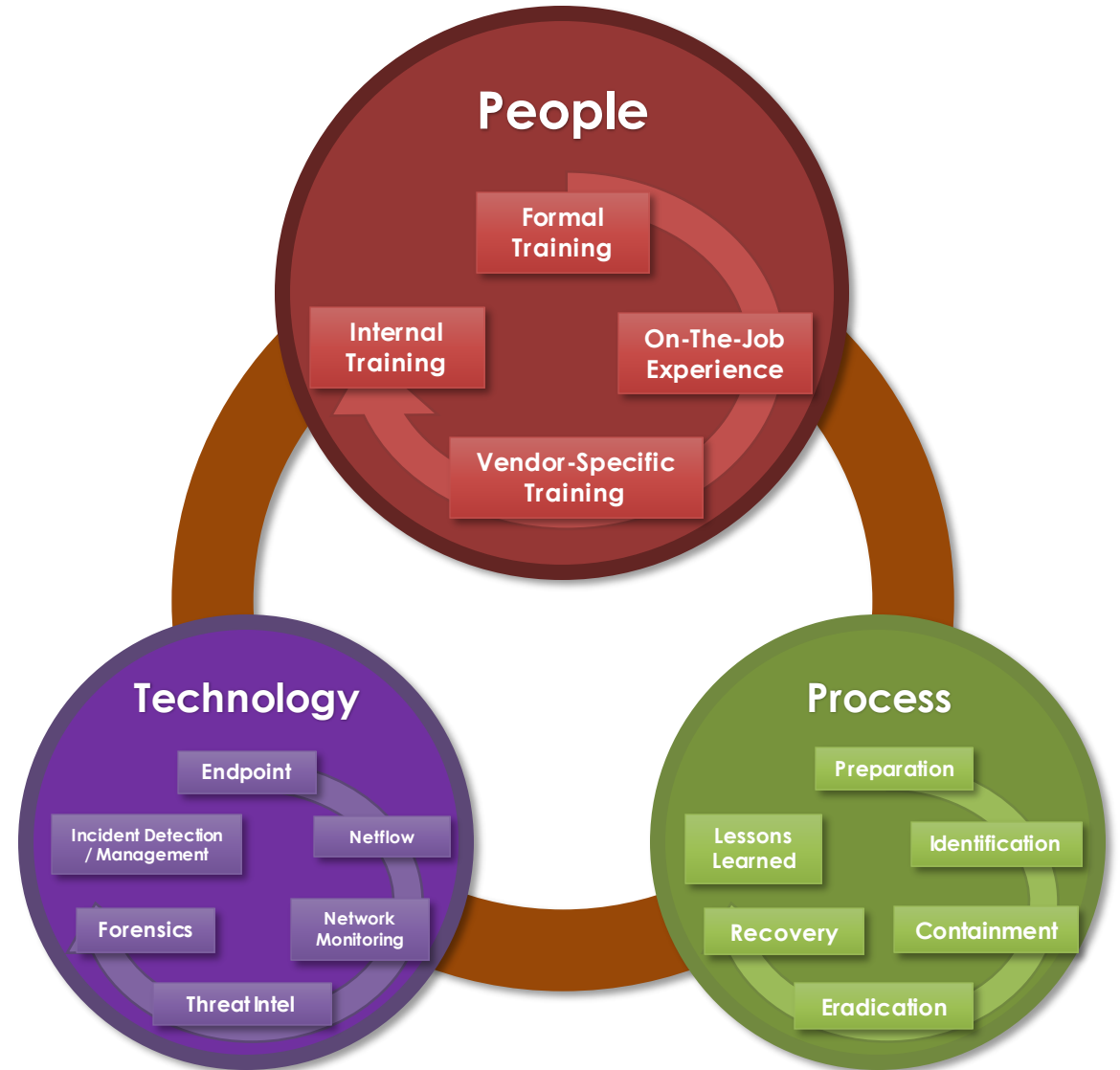
Security by optimism and prayer



Expert

Hoping Nobody Hacks You

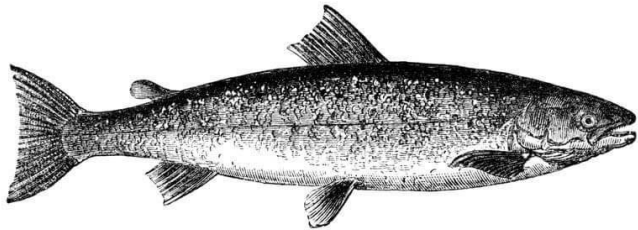
ORLY? @ThePracticalDev



Reference: <https://sibertor.com/wp-content/uploads/2016/07/building-world-class-security-operations-center-roadmap-35907.pdf>

Reality of our Current Situation

Security by optimism and prayer



Expert

Hoping Nobody Hacks You

ORLY?

@ThePracticalDev

What your defenders will do today

1. Four hours of meetings
2. Status Updates
3. Add notes to tickets
4. Timesheets
5. HR mandated training
6. close tickets as "False Positive"
7. update slide decks
8. update policies + KBs
9. 23 minutes of Infosec work

People

Normal Training

On-The-Job Experience

Job-Specific Training

Process

Preparation

Lessons Learned

Identification

Recovery

Containment

Eradication

Endpoint

Incident Detection / Management

Netflow

Forensics

Network Monitoring

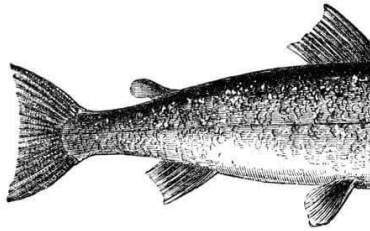
Threat Intel



Reference: <https://sibertor.com/wp-content/uploads/2016/07/building-world-class-security-operations-center-roadmap-35907.pdf>

Reality of our Current Situation

Security by optimism



Expert

Hoping N
Hacks Yo

ORLY?

What Attackers are doing today	What your defenders will do today
1. Breach your network	1. Four hours of meetings
2. Monetize	2. Status Updates
	3. Add notes to tickets
	4. Timesheets
	5. HR mandated training
	6. close tickets as "False Positive"
	7. update slide decks
	8. update policies + KBs
	9. 23 minutes of Infosec work

Who will win?

People

Formal training

On-The-Job Experience

Job-Specific training

Process

Preparation

Lessons Learned

Identification

Recovery

Containment

Eradication



DISCLAIMER: I will exercise my freedom of speech

KO...@GOOGLE.COM 08.10.2021 | 04:08

Hey

Thanks for heads up. we do not restrict the rights of our researchers. You are free to publish it.

ISAIAH.PUZON@GMAIL.COM 08.10.2021 | 04:10

Hey,

Thanks for the response. This is acknowledged! :)



DISCLAIMER: I will exercise my freedom of speech

KO...@GOOGLE.COM 08.10.2021 | 04:08

Hey

Thanks for heads up. **we do not restrict the rights of our researchers.** You are free to publish it.

ISAIAH.PUZON@GMAIL.COM 08.10.2021 | 04:10

Hey,

Thanks for the response. This is acknowledged! :)



DISCLAIMER: I will exercise my freedom of speech

KO...@GOOGLE.COM 08.10.2021 | 04:08

Hey

Thanks for heads up. we do not restrict the rights of our researchers. **You are free to publish it.**

ISAIAH.PUZON@GMAIL.COM 08.10.2021 | 04:10

Hey,

Thanks for the response. This is acknowledged! :)



Complexity of Online Security / Safety

☆ 201370894 Abuse Risk-related Methodology — YouTube Channel Name can be changed to an existing Channel Name without any Validation

0 people have starred this issue.

Component 889286

bu...@google.com <bu...@google.com> #1 Sep 28, 2021 02:13PM

Created issue (on behalf of isaiah.puzon@gmail.com).

Summary: Abuse Risk-related Methodology — YouTube Channel Name can be changed to an existing Channel Name without any Validation 02:13PM

The vulnerability is known to third parties!

Product: Youtube

URL: <https://www.youtube.com>

Vulnerability type: Other

Details

Summary: Abuse Risk-related Methodology - YouTube Channel Name can be changed to an existing Channel Name without any Validation

Any YouTube channel can impersonate another existing YouTube channel's name.

Please refer to the following PDF for more details:

- <https://drive.google.com/file/d/1RNDUy7zmzaRE91VrUGhmrGGblaWGCWR0/view?usp=sharing>

Attack scenario

Any YouTube user.

It is already being actively exploited by criminals.

Please refer to the following PDF for more details:

- <https://drive.google.com/file/d/1RNDUy7zmzaRE91VrUGhmrGGblaWGCWR0/view?usp=sharing>

Component:	310426	02:13PM
Type:	Customer Issue	02:13PM
Priority:	P4	02:13PM
Severity:	S4	02:13PM
Title:	Abuse Risk-related Methodology — YouTube Channel Name can be changed to an existing Channel Name without any Validation	02:13PM
Reporter:	<none> → isaiah.puzon@gmail.com (Isaiah Puzon)	02:13PM
+CC:	wo...@google.com, isaiah.puzon@gmail.com (Isaiah Puzon)	02:13PM
Status:	New	02:13PM



Complexity of Online Security / Safety

☆ 201146326 other in YouTube
0 people have starred this issue.
Component 889286

ap...@google.com <ap...@google.com> #1
Created issue (on behalf of isaiah.puzon@gmail.com).
Sep 25, 2021 06:43PM

Summary: Abuse Risk-related Methodology – YouTube Channel Name can be changed to an existing Channel Name without any Validation 06:43PM

Steps to reproduce (Mobile):
1. Open YouTube Android App (Must be logged in with a Gmail account)
2. Click profile photo on the top right & click "Your Channel"
3. Click "Edit Channel"
4. Edit Name to any existing channel

Browser/OS:
- Mozilla/5.0 (Linux; Android 10; ONEPLUS A5000) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Mobile Safari/537.36

Attack scenario:
Re-sending this since I didn't receive an email during my initial reporting of this.

This is actively being abused by malicious actors preying on the lay person.

Attack Scenario:
1. Form a criminal syndicate (or do it solo, idk)
2. Create a list of YouTube Influencers to target (usually those who do giveaways)
3. Create dummy Gmail accounts
4. Impersonate YouTube Influencers with this issue
5. ???
6. PROFIT!!!

Incident Report / Real-Life Use Case:
<https://drive.google.com/file/d/1b7JtREP3z9Oes7tKPU1Ud2tAPq14d9rr/view?usp=drivesdk>

Acquisition info:
It was acquired on October 9, 2006 - see <https://www.sec.gov/Archives/edgar/data/1288776/000119312506206884/dex991.htm>

Component: 310426 06:43PM
Type: Customer Issue 06:43PM
Priority: P4 06:43PM



Complexity of Online Security / Safety

Reward amounts for abuse-related methodologies

New! Rewards for abuse-related methodologies are based on a different scale and range from USD \$100 to \$13,337. The reward amount for these abuse-related bugs depends on the potential probability and impact of the submitted technique.

		Impact [1]		
		High	Medium	Low
Probability [2]	High	Up to \$13,337	\$3,133.7 to \$5,000	\$1,337
	Medium	\$3,133.7 to \$5,000	\$1,337	\$100 to \$500
	Low	\$1,337	\$100 to \$500	HoF Credit

[1] The impact assessment is based on the attack's potential for causing privacy violations, financial loss, and other user harm, as well as the user-base reached.

[2] The probability assessment takes into account the technical skill set needed to conduct the attack, the potential motivators of such an attack, and the likelihood of the vulnerability being discovered by an attacker.

The final amount is always chosen at the discretion of the reward panel. In particular, we may decide to pay higher rewards for unusually clever or severe vulnerabilities; decide to pay lower rewards for vulnerabilities that require unusual user interaction; decide that a single report actually constitutes multiple bugs; or that multiple reports are so closely related that they only warrant a single reward.

We understand that some of you are not interested in money. We offer the option to donate your reward to an established charity. If you do so, we will double your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

What is an abuse risk?

An abuse risk could be seen as a product feature that could cause unexpected damage to a user or platform when leveraged in an unexpected manner. Abuse risks arise when products don't have sufficient protections against its features being used in a malicious way.

For example, the ability to import your contacts into a social network app to see which one of your friends is using the app would be considered a feature. This feature could also become an abuse risk if there isn't a quota in place on the amount of contact lookups that could be done within this social network app during a given timeframe. Without any restrictions in place, malicious actors could use this feature to build a large database of users for their spam campaigns.

Contrary to security vulnerabilities, where an identified loophole requires a fix, abuse risks can often be inherent to product features. That means that oftentimes, they shouldn't be stopped fully but products need protections mitigating its exploitation at scale.

Reference:

<https://www.google.com/about/appsecurity/reward-program/>

<https://sites.google.com/site/bughunteruniversity/improve/what-is-an-abuse-risk>

KO...@GOOGLE.COM 07.10.2021 | 16:42

■ CLOSED

Status updated

Hi! We've reviewed your submission and decided not to track it as a security bug, as we are already aware of this issue. We have policies and protections to handle such instances. More about it [here](#).

For the same reason, your report will also not be accepted to our VRP. Only first reports of technical security vulnerabilities are in scope for VRP :(Sorry about that.

Nevertheless, we're looking forward to your next report! To maximize the chances of it being accepted, check out the [Bug Hunter University] (<https://bughunters.google.com/learn>) and learn some [Secrets of Google VRP](#).

Thanks again for your report and time,
Google Trust & Safety

07.10.2021 | 16:47

Many thanks!

Since this is not considered an issue, I presume it's alright for me to disclose this report publicly (e.g. Public Speaking Presentations) right?



Complexity of Online Security / Safety

Reward amounts for abuse-related methodologies

New! Rewards for abuse-related methodologies are based on a different scale and range from USD \$100 to \$13,337. The reward amount for these abuse-related bugs depends on the potential probability and impact of the submitted technique.

		Impact [1]		
		High	Medium	Low
Probability [2]	High	Up to \$13,337	\$3,133.7 to \$5,000	\$1,337
	Medium	\$3,133.7 to \$5,000	\$1,337	\$100 to \$500
	Low	\$1,337	\$100 to \$500	HoF Credit

[1] The impact assessment is based on the attack's potential for causing privacy violations, financial loss, and other user harm, as well as the user-base reached.

[2] The probability assessment takes into account the technical skill set needed to conduct the attack, the potential motivators of such an attack, and the likelihood of the vulnerability being discovered by an attacker.

The final amount is always chosen at the discretion of the reward panel. In particular, we may decide to pay higher rewards for unusually clever or severe vulnerabilities; decide to pay lower rewards for vulnerabilities that require unusual user interaction; decide that a single report actually constitutes multiple bugs; or that multiple reports are so closely related that they only warrant a single reward.

We understand that some of you are not interested in money. We offer the option to donate your reward to an established charity. If you do so, we will double your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

What is an abuse risk?

An abuse risk could be seen as a product feature that could cause unexpected damage to a user or platform when leveraged in an unexpected manner. Abuse risks arise when products don't have sufficient protections against its features being used in a malicious way.

For example, the ability to import your contacts into a social network app to see which one of your friends is using the app would be considered a feature. This feature could also become an abuse risk if there isn't a quota in place on the amount of contact lookups that could be done within this social network app during a given timeframe. Without any restrictions in place, malicious actors could use this feature to build a large database of users for their spam campaigns.

Contrary to security vulnerabilities, where an identified loophole requires a fix, abuse risks can often be inherent to product features. That means that oftentimes, they shouldn't be stopped fully but products need protections mitigating its exploitation at scale.

Reference:

<https://www.google.com/about/appsecurity/reward-program/>

<https://sites.google.com/site/bughunteruniversity/improve/what-is-an-abuse-risk>

KO...@GOOGLE.COM 07.10.2021 | 16:42

■ CLOSED

Status updated

Hi! We've reviewed your submission and decided not to track it as a security bug, as we are already aware of this issue. We have policies and protections to handle such instances. More about it [here](#).

For the same reason, your report will also not be accepted to our VRP. Only first reports of technical security vulnerabilities are in scope for VRP :(Sorry about that.

Nevertheless, we're looking forward to your next report! To maximize the chances of it being accepted, check out the [Bug Hunter University] (<https://bughunters.google.com/learn>) and learn some [Secrets of Google VRP](#).

Thanks again for your report and time,
Google Trust & Safety

07.10.2021 | 16:47

Many thanks!

Since this is not considered an issue, I presume it's alright for me to disclose this report publicly (e.g. Public Speaking Presentations) right?



Complexity of Online Security / Safety

Impersonation policy



The safety of our creators, viewers, and partners is our highest priority. We look to each of you to help us protect this unique and vibrant community. It's important you understand our Community Guidelines, and the role they play in our shared responsibility to keep YouTube safe. Take the time to carefully read the policy below. You can also check out [this page](#) for a full list of our guidelines.

Content intended to impersonate a person or channel is not allowed on YouTube. YouTube also enforces trademark holder rights. When a channel, or content in the channel, causes confusion about the source of goods and services advertised, it may not be allowed.

If you see content that violates this policy, [please report it](#).

- If you feel that yours or another creator's channel is being impersonated, you can report the channel by following the instructions [here](#).

What these policies mean for you

If you're posting content

Don't post content on YouTube if it fits any of the descriptions noted below.

- **Channel impersonation:** A channel that copies another channel's profile, background, or overall look and feel in such a way that makes it look like someone else's channel. The channel does not have to be 100% identical, as long as the intent is clear to copy the other channel.
- **Personal impersonation:** Content intended to look like someone else is posting it.



Complexity of Online Security / Safety

Impersonation policy



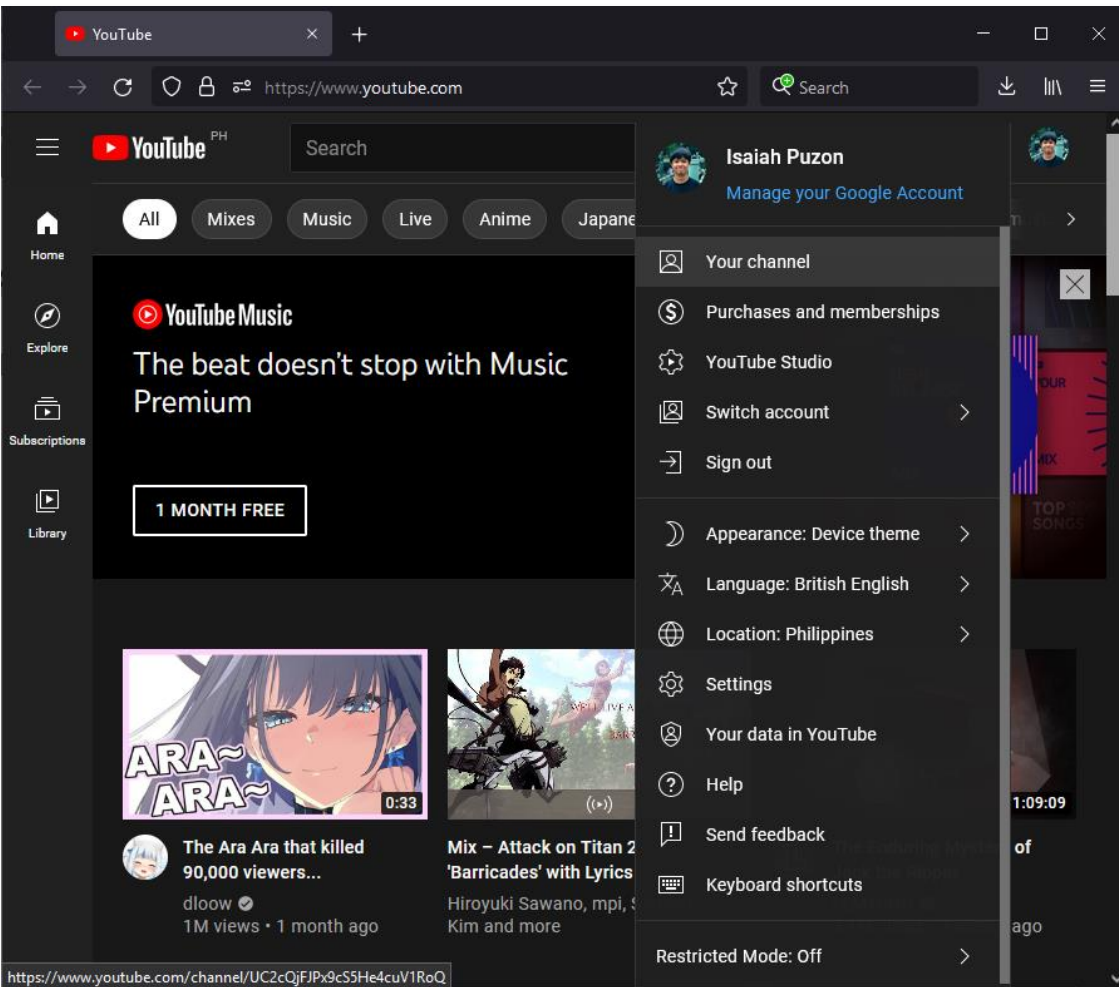


Abuse Risk-related Methodology

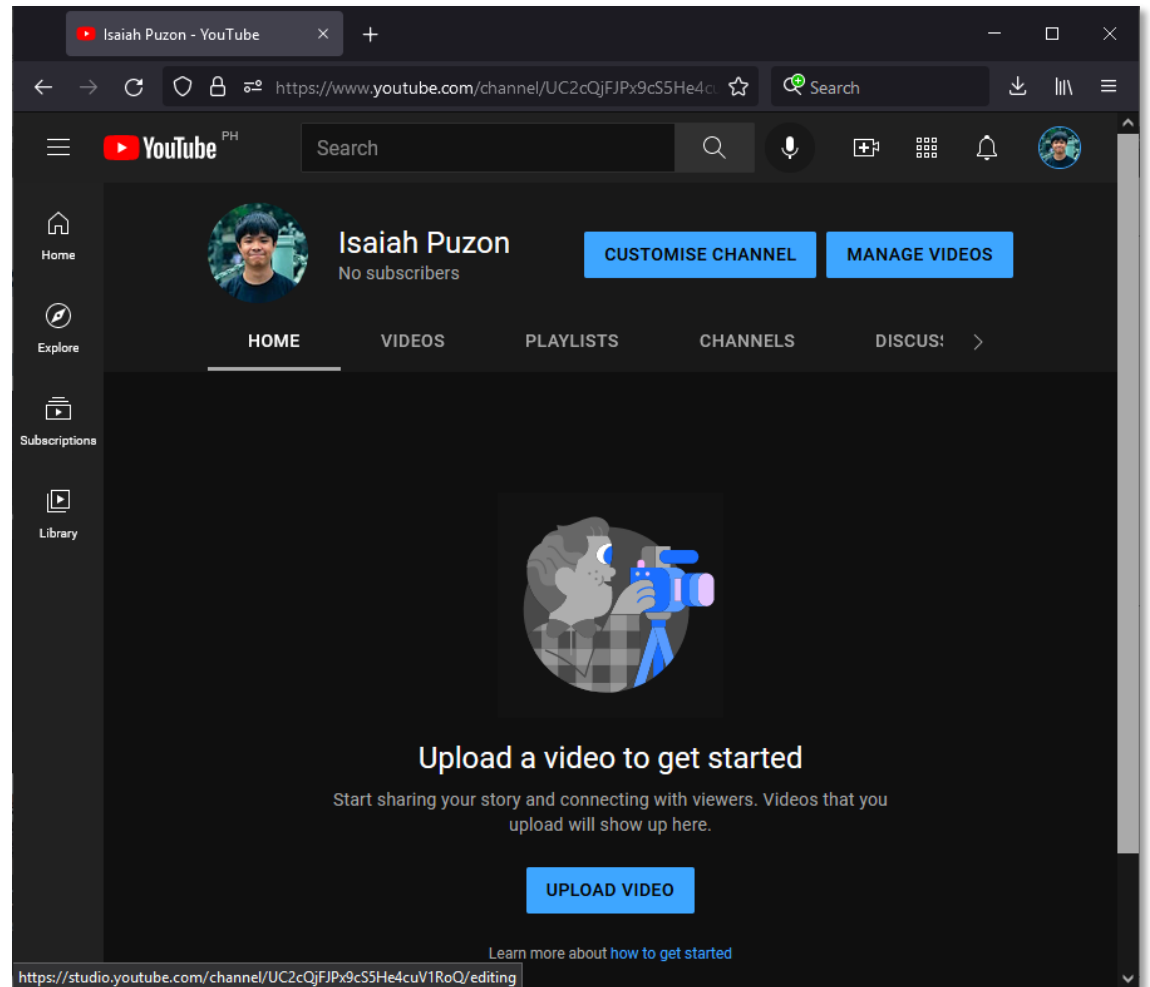
YouTube Channel Name can be changed to an existing Channel Name without any Validation

Replication Steps – Web-based through a Browser

#1 – While logged in to YouTube, click your profile picture and press **Your channel**

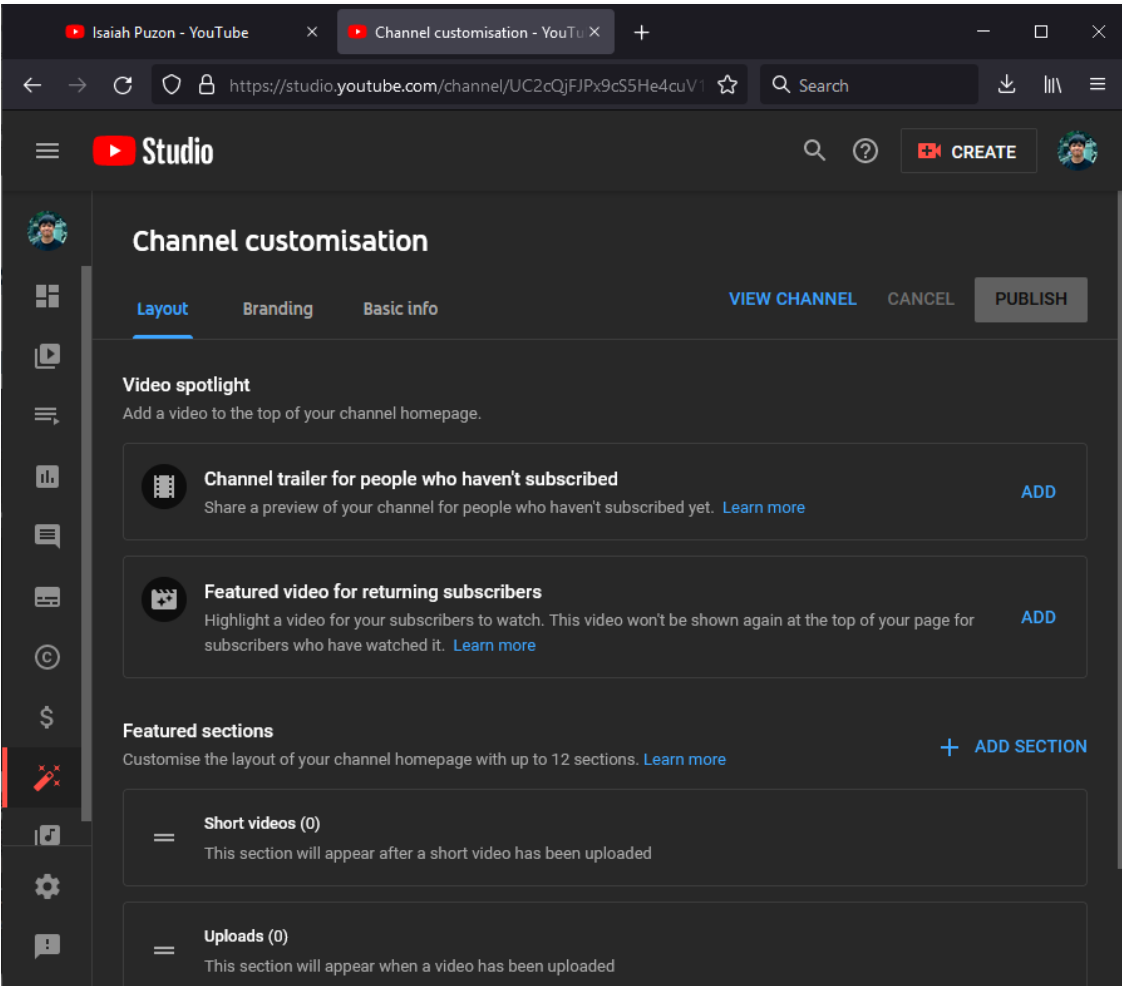


#2 – Press **CUSTOMISE CHANNEL**

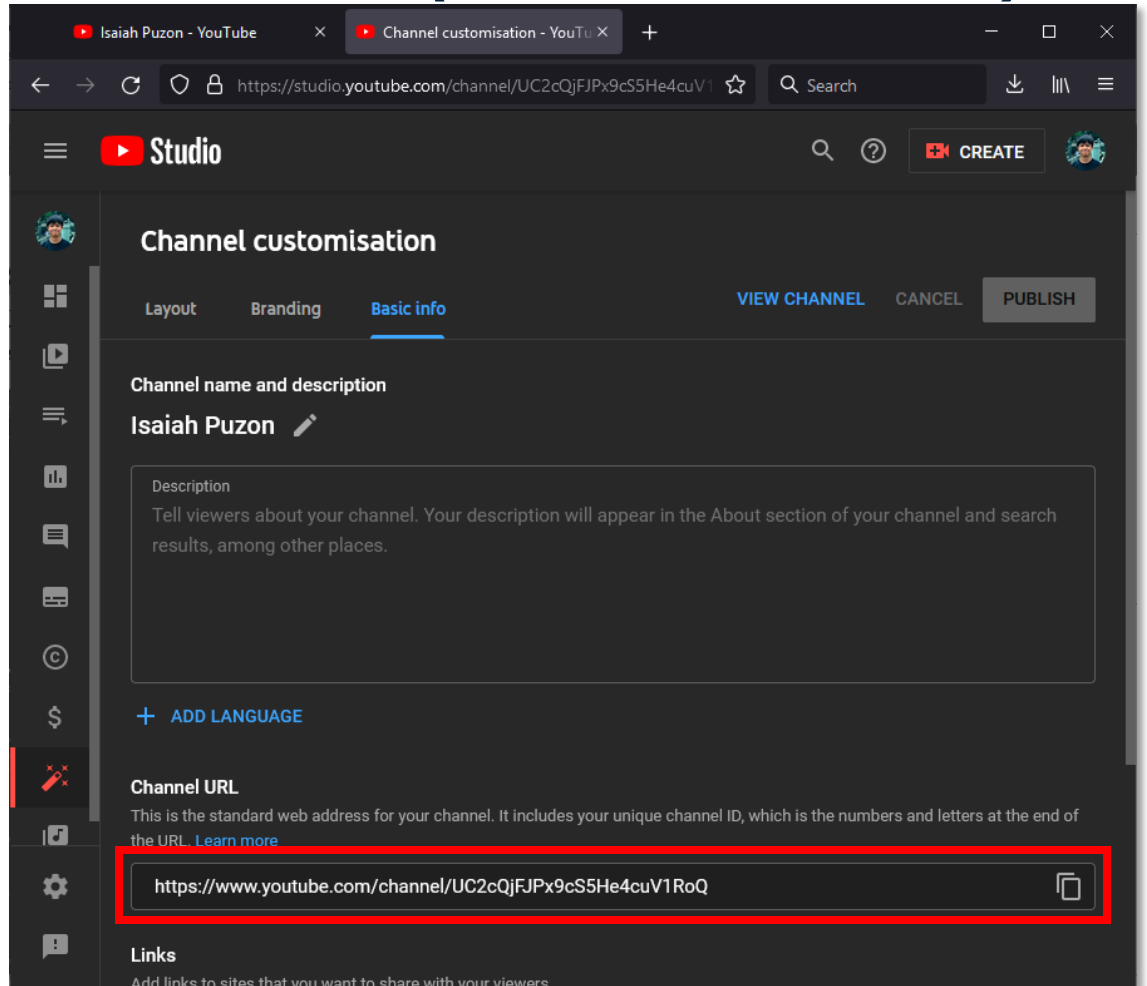


Replication Steps – Web-based through a Browser

#3 – Under **Channel customization**, press **Basic info**



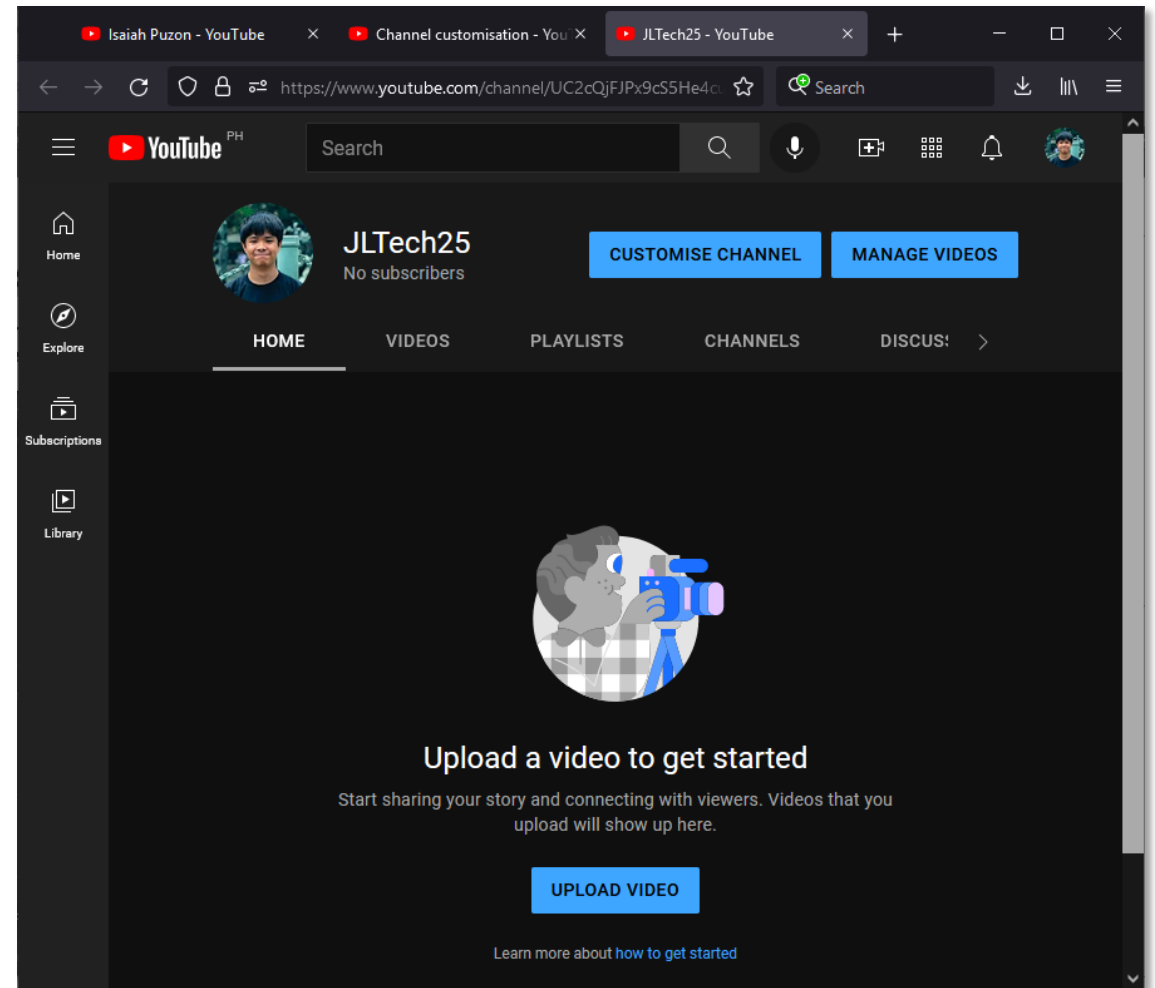
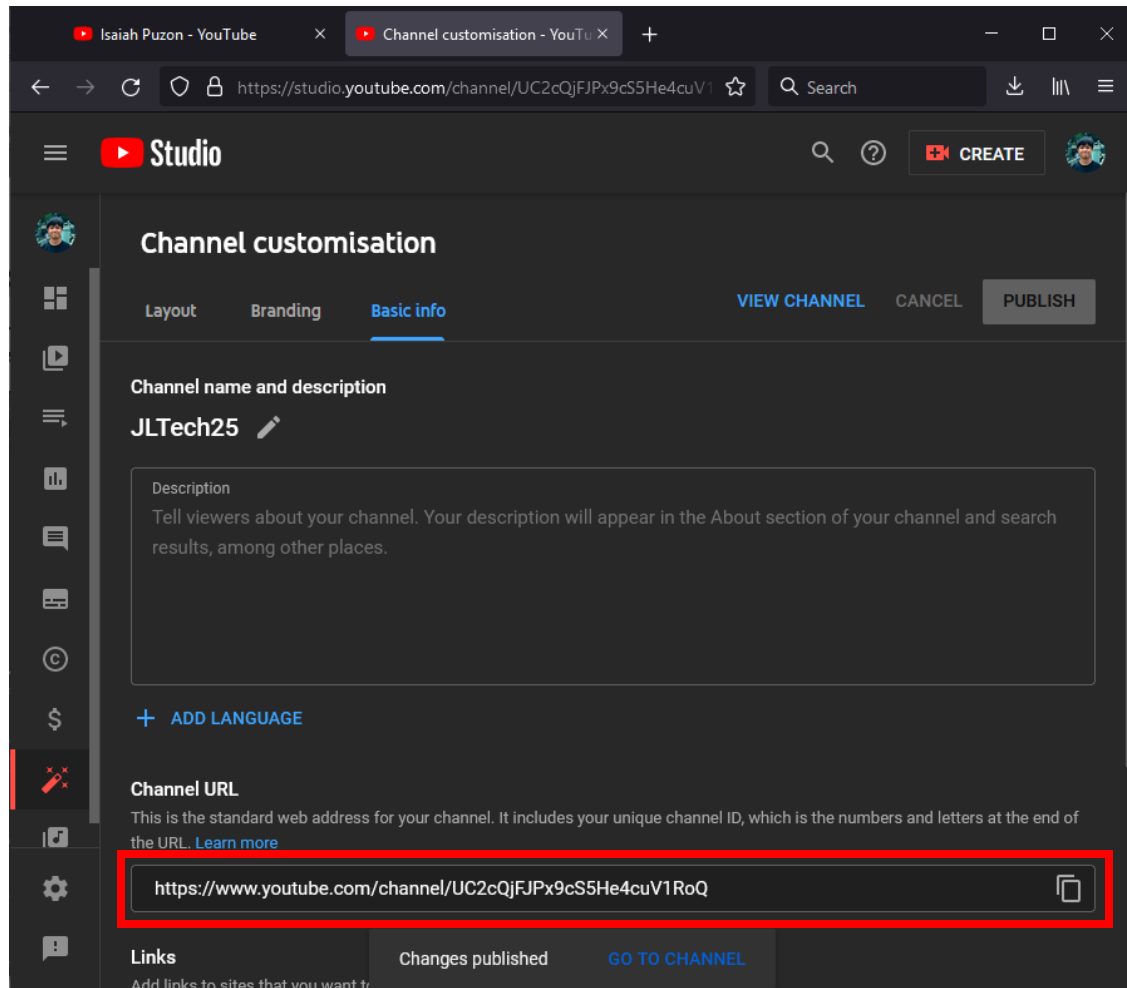
#4 – Press the **Edit** button & change the Channel name (**Note the Channel URL**)



Replication Steps – Web-based through a Browser

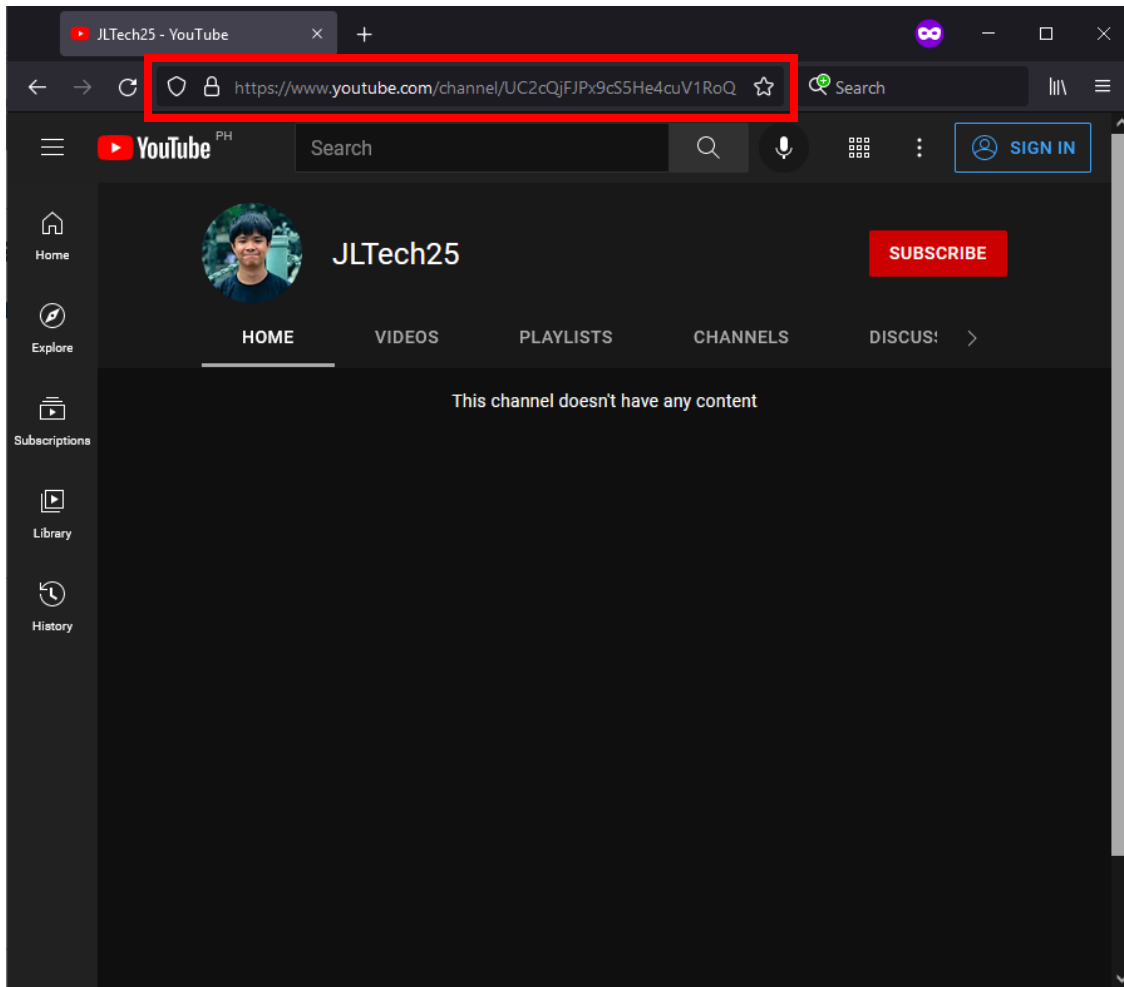
#5 – Edit Channel name, press **PUBLISH** then **VIEW CHANNEL**

#6 – Channel name has been changed



Replication Steps – Web-based through a Browser

#7 – Visit the Channel URL from #4 on a different browser (**e.g: Private Browsing**)

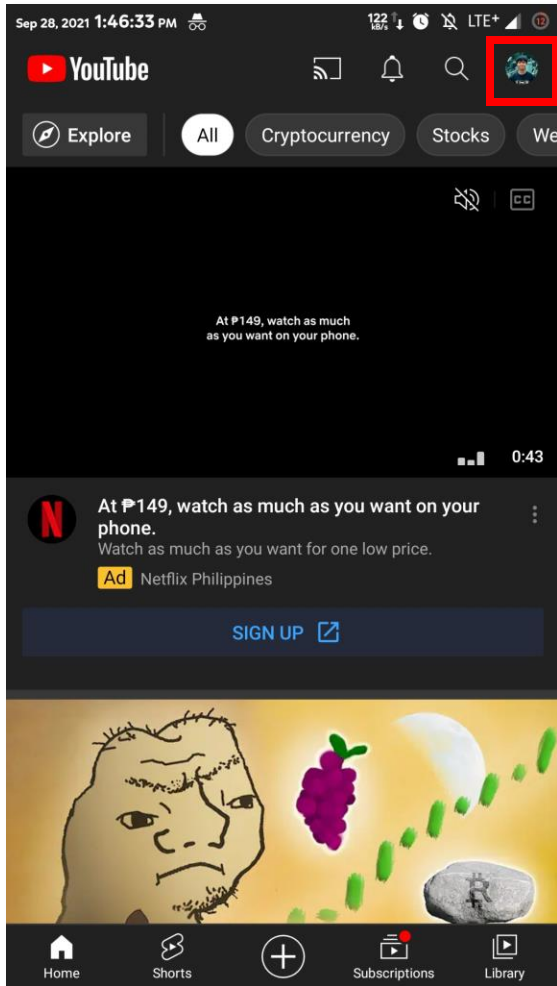


Key Points:

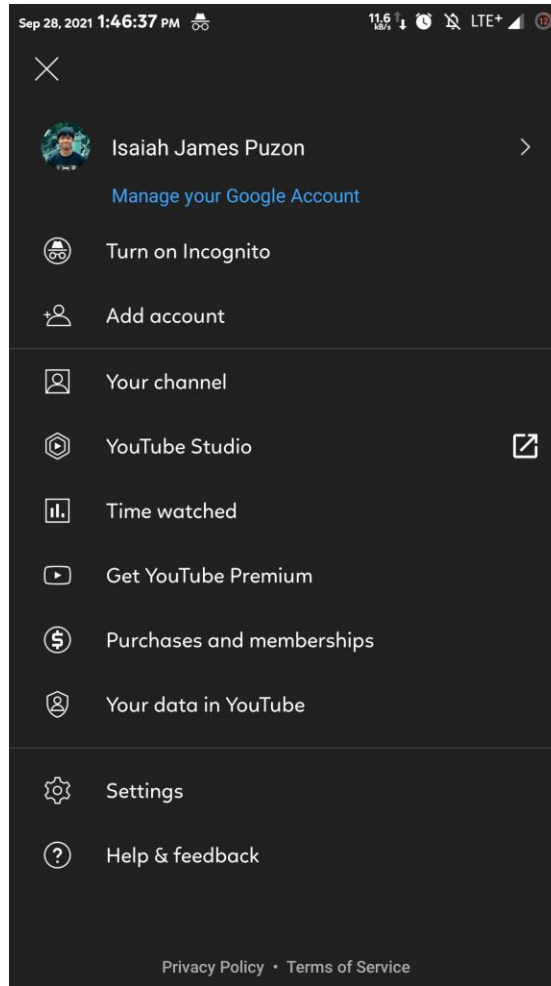
- This is already being actively abused by criminals
- It applies to both Web and Mobile versions of YouTube
- Any YouTube account can perform this (**even newly created ones**)
- This can lead to **extremely convincing phishing** & **social engineering** attacks
- **Criminals are already profiting from this**
- **Victims can only go to a corner and cry**

Replication Steps – Mobile Application

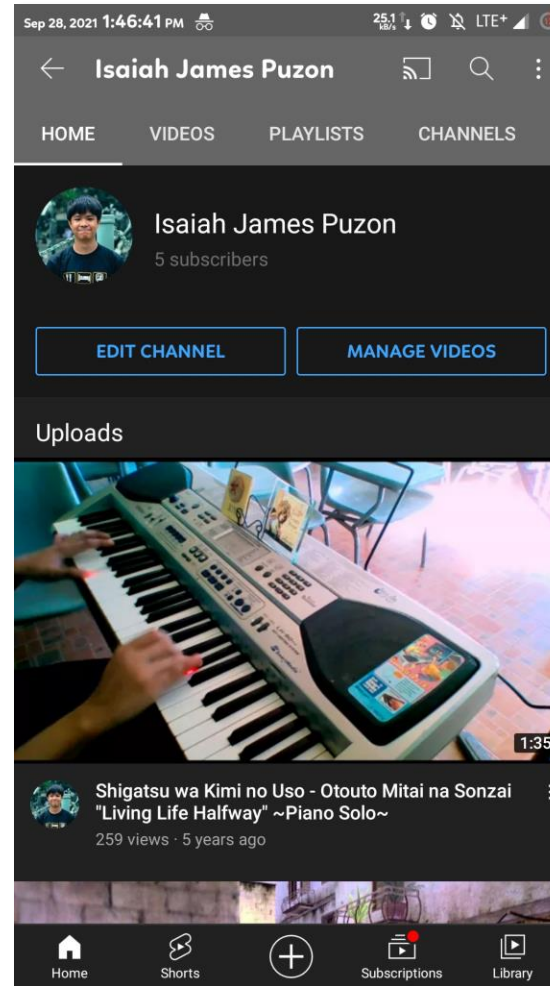
#1 – Open YouTube Mobile Application then click your **Profile Photo** at the **top right**



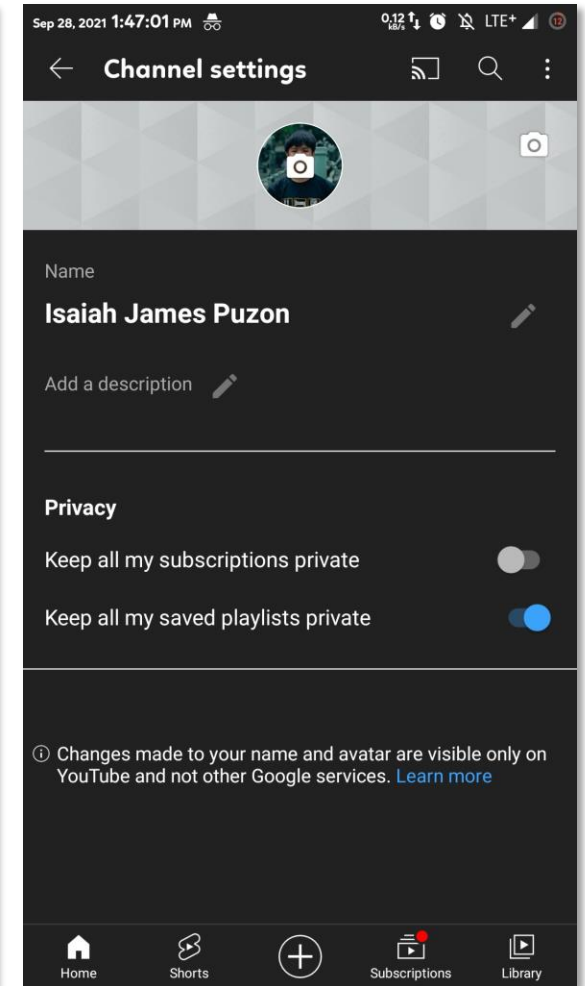
#2 – Click **Your Channel**



#3 – Click **EDIT CHANNEL**

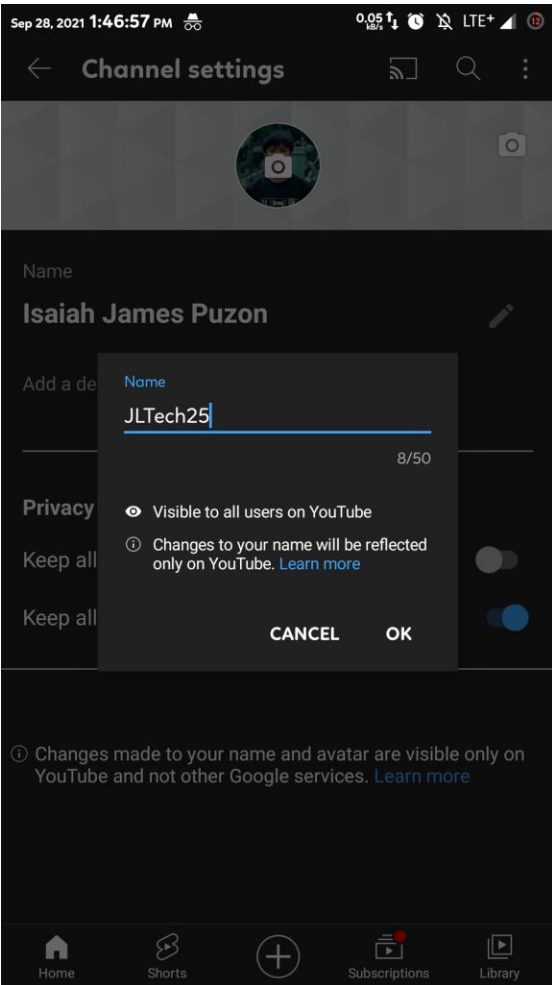


#4 – Press **Edit** button & change the **Channel Name**

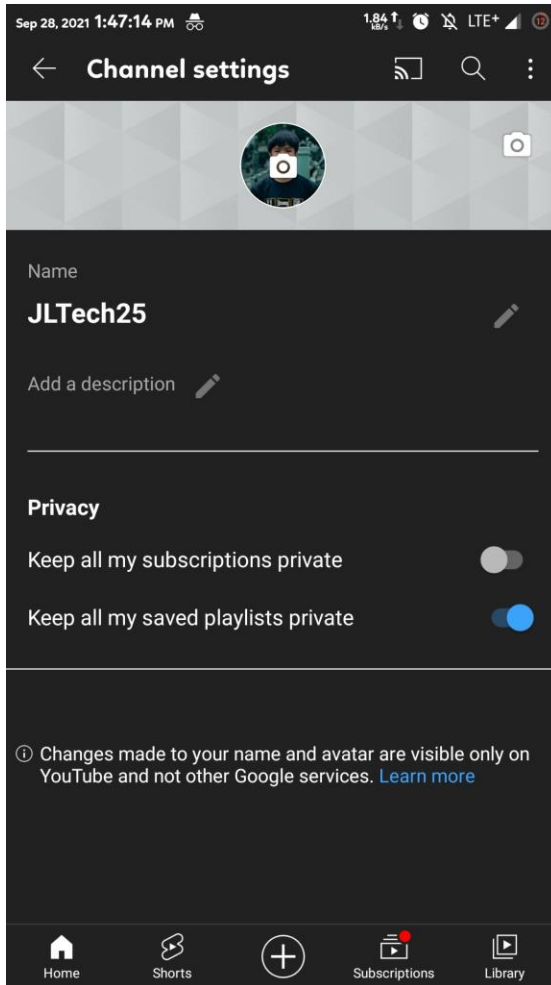


Replication Steps – Mobile Application

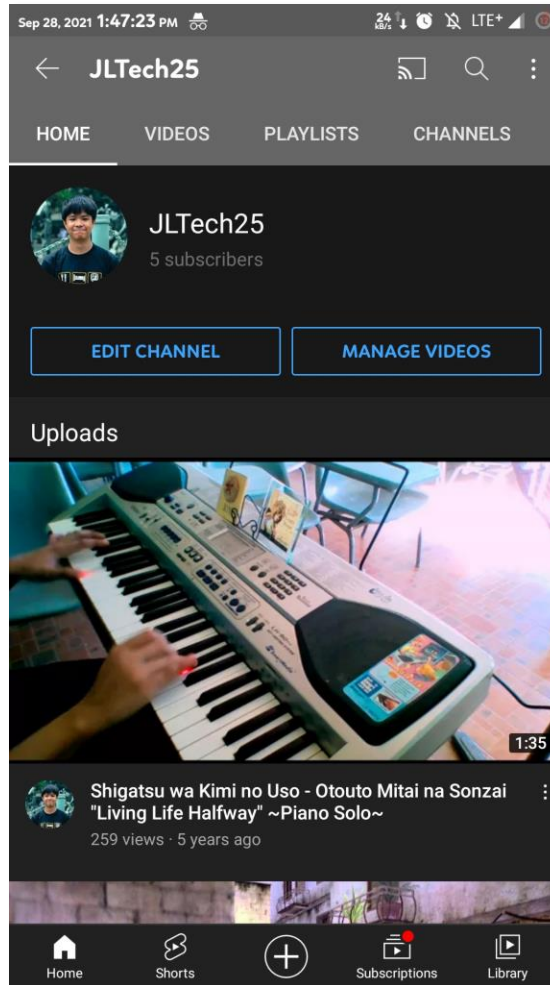
#5 – Change **Name** to an **existing** Channel's Name then press **OK**



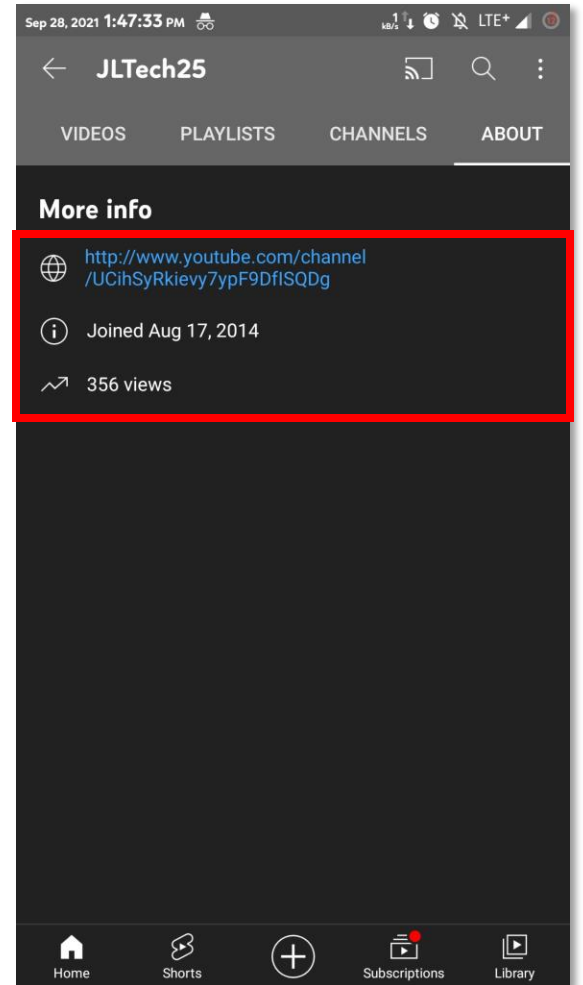
#6 – Press **Back**



#7 – Observe that the **Channel Name is changed** – Navigate to **About** tab

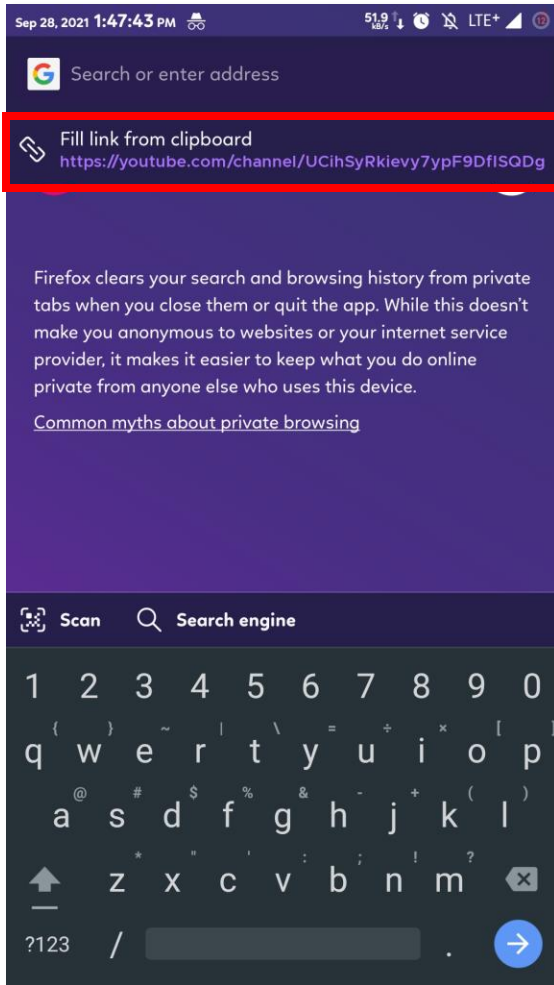


#8 – Copy the **Channel URL**

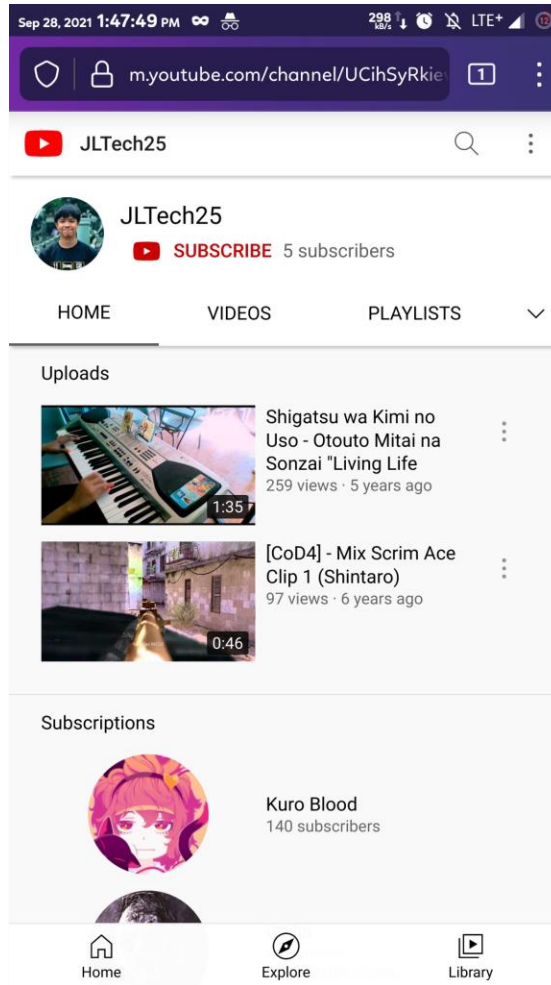


Replication Steps – Mobile Application

#9 – Access the copied Channel URL via **Private Browsing** tab



#10 – Observe the modified **Channel Name**



Key Points:

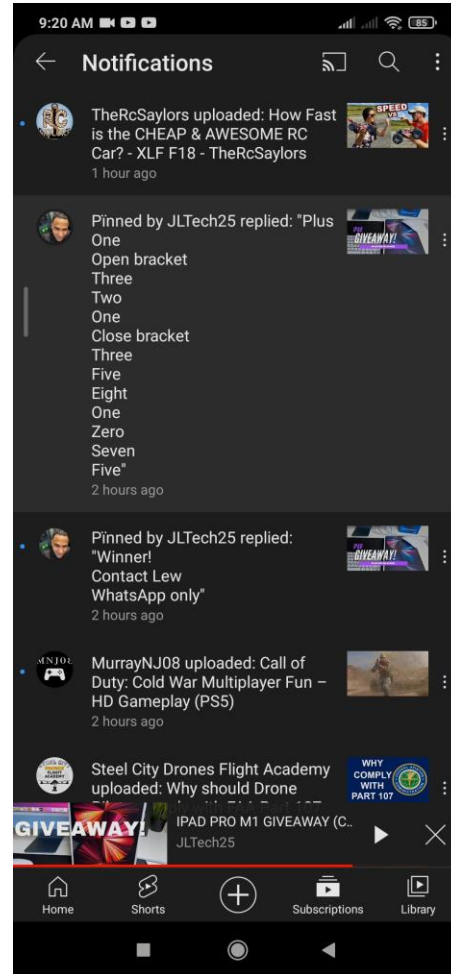
- This is already being **actively abused** by criminals
- It **applies to both Web and Mobile** versions of YouTube
- Any YouTube account can perform this **(even newly created ones)**
- This can lead to **extremely convincing phishing & social engineering** attacks
- **Criminals are already profiting from this**
- **Victims can only go to a corner and cry**

Use Case: Incident on September 15, 2021

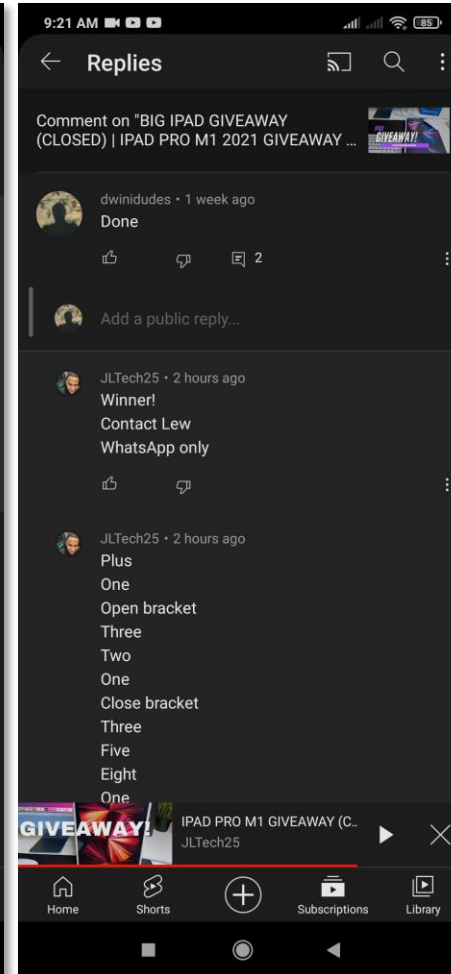
The user **"JLTech25"** posted a video titled: **"IPAD PRO M1 GIVEAWAY (CLOSED) 2021 | BIG GIVEAWAY | APPLE IPAD GIVEAWAY!!!"**

- **Link:** <https://www.youtube.com/watch?v=FJApybbCBe8>
- **Note:**
At 0:20 – 0:25 JLTech25 mentioned: "This giveaway is international we pay for shipping you don't have to pay for anything."
- **Context:**
My father (dwinidudes) posted a comment on this video about a week prior to the phishing attempt / malicious comment on September 15, 2021
- My father received a notification from **"JLTech25"** who apparently replied to his comment saying he is a "Winner" in this give away (see image # 1)
- Checked the notification to see the actual comment which states to contact "Lew" via WhatsApp number +1(321)3581075 (see image #2)
- Clicking the profile image of the commenter shows:
 - The channel was created only 2 hours ago
 - 118 comments were already made by the channel
 - They also replied to other comments on the video with the same message (see image 3)

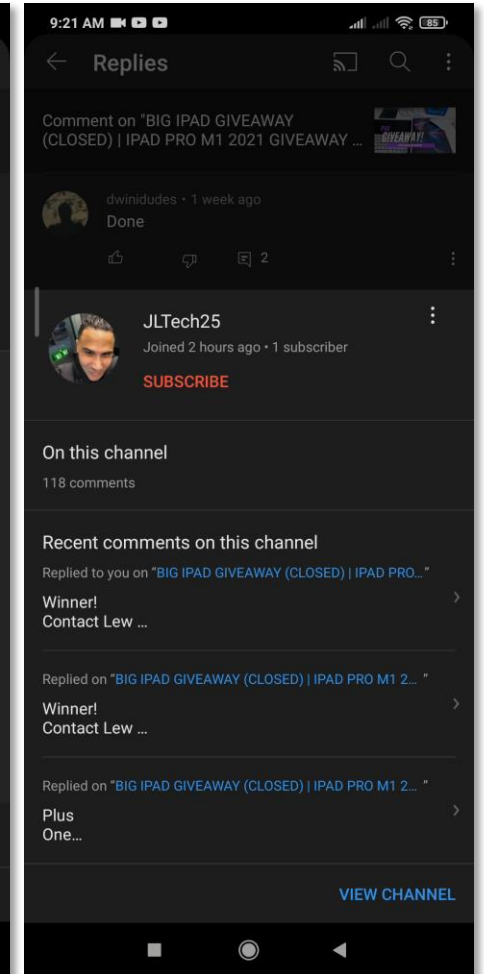
#1



#2



#3

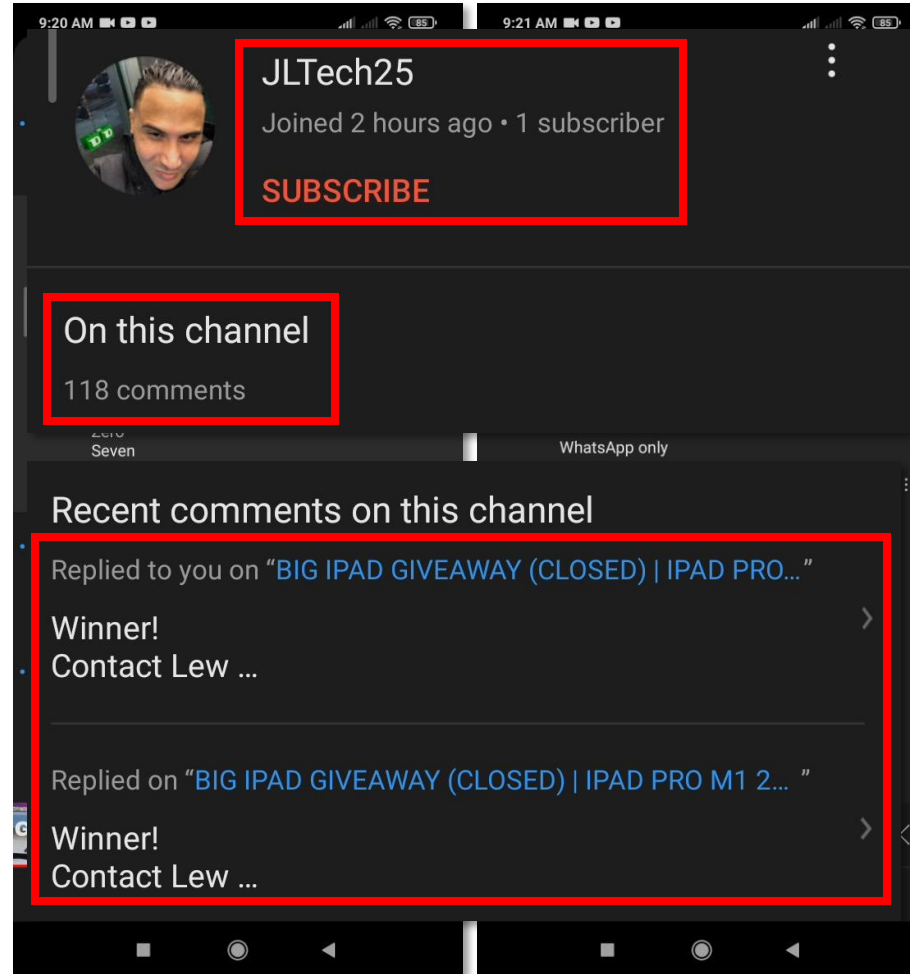


Use Case: Incident on September 15, 2021

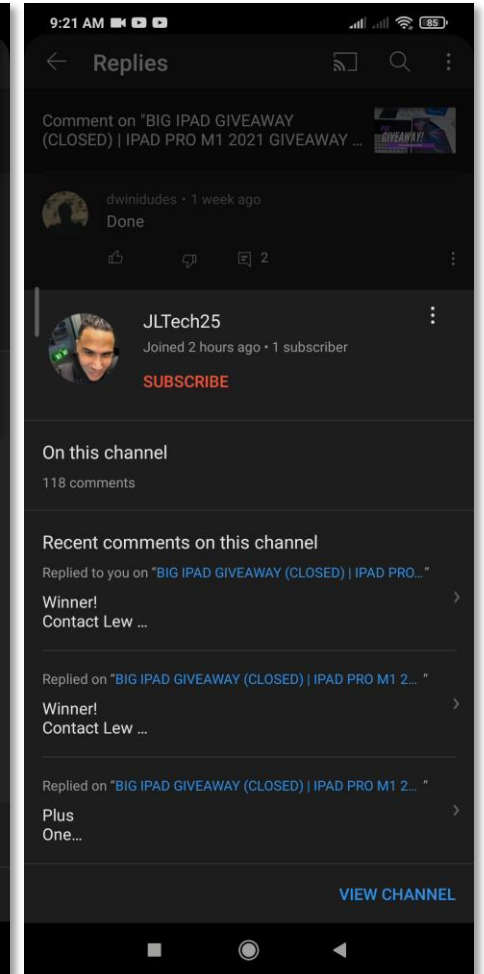
The user **"JLTech25"** posted a video titled:
"IPAD PRO M1 GIVEAWAY (CLOSED) 2021 | BIG GIVEAWAY | APPLE IPAD GIVEAWAY!!!"

- **Link:** <https://www.youtube.com/watch?v=FJApybbCBe8>
- **Note:**
At 0:20 – 0:25 JLTech25 mentioned: "This giveaway is international we pay for shipping you don't have to pay for anything."
- **Context:**
My father (dwinidudes) posted a comment on this video about a week prior to the phishing attempt / malicious comment on September 15, 2021
- My father received a notification from **"JLTech25"** who apparently replied to his comment saying he is a "Winner" in this give away (see image #1)
- Checked the notification to see the actual comment which states to contact "Lew" via WhatsApp number +1(321)3581075 (see image #2)
- Clicking the profile image of the commenter shows:
 - The channel was created only 2 hours ago
 - 118 comments were already made by the channel
 - They also replied to other comments on the video with the same message (see image 3)

#1



#2



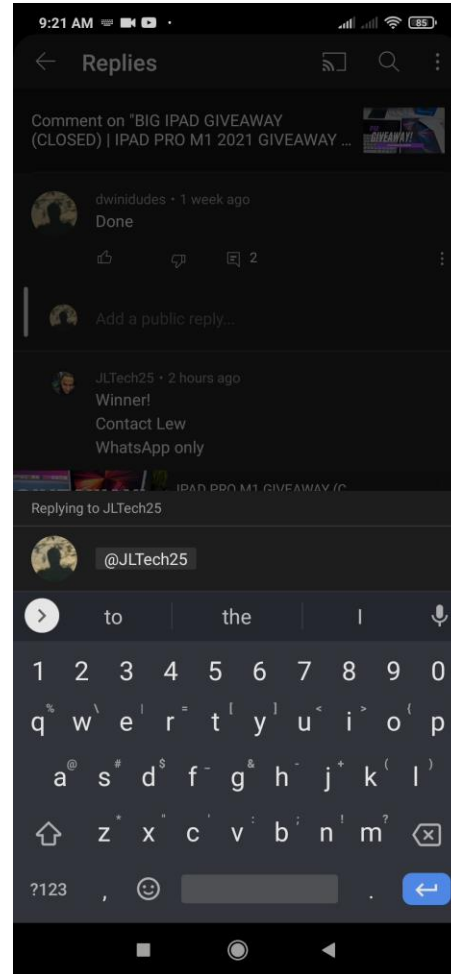
#3

Use Case: Incident on September 15, 2021

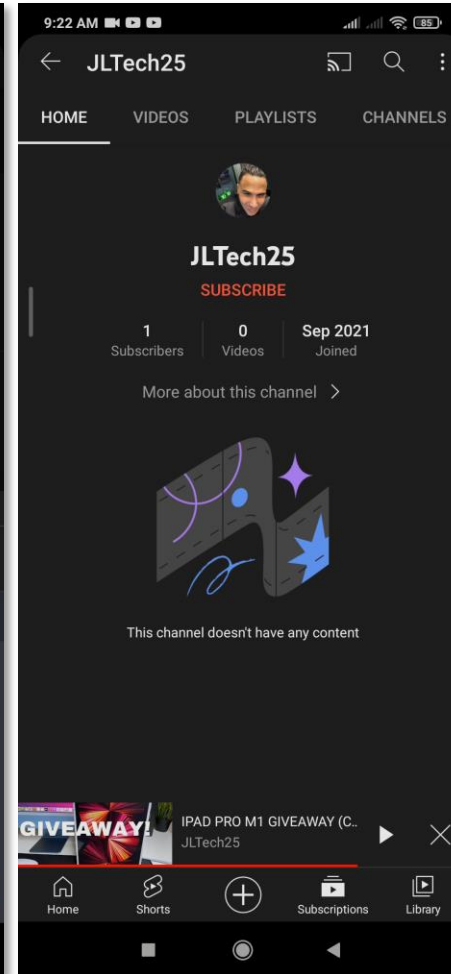
The user “**JLTech25**” posted a video titled: **“IPAD PRO M1 GIVEAWAY (CLOSED) 2021 | BIG GIVEAWAY | APPLE IPAD GIVEAWAY!!!”**

- **Link:** <https://www.youtube.com/watch?v=FJApybbCBe8>
- **Note:**
At 0:20 – 0:25 JLTech25 mentioned: “This giveaway is international we pay for shipping you don't have to pay for anything.”
- Replying to the scammer shows that their name is really **@JLTech25** (see image #4)
- Viewing the home page of the scammer's channel shows that it only has 1 subscriber & the account of my father is not subscribed to it (see image #5)
- Navigating to the about page shows the URL to the malicious actor's channel & that their join date is “September 15, 2021”
 - **URL to the Malicious Channel:**
<http://www.youtube.com/channel/UCwqm0K2swVRGwMuT7o7FU6g>

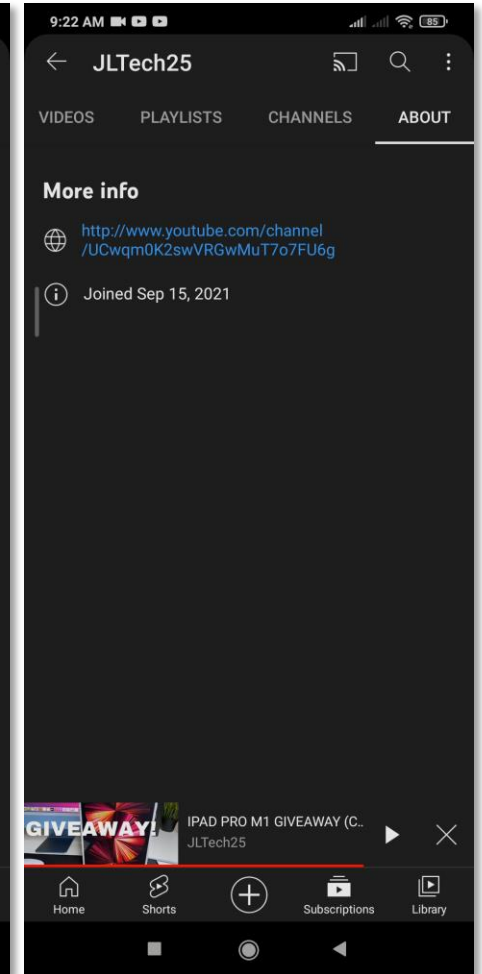
#4



#5



#6

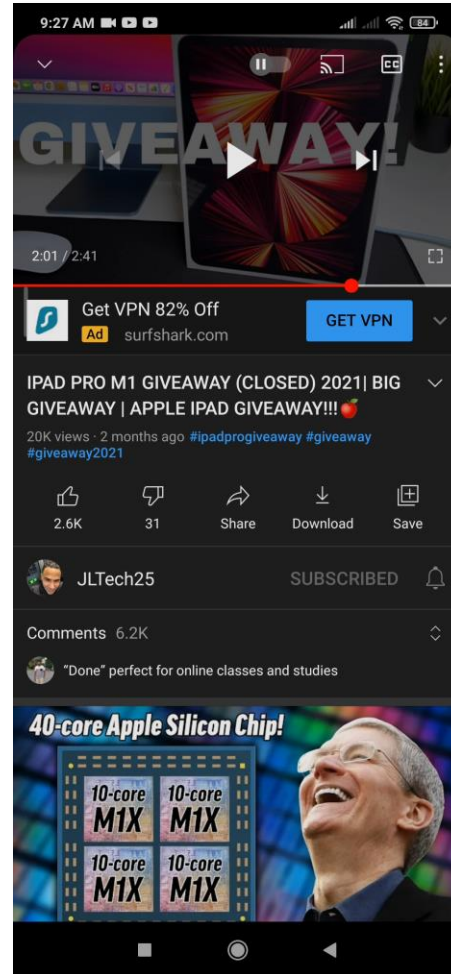


Use Case: Incident on September 15, 2021

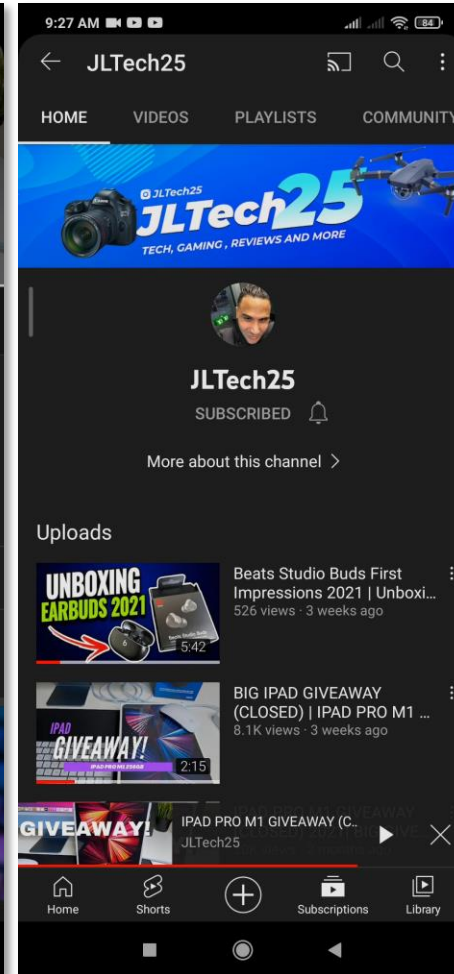
The user “**JLTech25**” posted a video titled: **“IPAD PRO M1 GIVEAWAY (CLOSED) 2021 | BIG GIVEAWAY | APPLE IPAD GIVEAWAY!!!”**

- **Link:** <https://www.youtube.com/watch?v=FJApybbCBe8>
- **Note:** At 0:20 – 0:25 JLTech25 mentioned: “This giveaway is international we pay for shipping you don't have to pay for anything.”
- After checking the malicious actor's page, I navigated to the original video & saw that my father's account is subscribed to the original **@JLTech25** (see image #7)
- The home page of **@JLTech25** shows that their channel has multiple videos uploaded (see image #8)
- The about page of **@JLTech25** shows the original URL to their channel, their location in the world, a join date of August 15, 2020 & 174,426 views (see image #9)
 - **URL to the original @JLTech25 Channel:**
http://www.youtube.com/channel/UCd_cVhbwMcTJAAZcKjy0fg

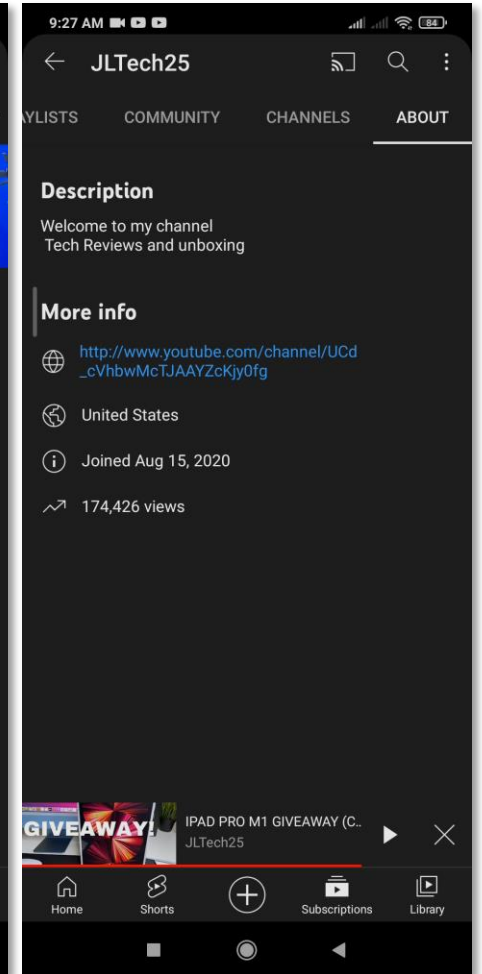
#7



#8

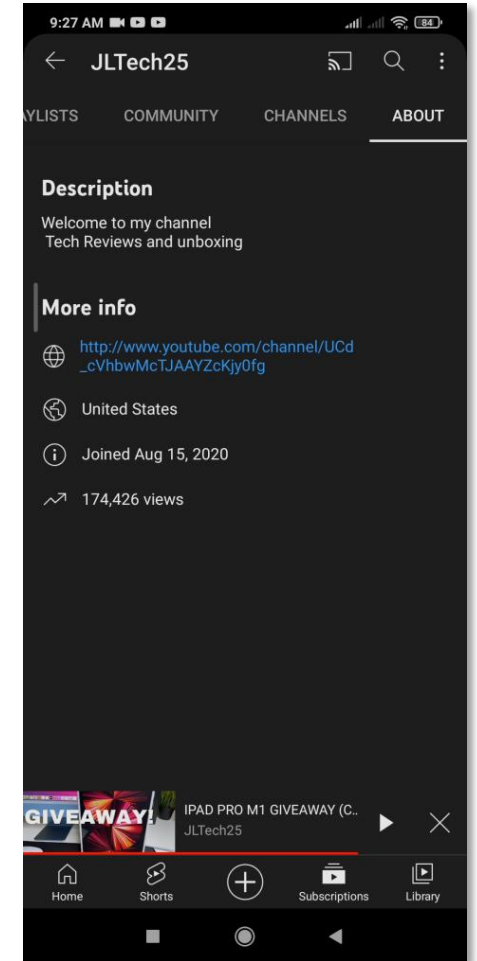
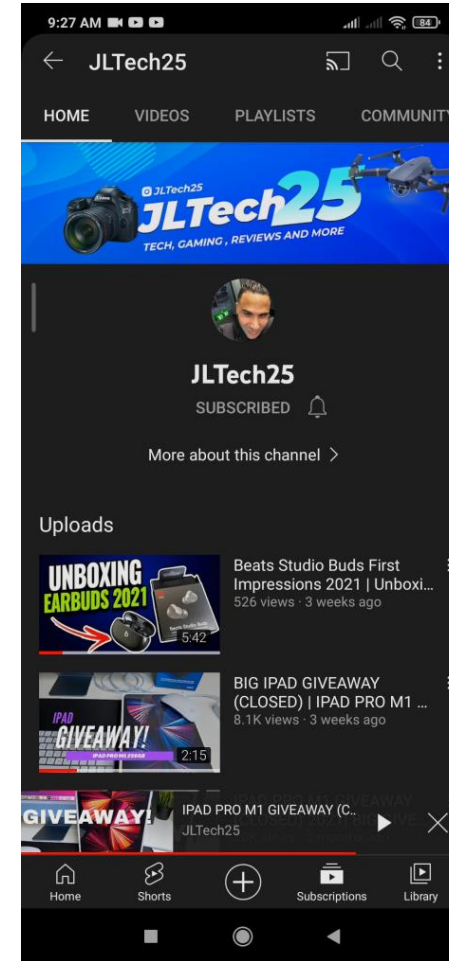
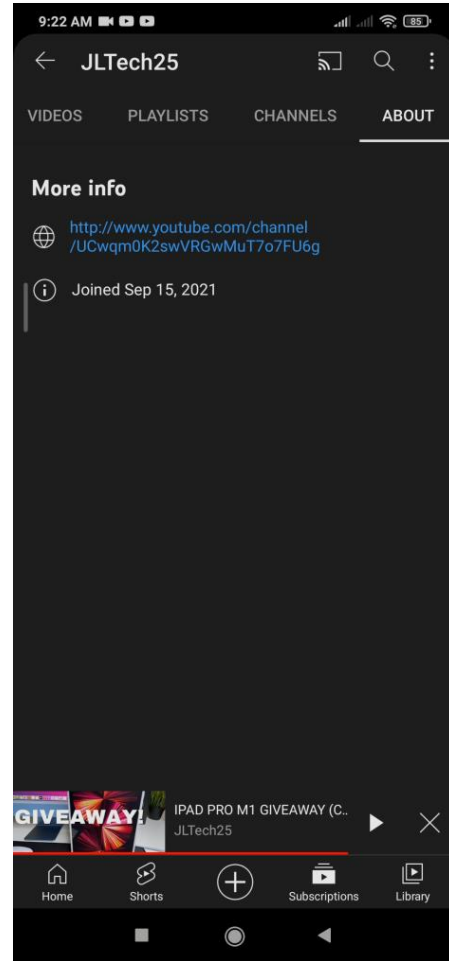
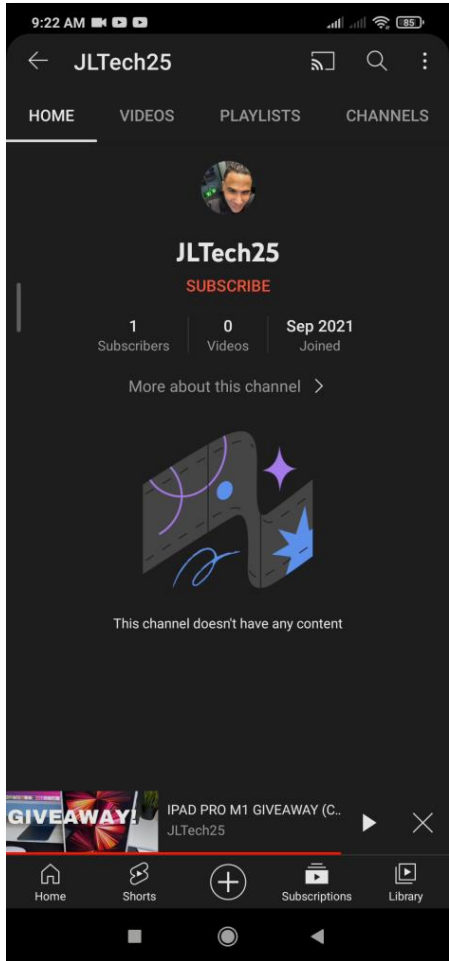


#9



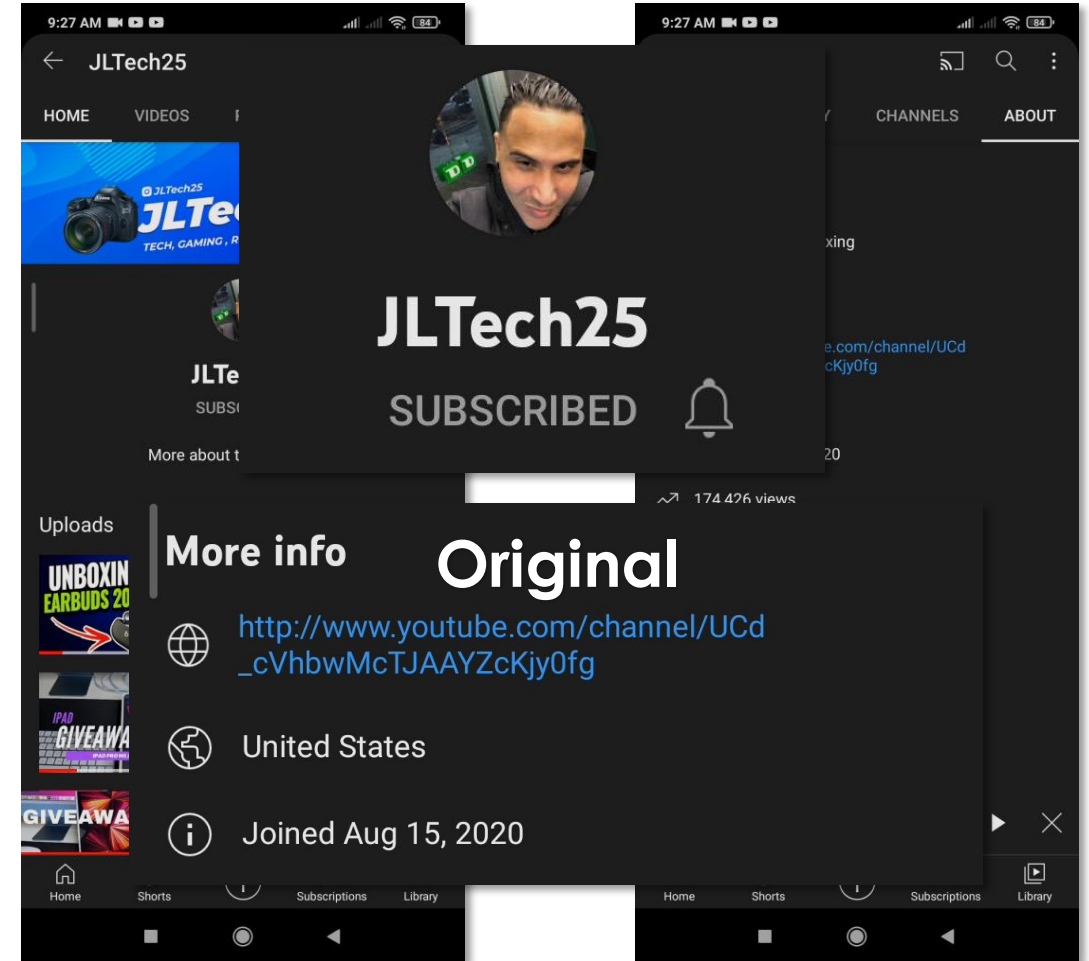
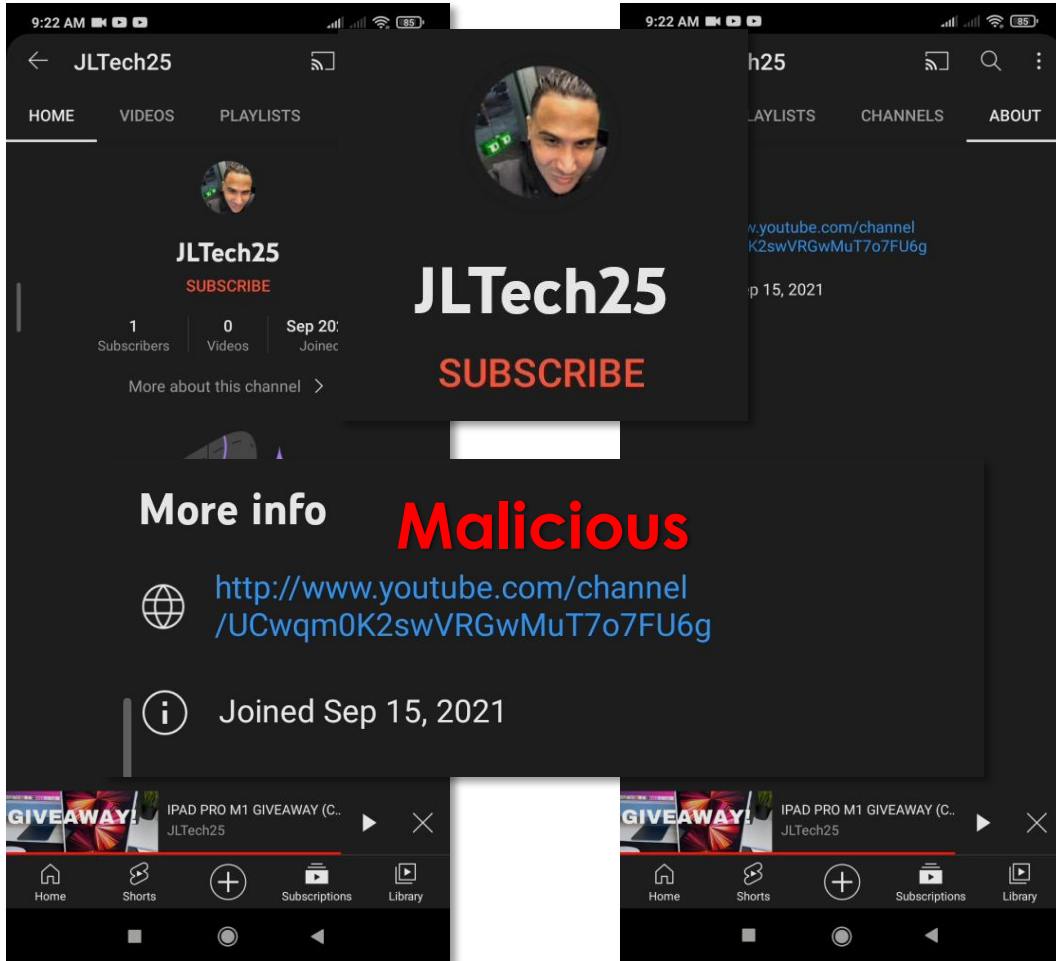
Use Case: Incident on September 15, 2021

Side-by-side comparison of malicious channel & original channel

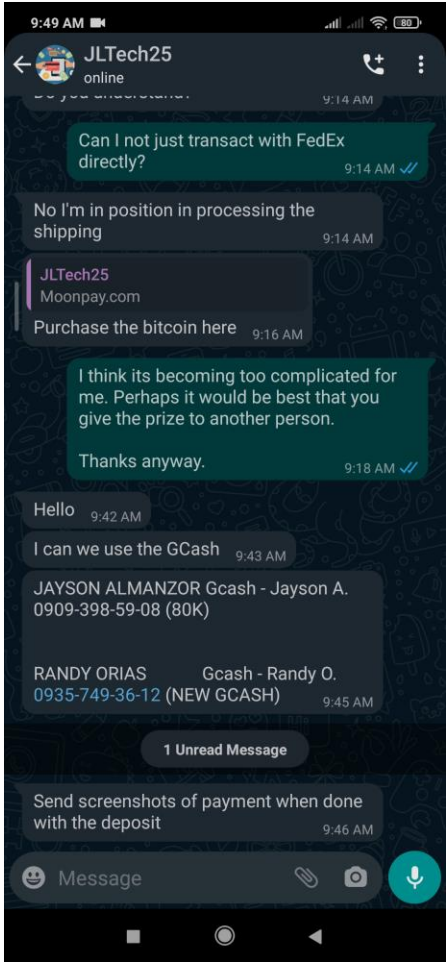
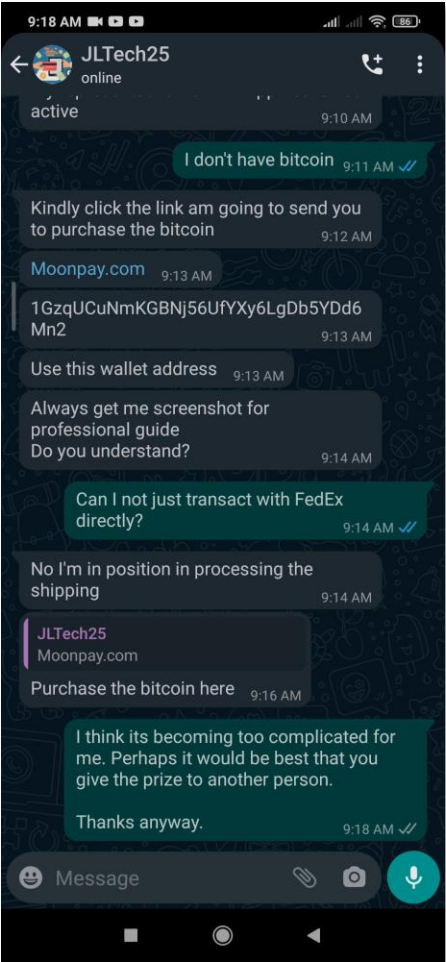


Use Case: Incident on September 15, 2021

Side-by-side comparison of malicious channel & original channel



Scammer details obtained during WhatsApp Conversation – They were coercing my father to send them \$140 for “shipping fees” via FedEx

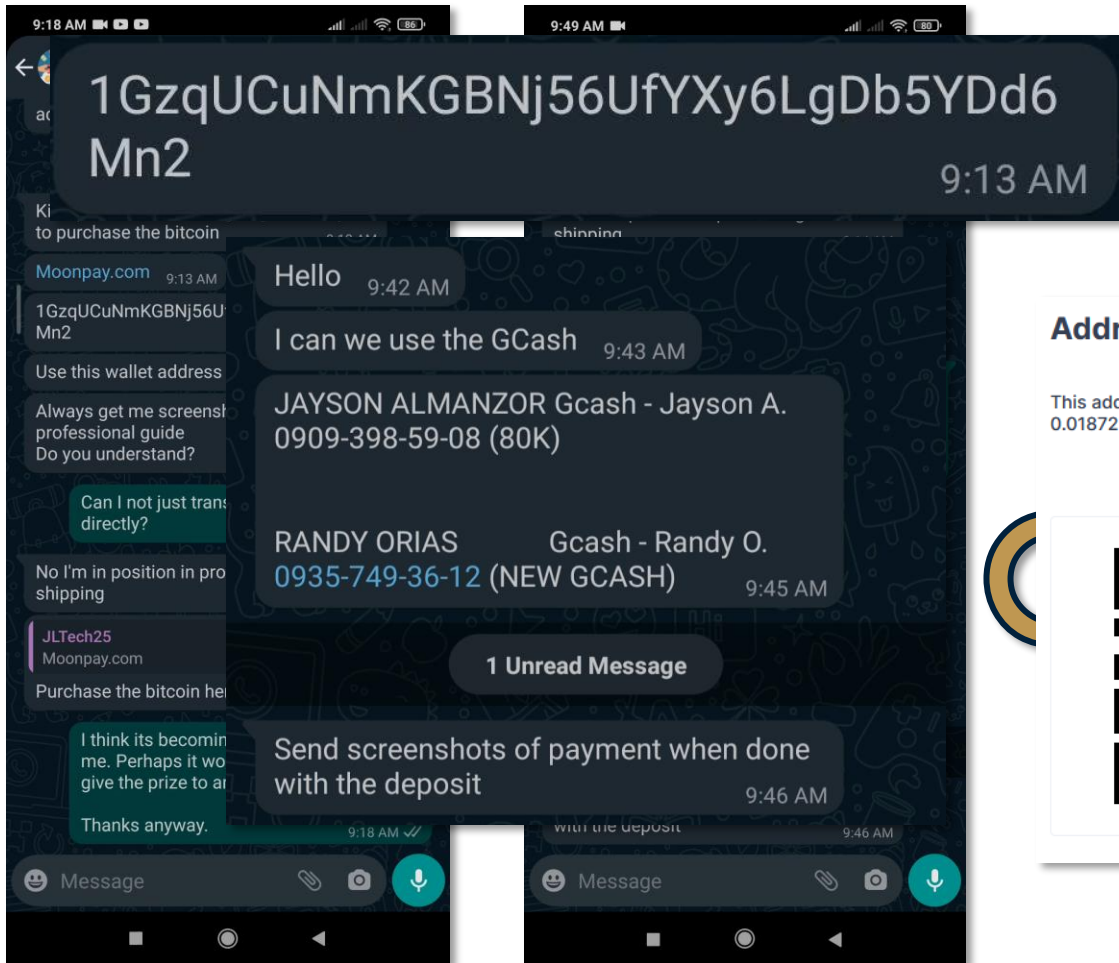


Scammer details obtained during WhatsApp Conversation – They were coercing my father to send them \$140 for “shipping fees” via FedEx

Unfortunately, it seems they were already able to steal 0.01872224 BTC (\$828.71 at the time)

Link:

<https://www.blockchain.com/btc/address/1GzqUCuNmKGBNj56UfYXy6LgDb5YDd6Mn2>



Address

USD BTC

This address has transacted 13 times on the Bitcoin blockchain. It has received a total of 0.01872224 BTC (\$828.71) and has sent a total of 0.01872224 BTC (\$828.71). The current value of this address is 0.00000000 BTC (\$0.00).



Address	1GzqUCuNmKGBNj56UfYXy6LgDb5YDd6Mn2
Format	BASE58 (P2PKH)
Transactions	13
Total Received	0.01872224 BTC
Total Sent	0.01872224 BTC
Final Balance	0.00000000 BTC



The End

Solution:

Validate YouTube Channel Name



Solution:

Validate YouTube Channel Name

Google already validates usernames for new email registrations, why not apply the same checks to YouTube Channels?



Solution:

Validate YouTube Channel Name

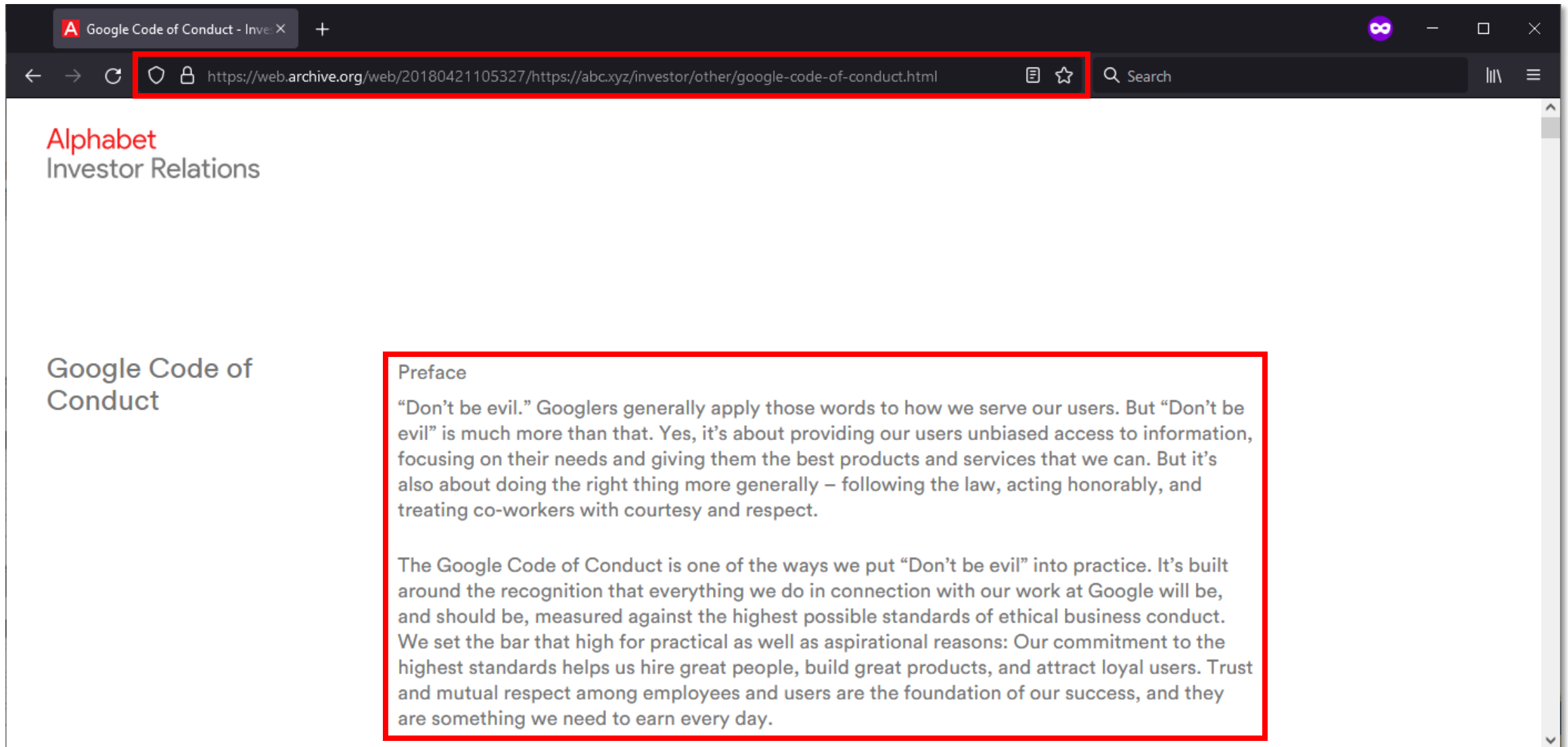
Google already validates usernames for new email registrations, why not apply the same checks to YouTube Channels?

Question:

Why does Google allow impersonation of YouTube Channels?



Google Code of Conduct – 2017



The screenshot shows a web browser window with a dark theme. The address bar is highlighted in red and contains the URL: <https://web.archive.org/web/20180421105327/https://abc.xyz/investor/other/google-code-of-conduct.html>. The page content includes the "Alphabet Investor Relations" logo and the title "Google Code of Conduct". A red box highlights the "Preface" section, which contains the following text:

Preface

“Don’t be evil.” Googlers generally apply those words to how we serve our users. But “Don’t be evil” is much more than that. Yes, it’s about providing our users unbiased access to information, focusing on their needs and giving them the best products and services that we can. But it’s also about doing the right thing more generally – following the law, acting honorably, and treating co-workers with courtesy and respect.

The Google Code of Conduct is one of the ways we put “Don’t be evil” into practice. It’s built around the recognition that everything we do in connection with our work at Google will be, and should be, measured against the highest possible standards of ethical business conduct. We set the bar that high for practical as well as aspirational reasons: Our commitment to the highest standards helps us hire great people, build great products, and attract loyal users. Trust and mutual respect among employees and users are the foundation of our success, and they are something we need to earn every day.



Google Code of Conduct – 2017

The screenshot shows a web browser window with a dark theme. The address bar is highlighted with a red box and contains the URL: <https://web.archive.org/web/20180421105327/https://abc.xyz/investor/other/google-code-of-conduct.html>. The page content includes:

Bribery and Government Ethics Policy. Carefully follow the limits and prohibitions described there, and obtain any required pre-approvals. If after consulting the Policy you aren't sure what to do, ask Ethics & Compliance.

VIII. Conclusion

Google aspires to be a different kind of company. It's impossible to spell out every possible ethical scenario we might face. Instead, we rely on one another's good judgment to uphold a high standard of integrity for ourselves and our company. We expect all Googlers to be guided by both the letter and the spirit of this Code. Sometimes, identifying the right thing to do isn't an easy call. If you aren't sure, don't be afraid to ask questions of your manager, Legal or Ethics & Compliance.

And remember... don't be evil, and if you see something that you think isn't right – speak up!

Last updated October 12, 2017

Alphabet



Google Code of Conduct – 2021

Alphabet
Investor Relations

Google Code of Conduct

The Google Code of Conduct is one of the ways we put Google’s values into practice. It’s built around the recognition that everything we do in connection with our work at Google will be, and should be, measured against the highest possible standards of ethical business conduct. We set the bar that high for practical as well as aspirational reasons: Our commitment to the highest standards helps us hire great people, build great products, and attract loyal users. Respect for our users, for the opportunity, and for each other are foundational to our success, and are something we need to support every day.

So please do read the Code and Google’s values, and follow both in spirit and letter, always bearing in mind that each of us has a personal responsibility to incorporate, and to encourage other Googlers to incorporate, the principles of the Code and values into our work. And if you have a question or ever think that one of your fellow Googlers or the company as a whole may be falling short of our commitment, don’t be silent. We want – and need – to hear from you.

Who Must Follow Our Code?

We expect all of our employees and Board members to know and follow the Code. Failure to do so can result in disciplinary action, including termination of employment. Moreover, while the



Google Code of Conduct – 2021

to do, ask Ethics & Compliance.

VIII. Conclusion

Google aspires to be a different kind of company. It's impossible to spell out every possible ethical scenario we might face. Instead, we rely on one another's good judgment to uphold a high standard of integrity for ourselves and our company. We expect all Googlers to be guided by both the letter and the spirit of this Code. Sometimes, identifying the right thing to do isn't an easy call. If you aren't sure, don't be afraid to ask questions of your manager, Legal or Ethics & Compliance.

And remember... don't be evil, and if you see something that you think isn't right – speak up!

Last updated September 25, 2020

[Back to top](#)

Alphabet

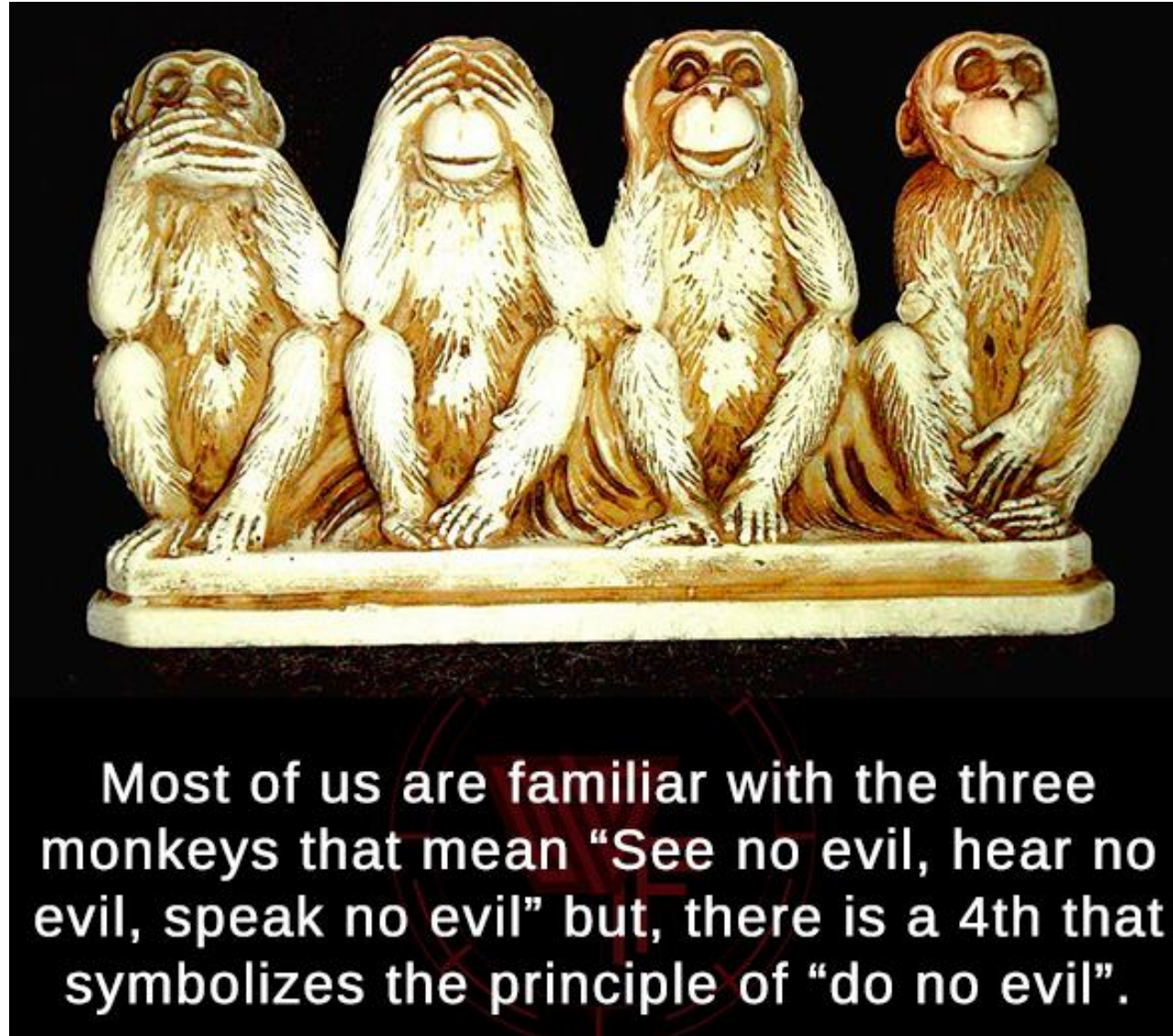


If you are neutral in situations of injustice, you have chosen the side of the oppressor.

- Desmond Tutu



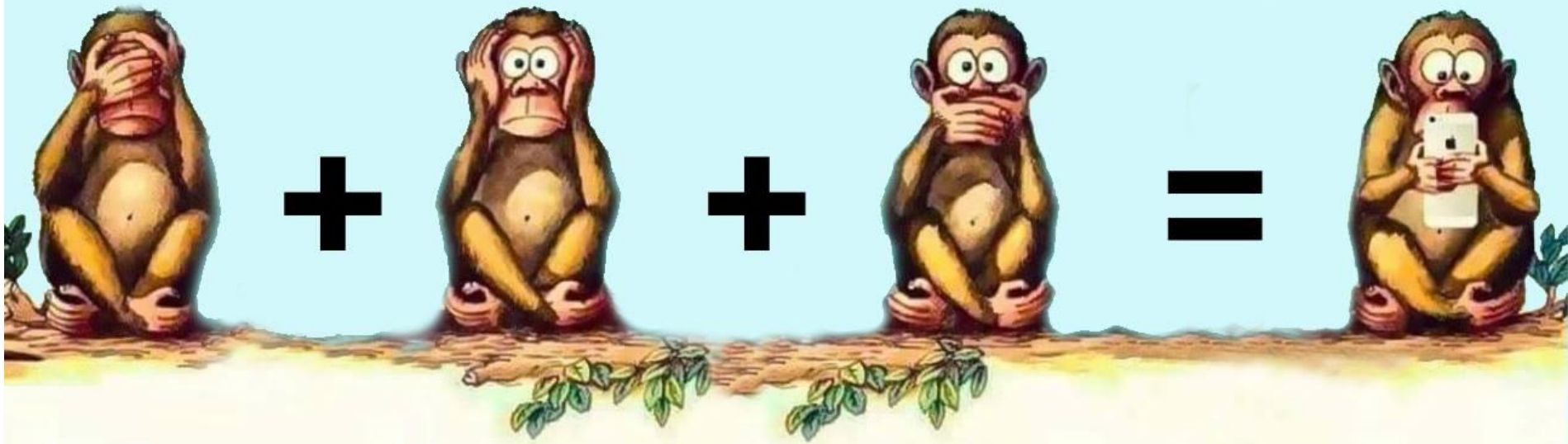
Complexity of Online Security / Safety



Most of us are familiar with the three monkeys that mean “See no evil, hear no evil, speak no evil” but, there is a 4th that symbolizes the principle of “do no evil”.

Finally the **fourth** ape!

“He sees **nobody**, hears **nobody** and speaks to **nobody**.”



See memes happen in real life



InfoSec people



Noooo!!!!
Do not open *invoice.exe*

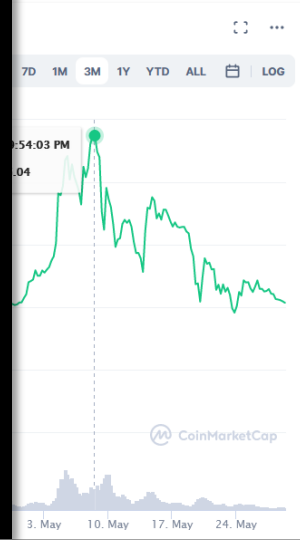
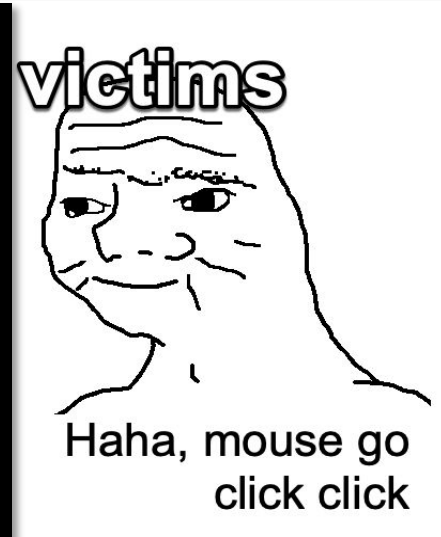
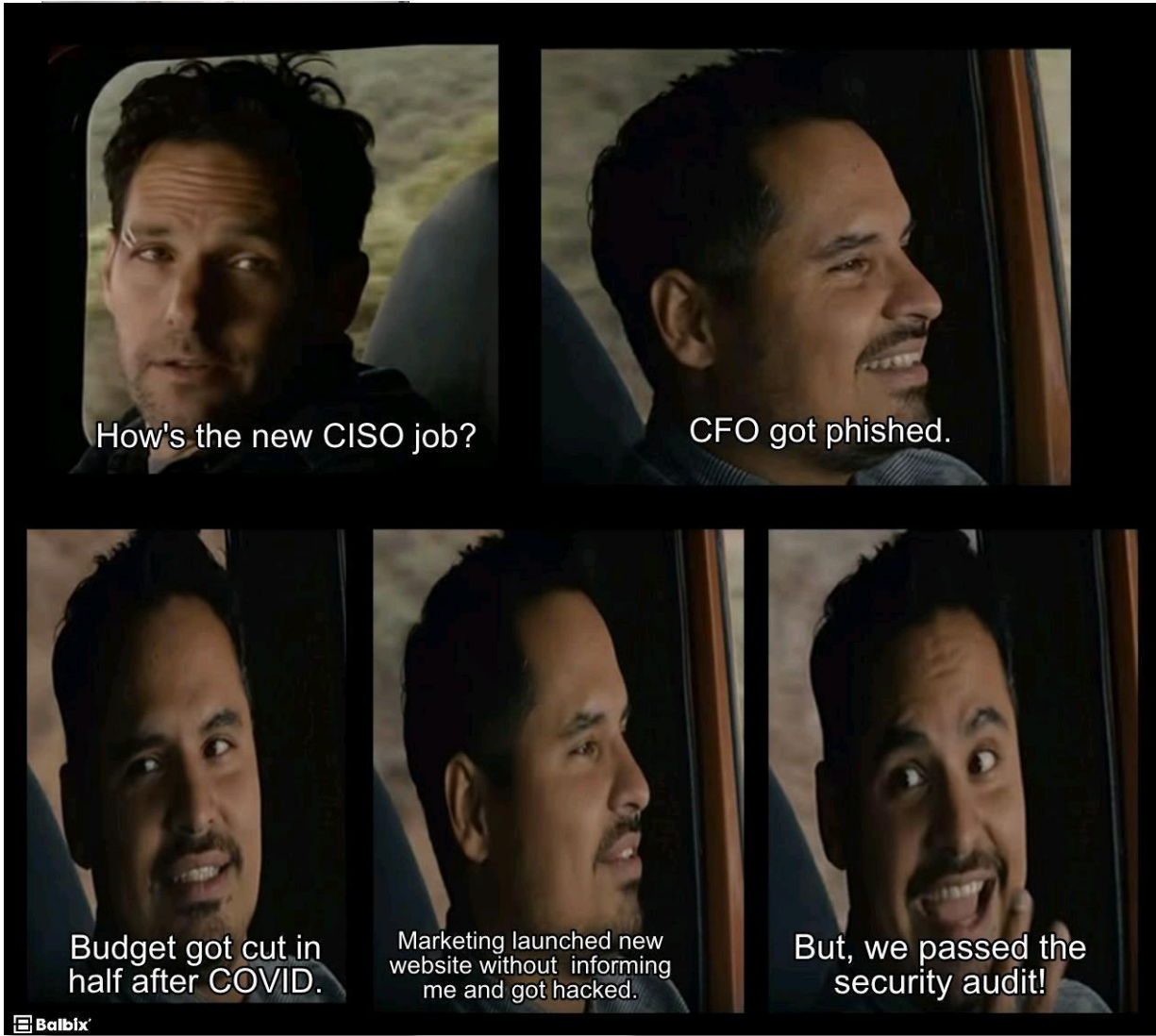
victims



Haha, mouse go
click click



See memes happen in real life



See memes happen in real life



See memes happen in real life



See memes happen in real life

Microsoft Security @msftsec... · 14h ...
Tell us you work in security without telling us you work in security.
690 replies 270 retweets 687 likes

IT Spook @IT_Spook
Replying to @msftsecurity
I drink heavily and weep for the future of humanity on a daily basis.
3:31 am · 3/2/21 · Twitter for iPhone



See memes happen in real life



A screenshot of a Twitter thread. At the top is the profile of Microsoft Security (@msftsec...), which includes the Windows logo and a verified badge. The tweet text reads: "Tell us you work in security without telling us you work in security." Below the text are icons for replies (690), retweets (270), likes (687), and a share icon. Below this is a reply from IT Spook (@IT_Spook) with a profile picture of a black bat silhouette. The reply text says: "Replying to @msftsecurity" and "I drink heavily and weep for the future of humanity on a daily basis." At the bottom of the screenshot, it shows the time "3:31 am · 3/2/21" and "Twitter for iPhone". A small "Balbix" logo is visible in the bottom left corner of the screenshot.



Phishing Awareness: Dealing with Phishing as an individual

Personal Opinion:
Words do not really protect people
Action speak louder than words

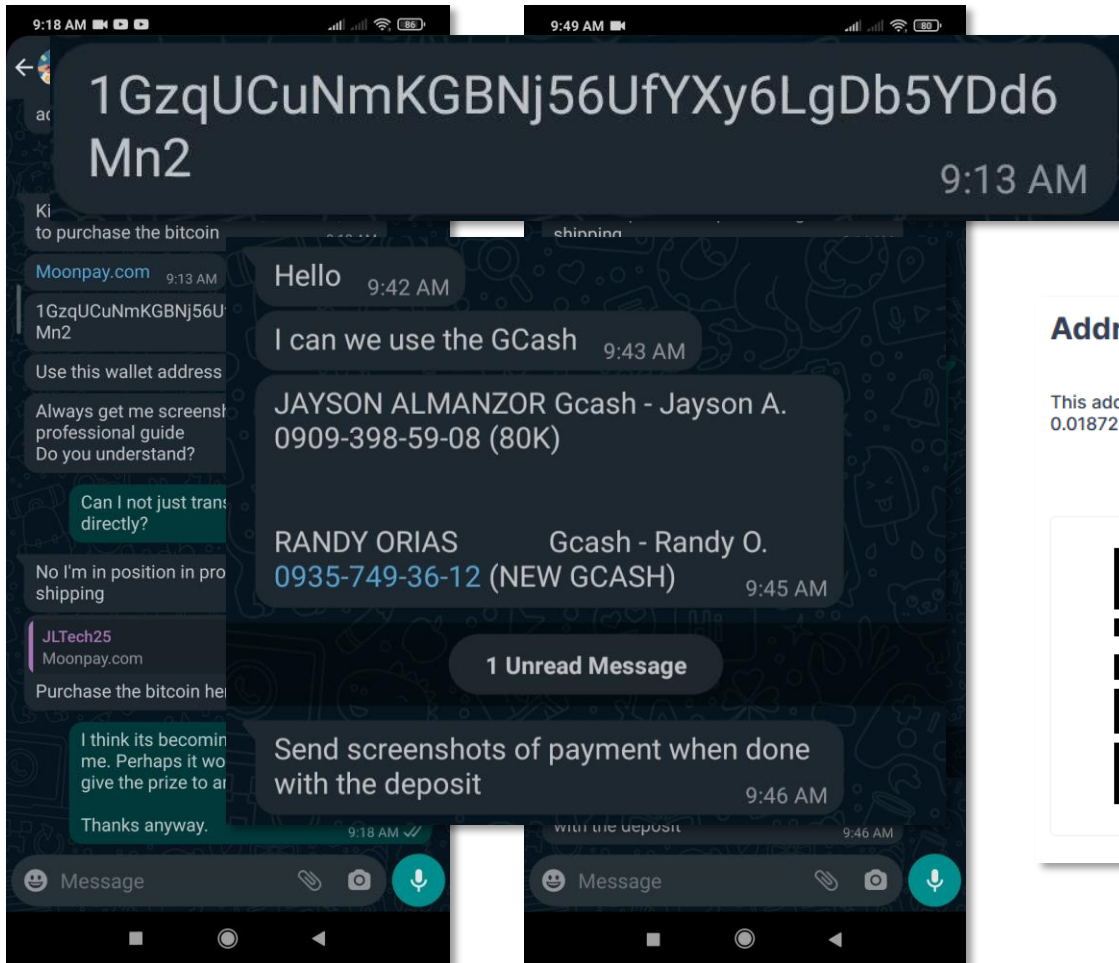


Scammer details obtained during WhatsApp Conversation – They were coercing my father to send them \$140 for “shipping fees” via FedEx

Unfortunately, it seems they were already able to steal 0.01872224 BTC (\$828.71 at the time)

Link:

<https://www.blockchain.com/btc/address/1GzqUCuNmKGBNj56UfYXy6LgDb5YDd6Mn2>



Address

USD BTC

This address has transacted 13 times on the Bitcoin blockchain. It has received a total of 0.01872224 BTC (\$828.71) and has sent a total of 0.01872224 BTC (\$828.71). The current value of this address is 0.00000000 BTC (\$0.00).



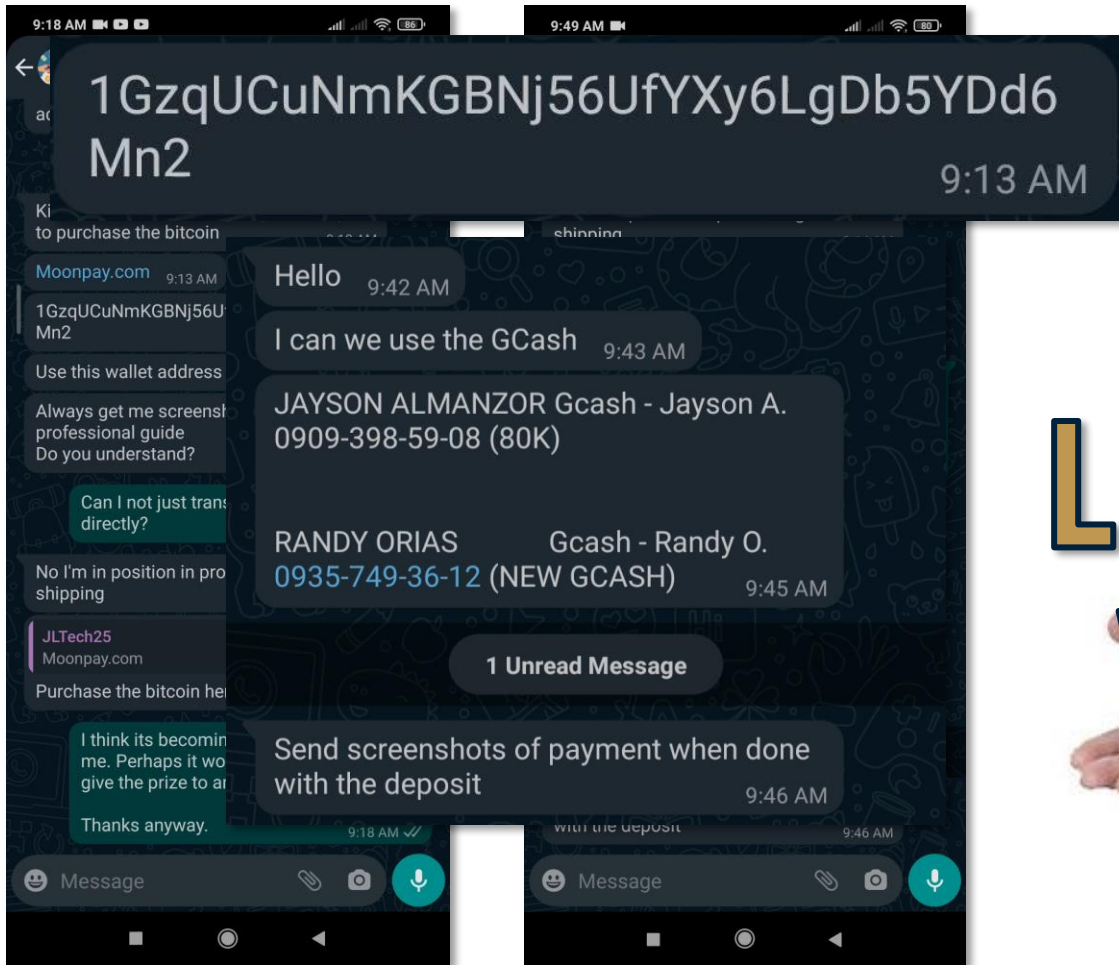
Address	1GzqUCuNmKGBNj56UfYXy6LgDb5YDd6Mn2
Format	BASE58 (P2PKH)
Transactions	13
Total Received	0.01872224 BTC
Total Sent	0.01872224 BTC
Final Balance	0.00000000 BTC

Scammer details obtained during WhatsApp Conversation – They were coercing my father to send them \$140 for “shipping fees” via FedEx

Unfortunately, it seems they were already able to steal 0.01872224 BTC (\$828.71 at the time)

Link:

<https://www.blockchain.com/btc/address/1GzqUCuNmKGBNj56UfYXy6LgDb5YDd6Mn2>



Personal Opinion:
***We all use the same technology but come
from different perspectives***



Phishing Awareness: Dealing with Phishing as an individual

From an ordinary person's perspective:

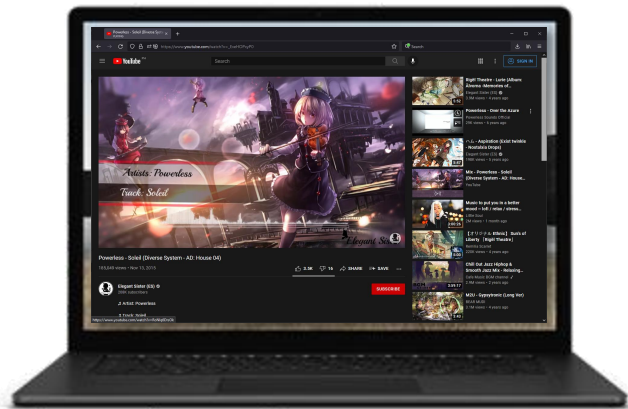
- *Device (Laptop, Mobile, Tablet, etc.)*
- *Browser (Internet Explorer, Chrome, Firefox, etc.)*
- *Applications (Facebook, YouTube, Gmail, Outlook, etc.)*



Phishing Awareness: Dealing with Phishing as an individual

From an ordinary person's perspective:

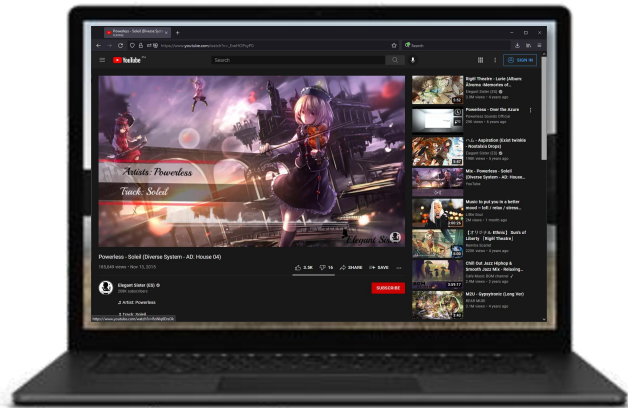
- *Device (Laptop, Mobile, Tablet, etc.)*
- *Browser (Internet Explorer, Chrome, Firefox, etc.)*
- *Applications (Facebook, YouTube, Gmail, Outlook, etc.)*



Phishing Awareness: Dealing with Phishing as an individual

From an ordinary person's perspective:

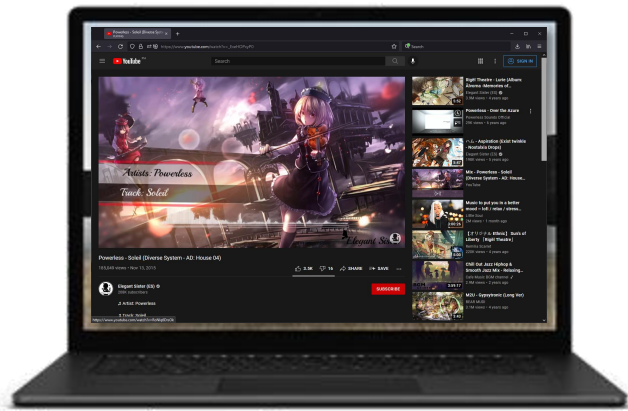
- **Device (Laptop, Mobile, Tablet, etc.)**
- **Browser (Internet Explorer, Chrome, Firefox, etc.)**
- **Applications (Facebook, YouTube, Gmail, Outlook, etc.)**



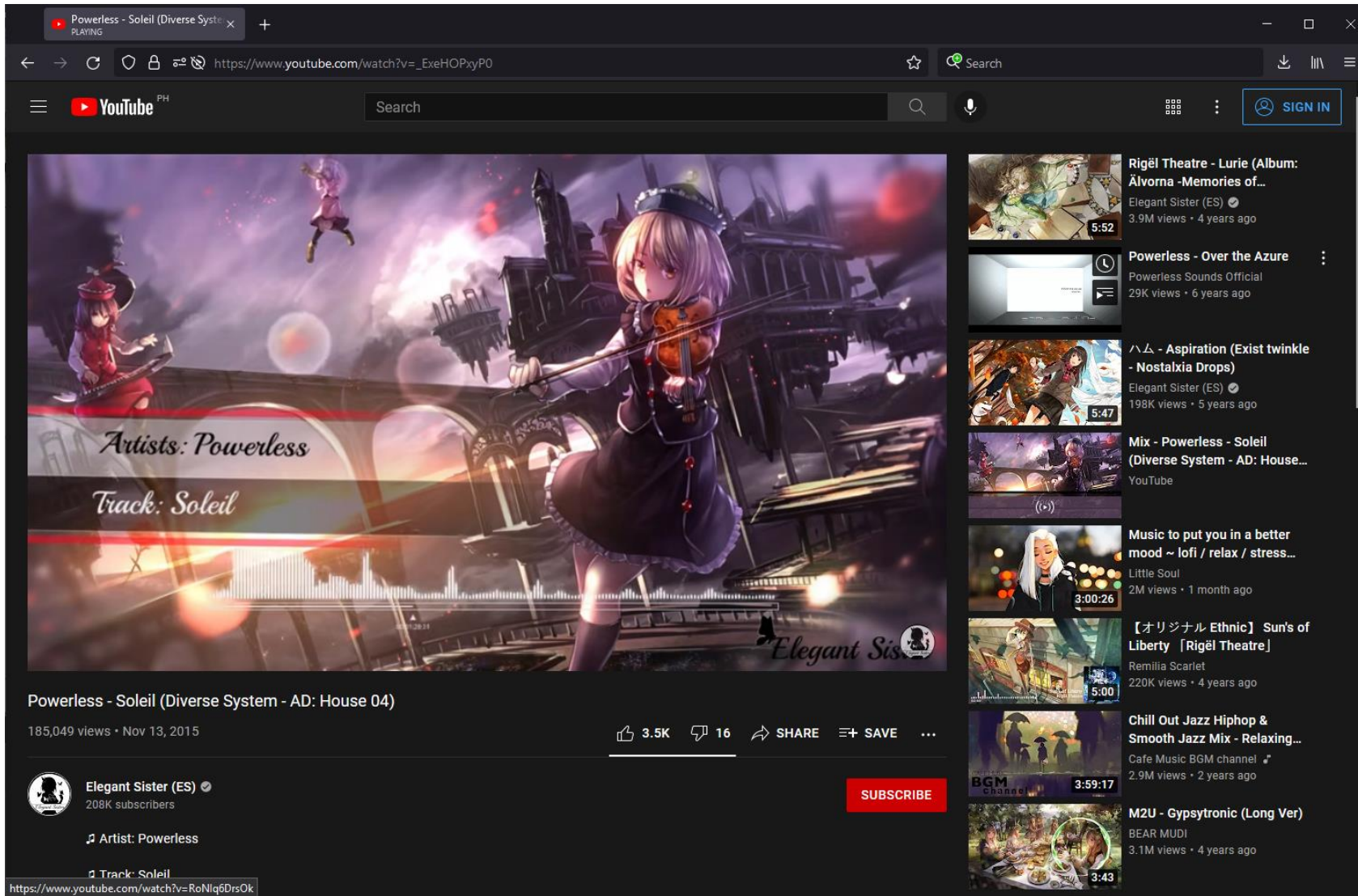
Phishing Awareness: Dealing with Phishing as an individual

From an ordinary person's perspective:

- **Device (Laptop, Mobile, Tablet, etc.)**
- **Browser (Internet Explorer, Chrome, Firefox, etc.)** – This is also an application
- **Applications (Facebook, YouTube, Gmail, Outlook, etc.)**



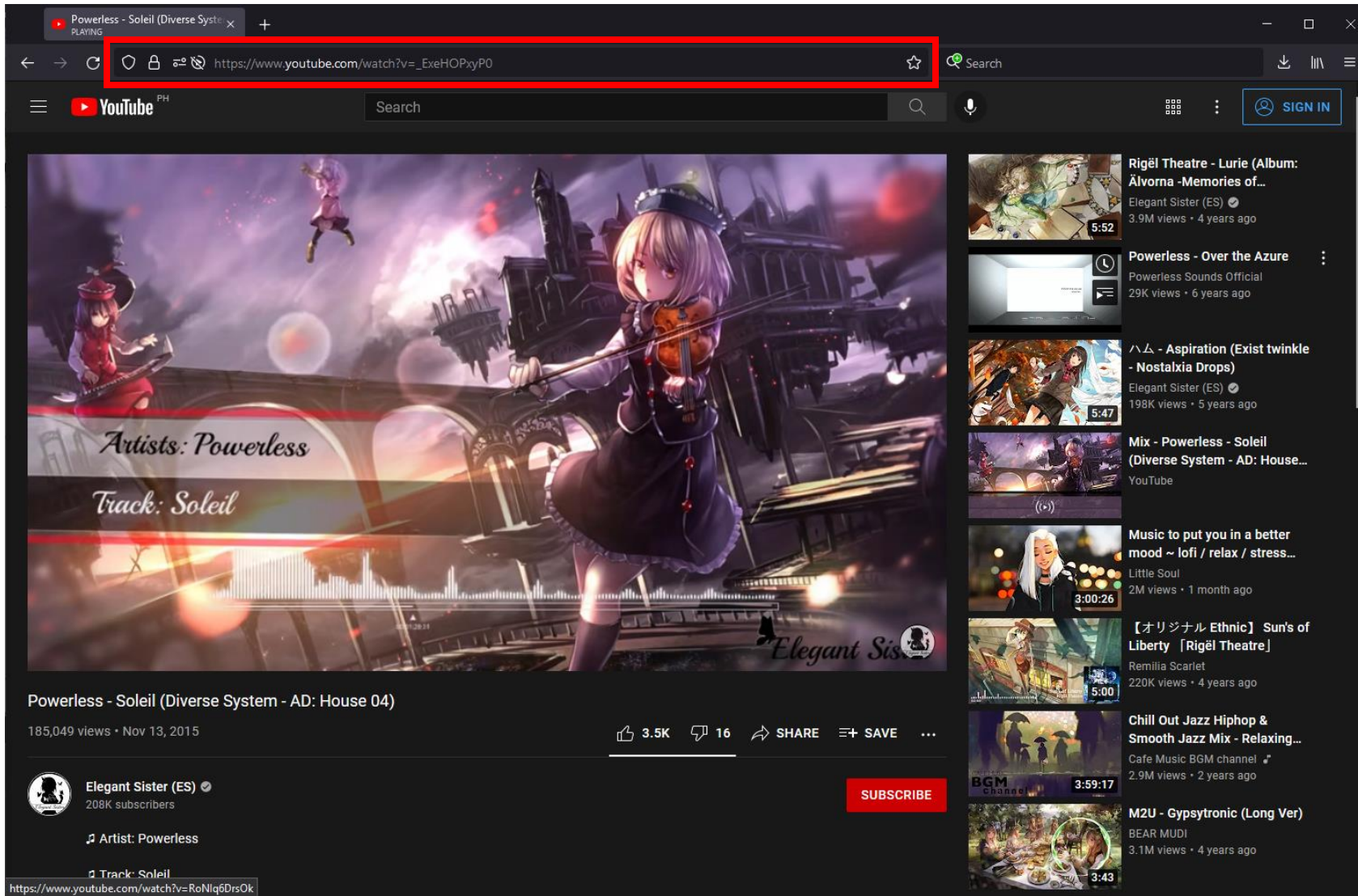
Phishing Awareness: Dealing with Phishing as an individual



Web browser: Firefox
Application: YouTube



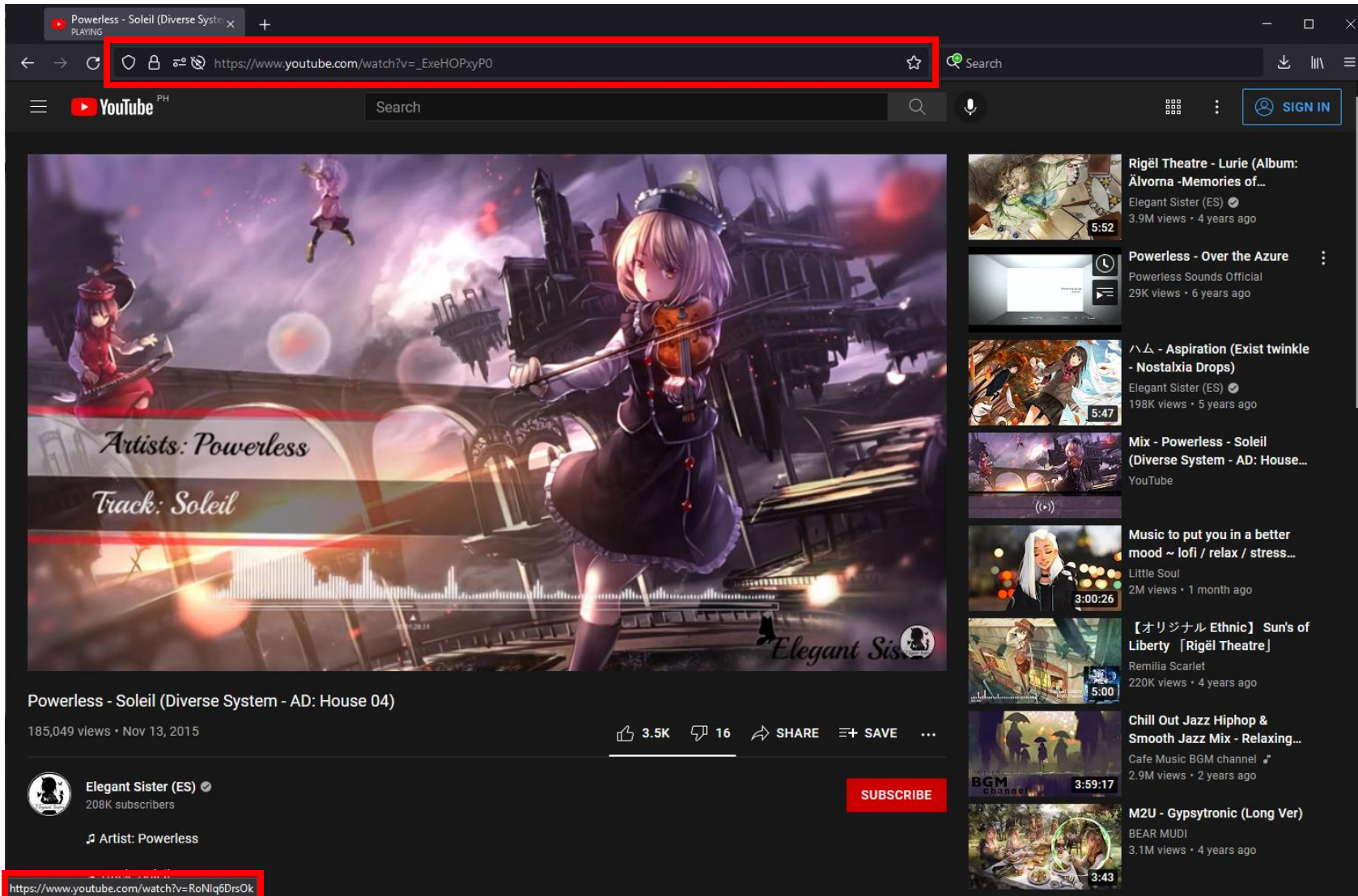
Phishing Awareness: Dealing with Phishing as an individual



Web browser: Firefox
Application: YouTube



Phishing Awareness: Dealing with Phishing as an individual



Web browser: Firefox
Application: YouTube



Phishing Awareness: Dealing with Phishing as an individual

Web browser: Firefox
Application: YouTube

URL

Artists: Powerless
Track: Soleil

Powerless - Soleil (Diverse System - AD: House 04)
185,049 views · Nov 13, 2015

<https://www.youtube.com/watch?v=RoNlq6DrsOk>

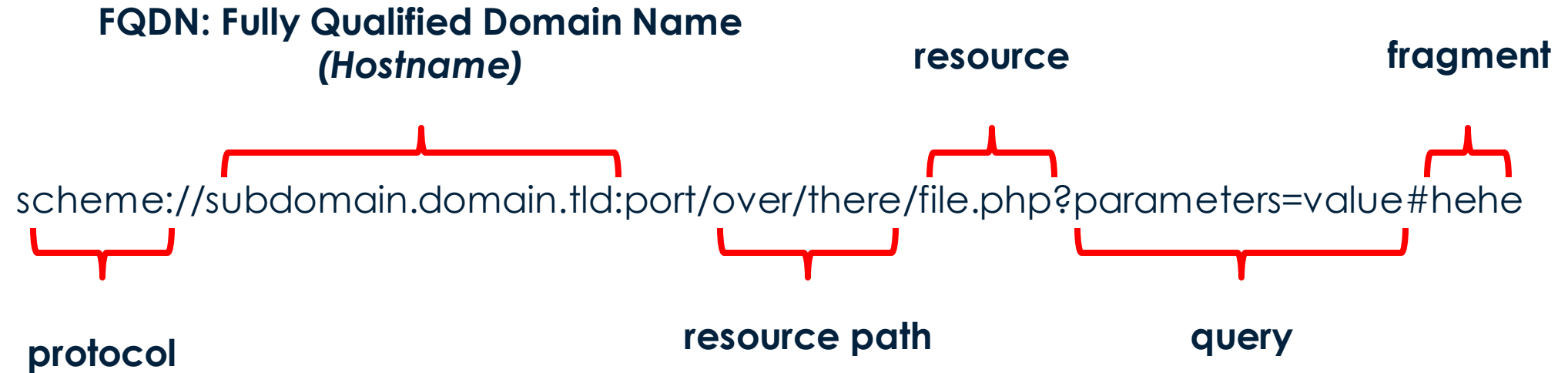
Artist: Powerless

<https://www.youtube.com/watch?v=RoNlq6DrsOk>



Phishing Awareness: Uniform Resource Locator (URL)

RFC 1738 – Uniform Resource Locator Components



Phishing Awareness: Uniform Resource Locator (URL)

RFC 1738 – Uniform Resource Locator Components

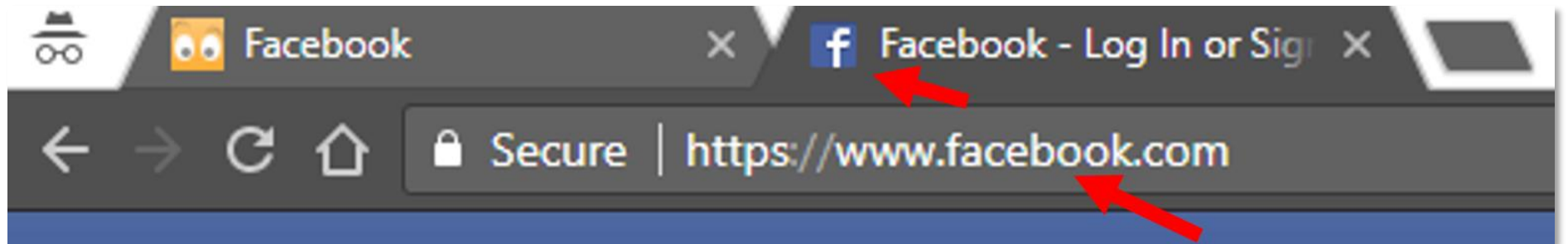
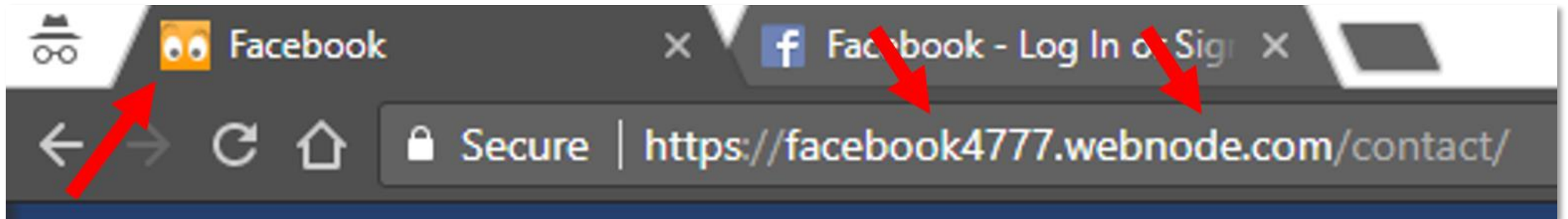
<https://cogia.edu.ph.cutedalmatianpuppies.ml/e.php?e=admin@cogia.edu.ph>

When determining a **phishing** page, always look at the portion of the **URL** right **before** the resource path **SLASH (/)**



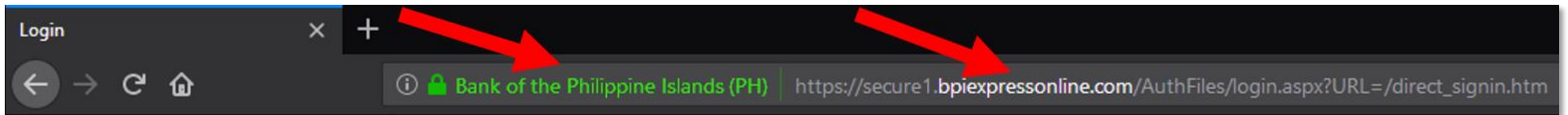
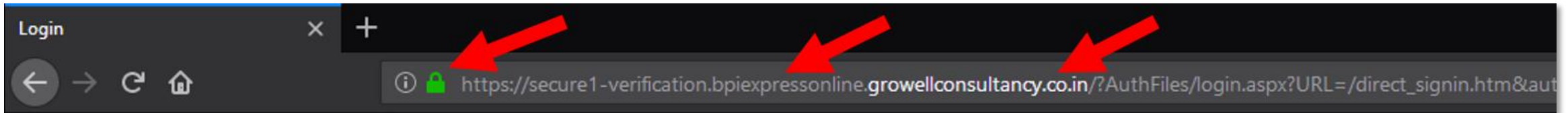
Phishing Awareness: Uniform Resource Locator (URL)

Phishing in 2018



Phishing Awareness: Uniform Resource Locator (URL)

Phishing in 2018



Phishing Awareness: Uniform Resource Locator (URL)

Phishing in 2018

20 Real life examples of Punycode with big brands

Wandera's Zero-day phishing research has been identifying Punycode attacks since 2017. We've seen a 250% increase in the number of Punycode domains over the last 12 months:

Brand	What the user sees	The Punycode
Adidas	adidas.de	http://xn--addas-o4a.de/
Aerlingus	aerlingus.com	xn--aerlngus-j80d.com
Aerlingus	aerlingus.com	xn--aelngus-of0d.com
Air France	airfrance.com	xn--airfrnce-rx0d.com
British Airways	britishairways.com	xn--britishairays-541g.com
British Airways	britishairways.com	xn--britishirways-of2g.com
Google	google.com	xn--googe-95a.com
Haribo	haribo.com	xn--harbo-p4a.com

1. Instagram Lookalike Domains

At first glance, the domains below are the same as `instagram[.]com`, with only one using the `.xyz` generic TLD (gTLD). But if you look closely, you will see non-Latin characters in some of the domains in the mix. We included their respective IDN versions obtained using Punycode for comparison.

- `instagram[.]com` (`xn--instagram-7pb[.]com`)
- `instagram[.]com` (`xn--nstagram-s29c[.]com`)
- `instagram[.]com` (`xn--instaram-tgb[.]com`)
- `instagram[.]com` (`xn--instagra-o89c[.]com`)
- `instagram[.]com` (`xn--instaram-3sd[.]com`)

References:

- <https://www.wandera.com/punycode-attacks/>
- <https://cybersecurityventures.com/beware-of-lookalike-domains-in-punycode-phishing-attacks/>



Phishing Awareness: Uniform Resource Locator (URL)

Phishing in 2018

Before (punycode ì)

Set Firefox config to show punycode

Preference Name	Status	Type	Value
network.IDN_show_punycode	modified	boolean	true
network.standard-url.punycode-host	default	boolean	true

After

xn--polonex-3ya.com

References:

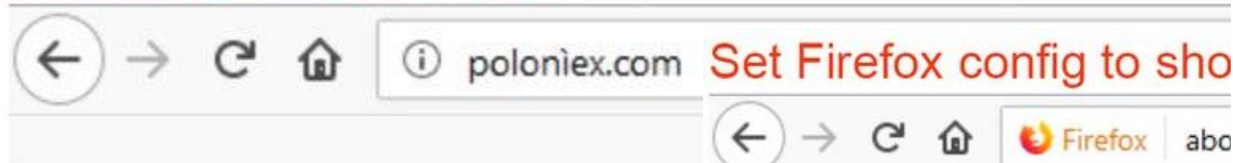
- <https://mobile.twitter.com/MickD/status/965610955366387712> (deleted tweet? ldk)
- <https://discourse.world/h/2018/01/22/Phishing-with-characters-from-other-layouts-in-the-URL-does-not-go-away>



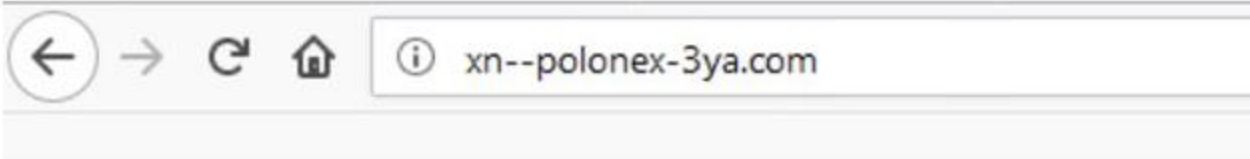
Phishing Awareness: Uniform Resource Locator (URL)

Phishing in 2018

Before (punycode i)



After

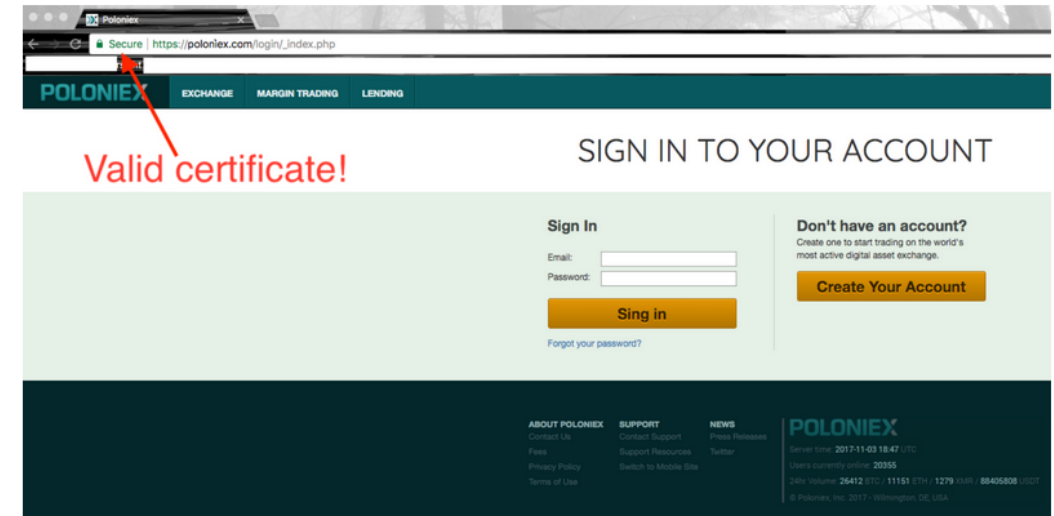


ivansychev January 22, 2018 at 09:00

Phishing with characters from other layouts in the URL does not go away

[Information Security](#)

Phishing has been around for a long time. It is impossible to calculate how many people provided passwords from social networks and email services, data of their credit cards and bank accounts to fraudsters on a silver platter, without making sure that it was Vkontakte and not Vkontaktle in the address bar at the time of entering the login and password. One way that you can mask an address is to use characters from other alphabets.



Examples of phishing sites include the poloniex.com page, which copies the cryptocurrency exchange poloniex.com

References:

- <https://mobile.twitter.com/MickD/status/965610955366387712> (deleted tweet? ldk)
- <https://discourse.world/h/2018/01/22/Phishing-with-characters-from-other-layouts-in-the-URL-does-not-go-away>



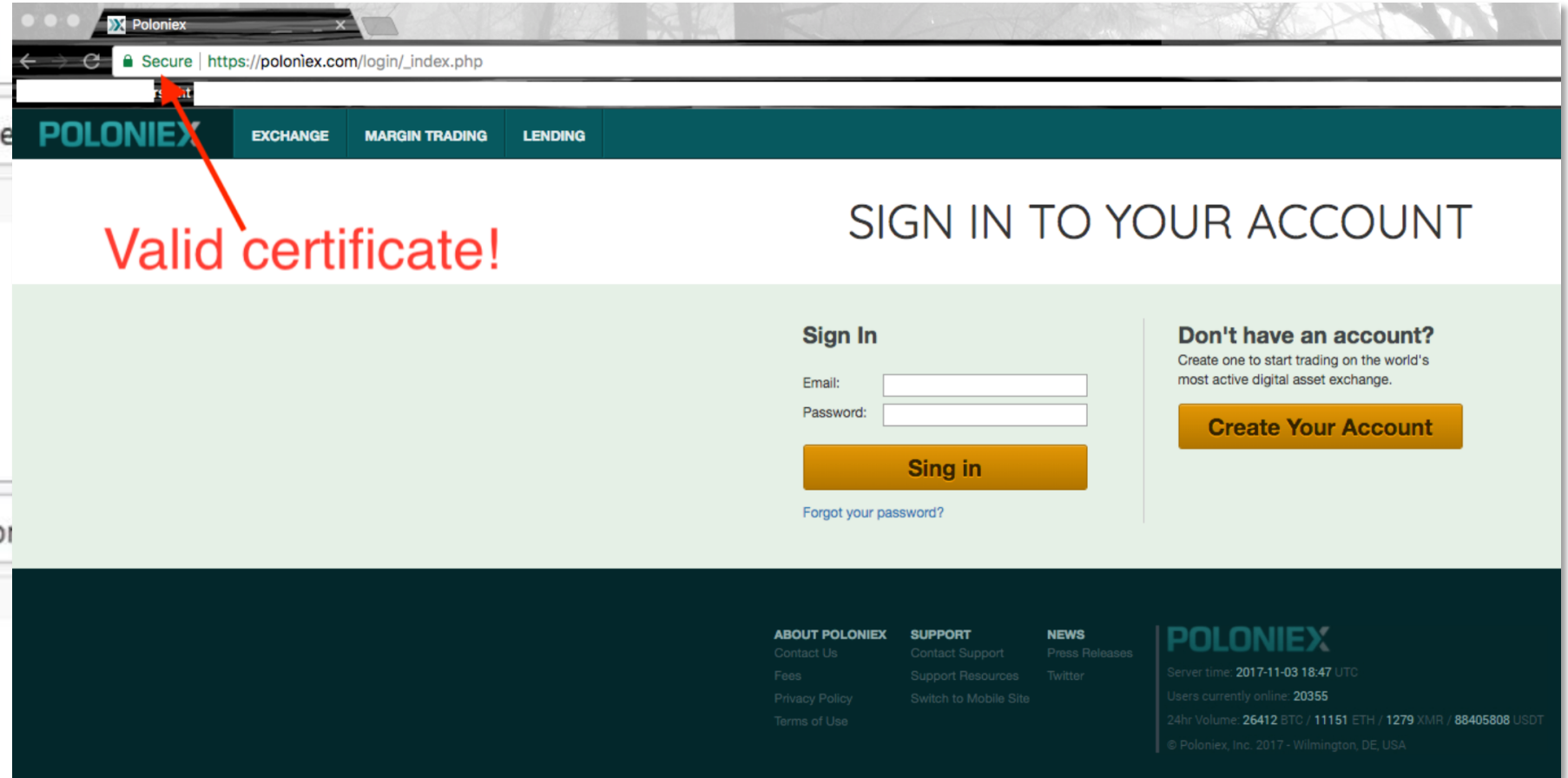
Phishing Awareness: Uniform Resource Locator (URL)

ivansychev January 22, 2018 at 09:00

Phishing with characters from other layouts in the URL does not go away

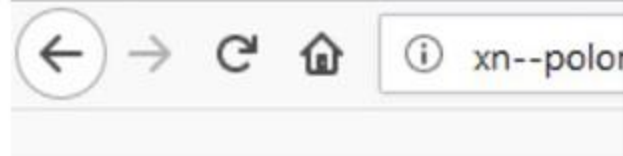
Phishing in 2018

Before (punycode i)



Valid certificate!

After



References:

- <https://mobile.twitter.com/MickD/status/965610955366387712> (deleted tweet? ldk)
- <https://discourse.world/h/2018/01/22/Phishing-with-characters-from-other-layouts-in-the-URL-does-not-go-away>



Phishing Awareness: Uniform Resource Locator (URL)

RFC 1738 – Uniform Resource Locator Components

<https://cogia.edu.ph.cutedalmatianpuppies.ml/e.php?e=admin@cogia.edu.ph>

When determining a **phishing** page, always look at the portion of the **URL** right **before** the resource path **SLASH (/)**



Phishing Awareness: Uniform Resource Locator (URL)

RFC 1738 – Uniform Resource Locator Components

<https://cogia.edu.ph.cutedalmatianpuppies.ml/e.php?e=admin@cogia.edu.ph>

When determining a **phishing** page, always look at the portion of the **URL** right **before** the resource path **SLASH (/)**

Also watch out for *intent*



Phishing Awareness: Dealing with Phishing as an individual

They exploit our vulnerable nature (More brazenly in 2021)

- **Our lack of**
 - *Awareness*
 - *Knowledge*
 - *Discipline*
 - *Self-control*

- **Our vices**
 - *Greed*
 - *Envy*
 - *Impatience*

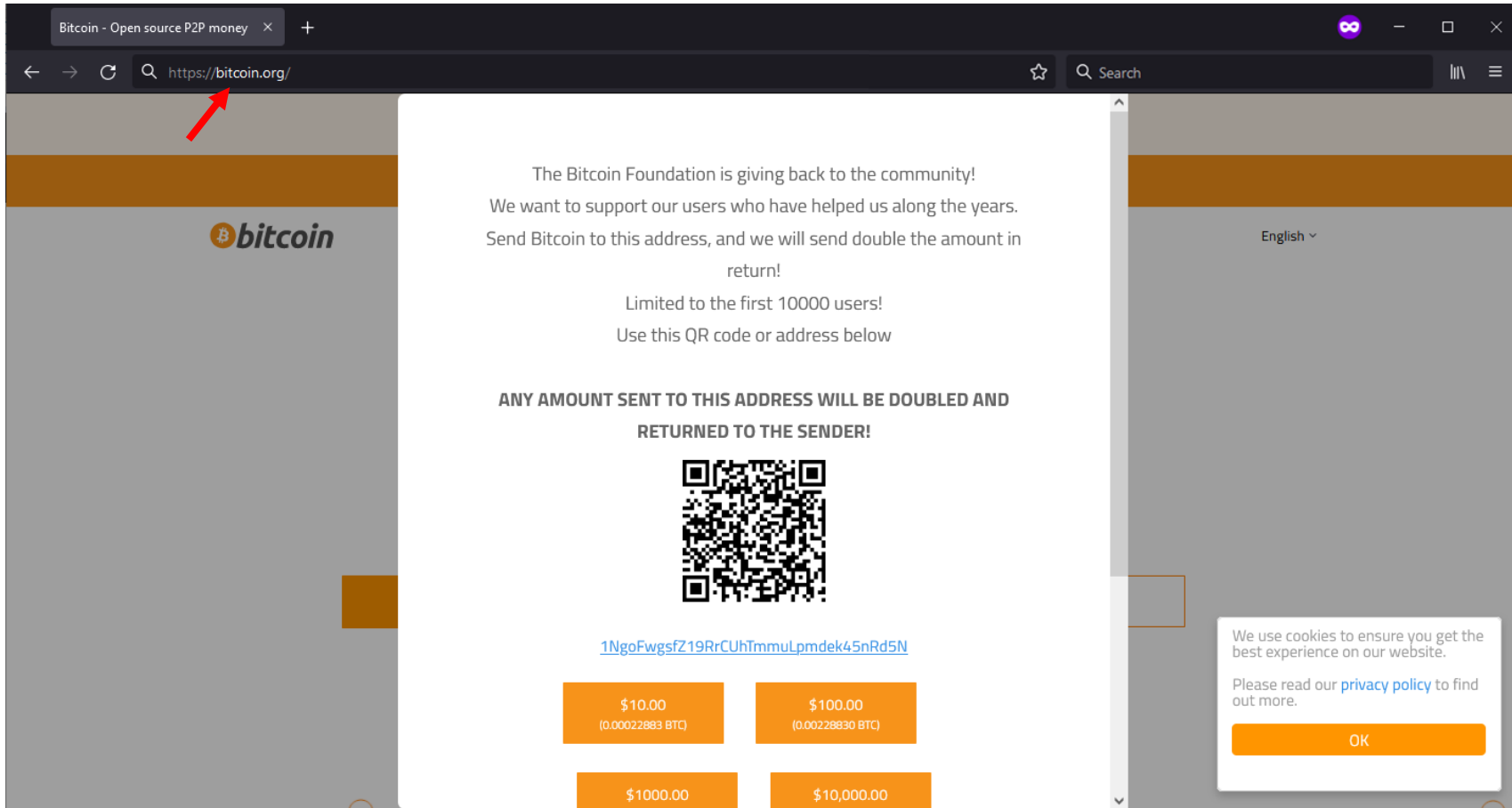
- **Etc.**

- **Our natural desires to**
 - *Help others*
 - *Feel good about ourselves*
 - *Be curious*
 - *Be Independent*



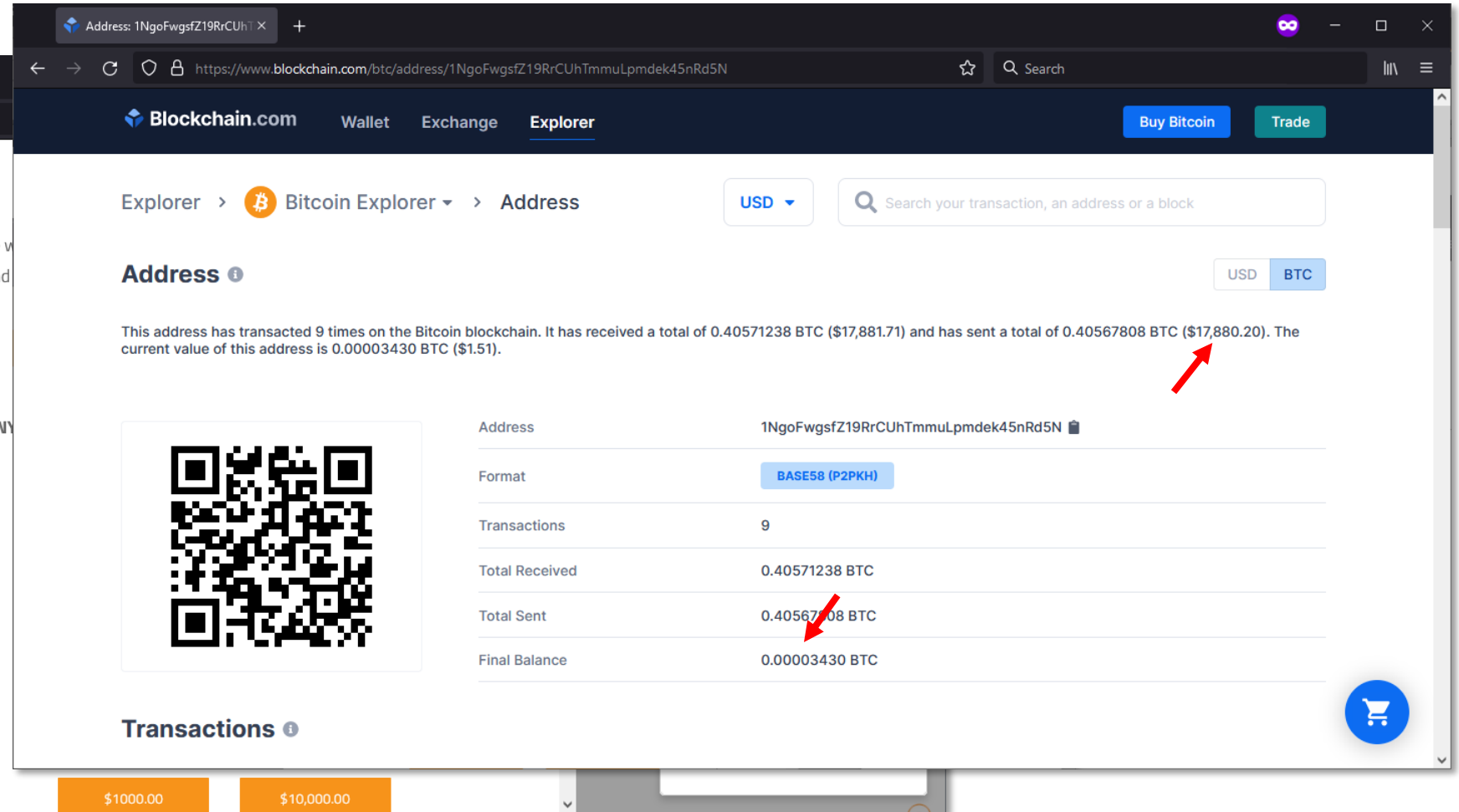
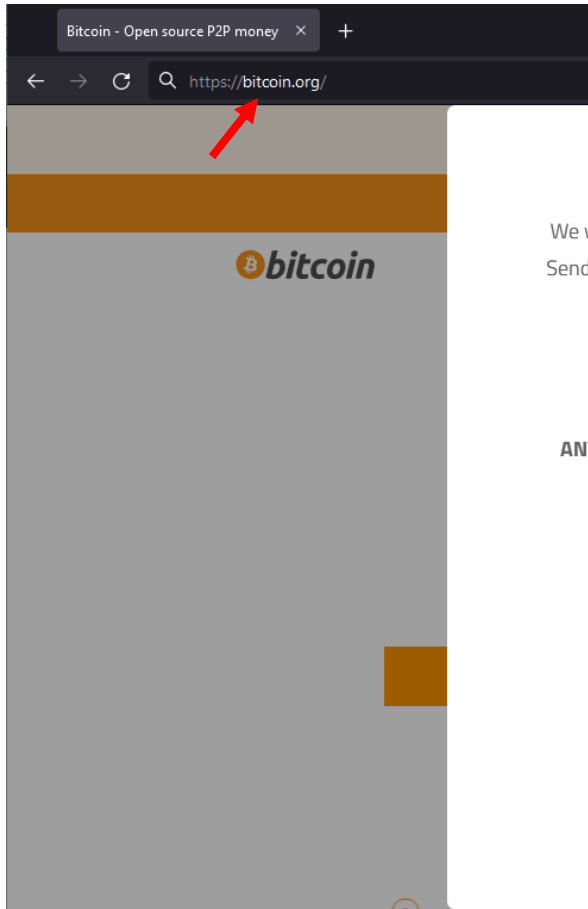
Phishing Awareness: Observing Intent

Phishing in 2021



Phishing Awareness: Observing Intent

Phishing in 2021



Phishing Awareness: Observing Intent

Phishing in 2021

The image shows a browser window with a Bitcoin address: `1NgoFwgsfZ19RrCUhT...`. Below the browser, three tweets are displayed, all promoting a Bitcoin giveaway scam. The Bitcoin address `bc1qxy2kgdygjrqtzq2n0yrf2493p83kkfjhx0wlh` is highlighted in red in each tweet.

Jeff Bezos (@JeffBezos)
Pinned Tweet
I have decided to give back to my community.
All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of \$50,000,000.
`bc1qxy2kgdygjrqtzq2n0yrf2493p83kkfjhx0wlh`
Enjoy!
5:07 PM · Jul 15, 2020 · Twitter Web App
678 Retweets and comments 822 Likes

Elon Musk (@elonmusk)
Elon Musk Retweeted
Feeling grateful, doubling all payments sent to my BTC address!
You send \$1,000, I send back \$2,000!
Only doing this for the next 30 minutes.
`bc1qxy2kgdygjrqtzq2n0yrf2493p83kkfjhx0wlh`
4:27 PM · Jul 15, 2020 · Twitter Web App
2.2K Retweets and comments 5.5K Likes

Bill Gates (@BillGates)
Everyone is asking me to give back, and now is the time.
I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.
BTC Address -
`bc1qxy2kgdygjrqtzq2n0yrf2493p83kkfjhx0wlh`
Only going on for 30 minutes! Enjoy!
4:34 PM · Jul 15, 2020 · Twitter Web App
194 Retweets and comments 389 Likes

Final Balance 0.00003430 BTC

Transactions ⓘ

\$1000.00 \$10,000.00

Reference: <https://www.businessinsider.com/elon-musk-bill-gates-twitter-hacked-bitcoin-crypto-giveaway-scam-2020-7>



Phishing Awareness: Observing Intent

The screenshot shows a Bitcoin Explorer page for the address `bc1qxy2kgdygjr...`. The page displays transaction statistics and a QR code. A Twitter post from Jeff Bezos is overlaid on the left side, containing the same Bitcoin address. A red box highlights the address in both the tweet and the Explorer page. A red arrow points to the 'Total Sent' value in the Explorer page.

Twitter Post:

Pinned Tweet
Jeff Bezos @JeffBezos
I have decided to...
All Bitcoin sent to...
doubled. I am on...
bc1qxy2kgdygjr...
Enjoy!
5:07 PM · Jul 15, 2020
678 Retweets and comments

Blockchain.com Explorer:

Address: bc1qxy2kgdygjr...
Blockchain.com | Wallet | Exchange | Explorer | Buy Bitcoin | Trade

Explorer > Bitcoin Explorer > Address

Address **bc1qxy2kgdygjr...**

This address has transacted 463 times on the Bitcoin blockchain. It has received a total of 12.91845467 BTC (\$568,587.18) and has sent a total of 12.87005839 BTC (\$566,457.09). The current value of this address is 0.04839628 BTC (\$2,130.09).

Address	bc1qxy2kgdygjr...
Format	BECH32 (P2WPKH)
Transactions	463
Total Received	12.91845467 BTC
Total Sent	12.87005839 BTC
Final Balance	0.04839628 BTC

Transactions

Reference: <https://www.businessinsider.com/elon-musk-bill-gates-twitter-hacked-bitcoin-crypto-giveaway-scam-2020-7>

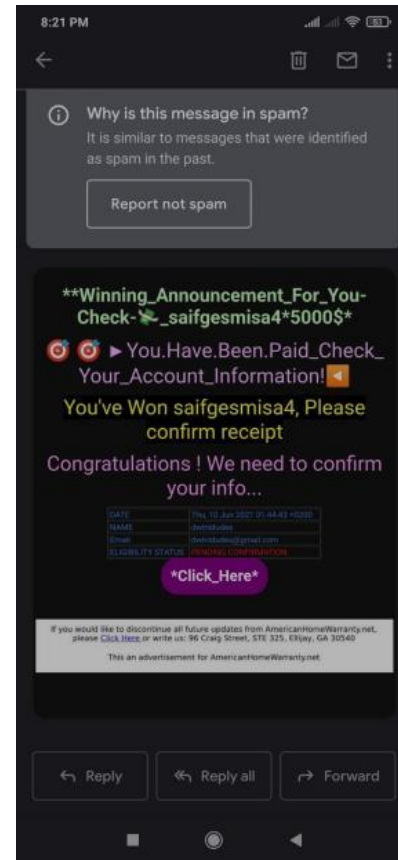
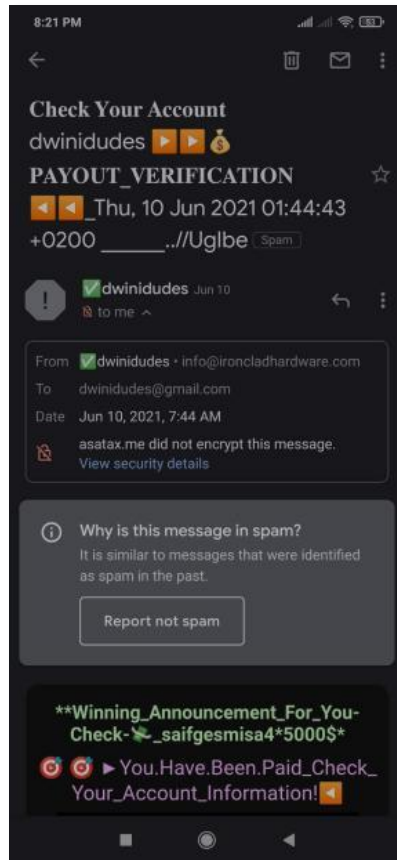


Personal Observation:
Criminals are capitalizing on the fact that most people are too lazy to read the fine prints



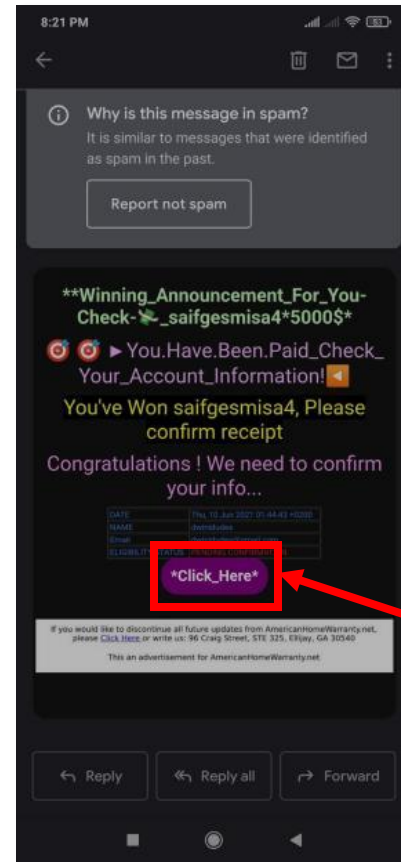
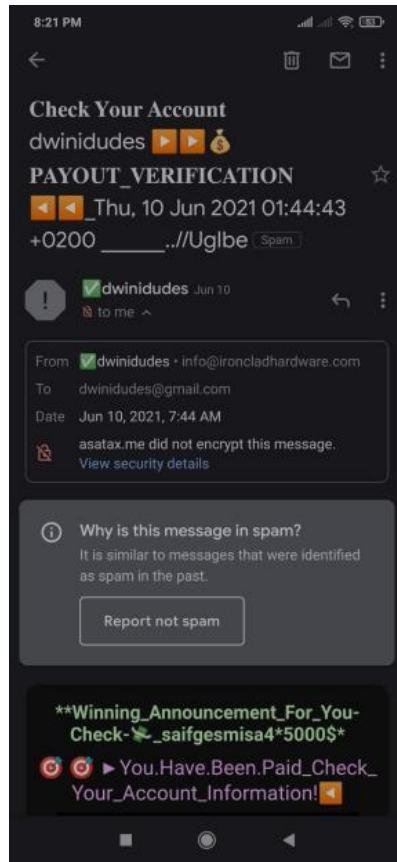
Phishing Awareness: Observing Intent

Phishing in 2021



Phishing Awareness: Observing Intent

Phishing in 2021

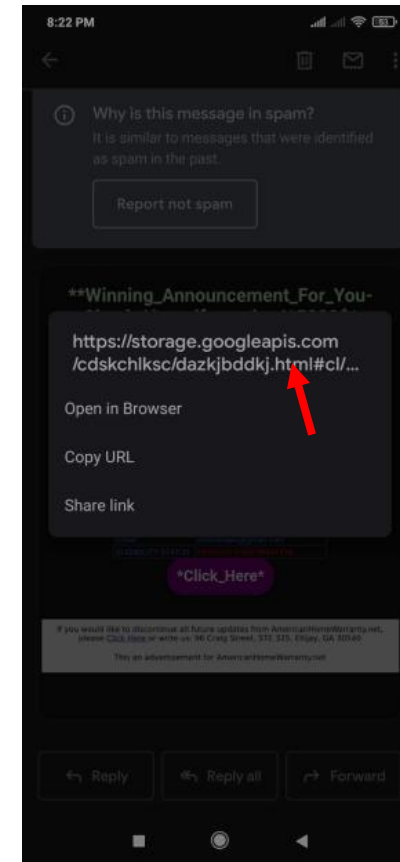
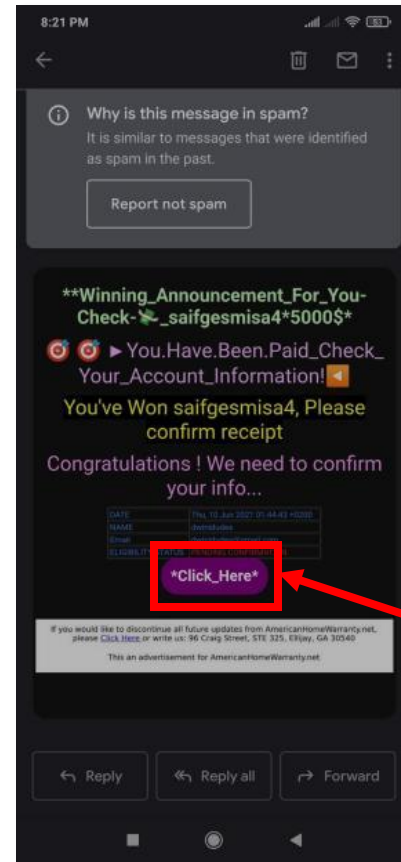
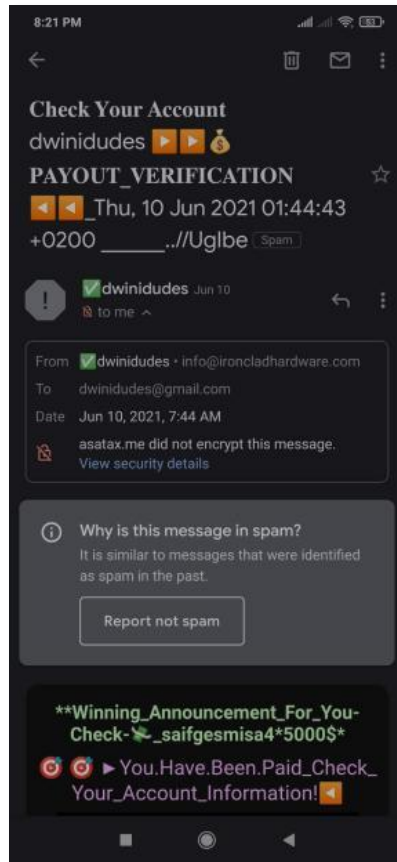


Long Press



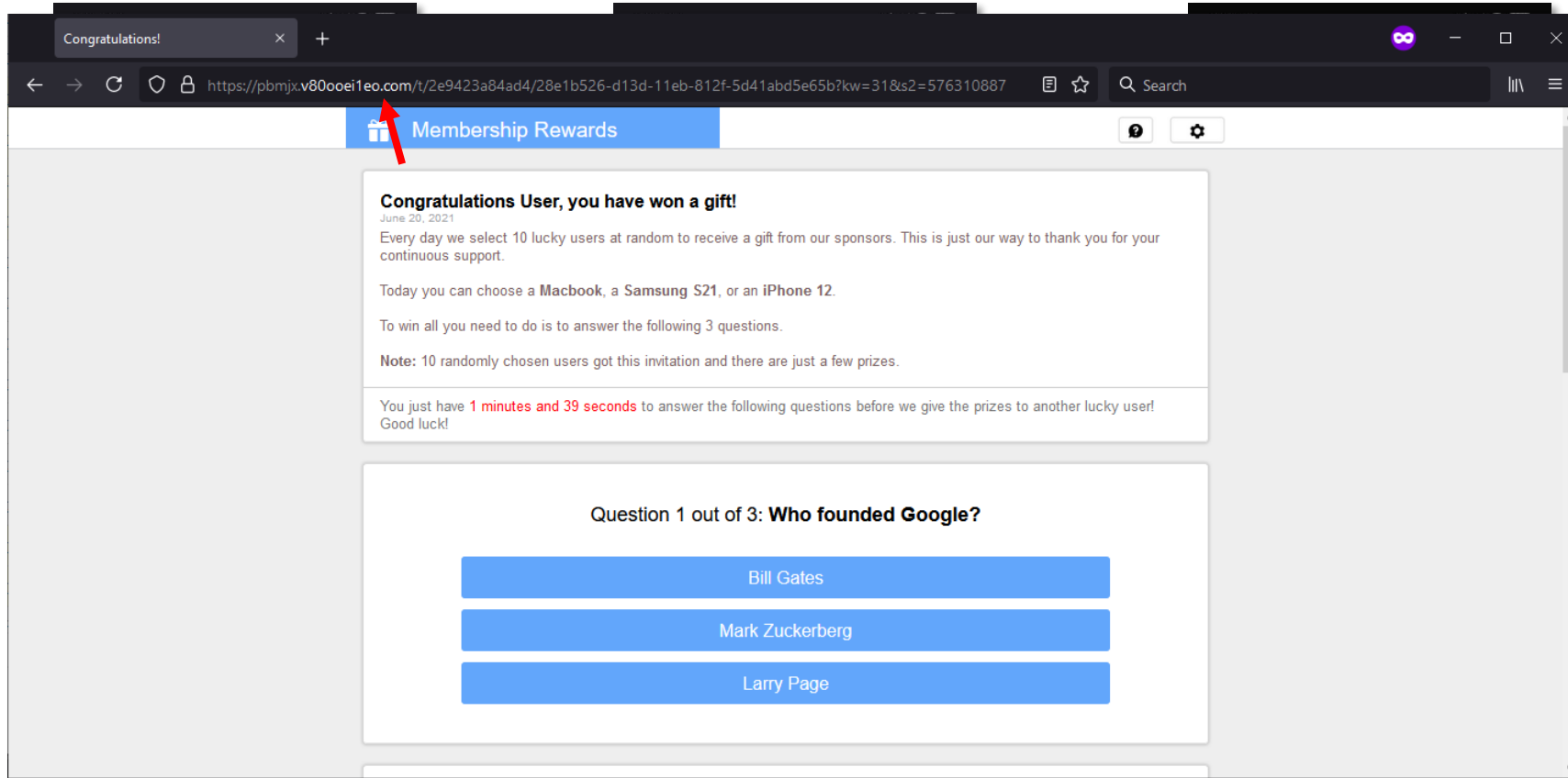
Phishing Awareness: Observing Intent

Phishing in 2021



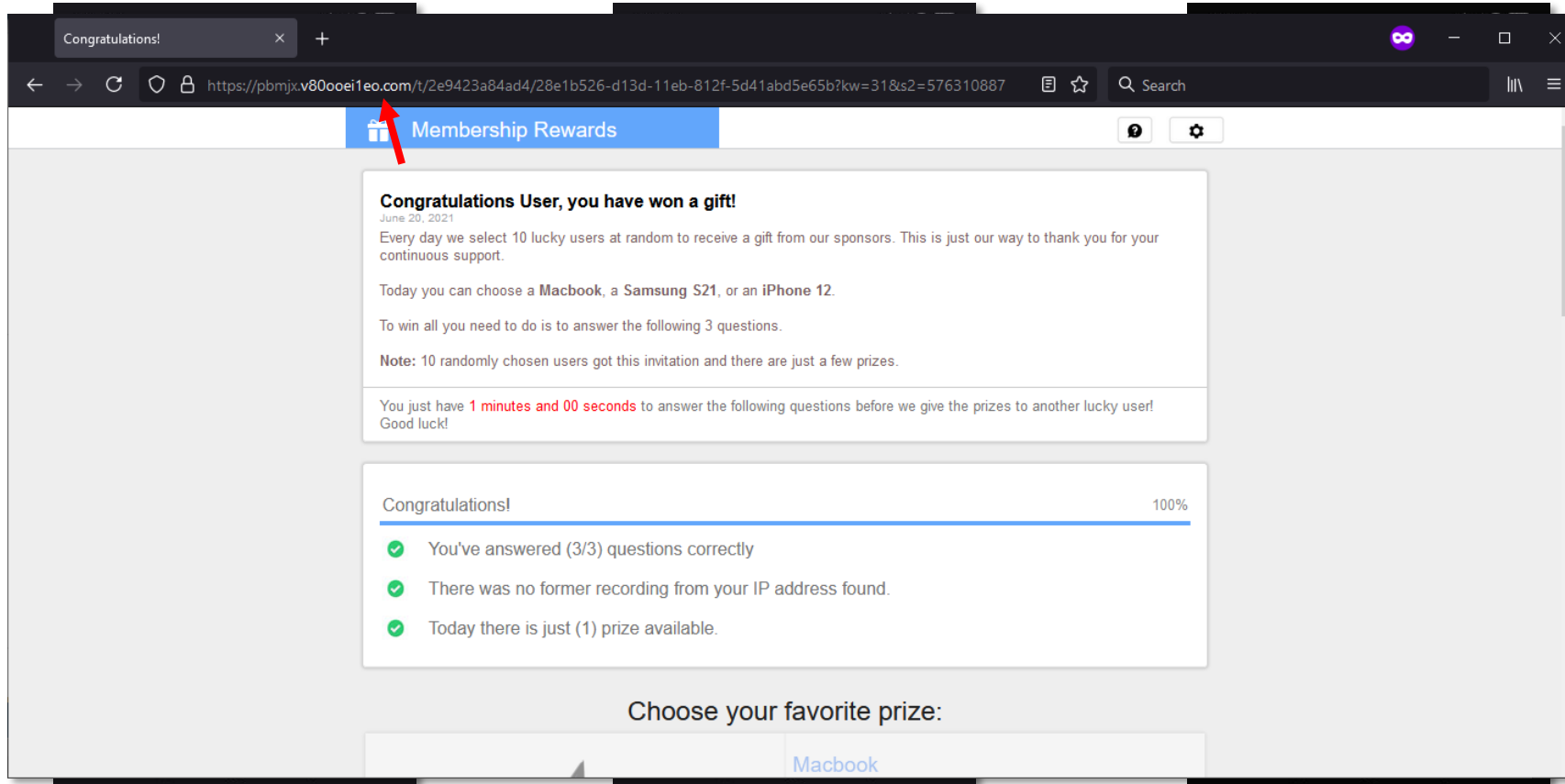
Phishing Awareness: Observing Intent

Phishing in 2021



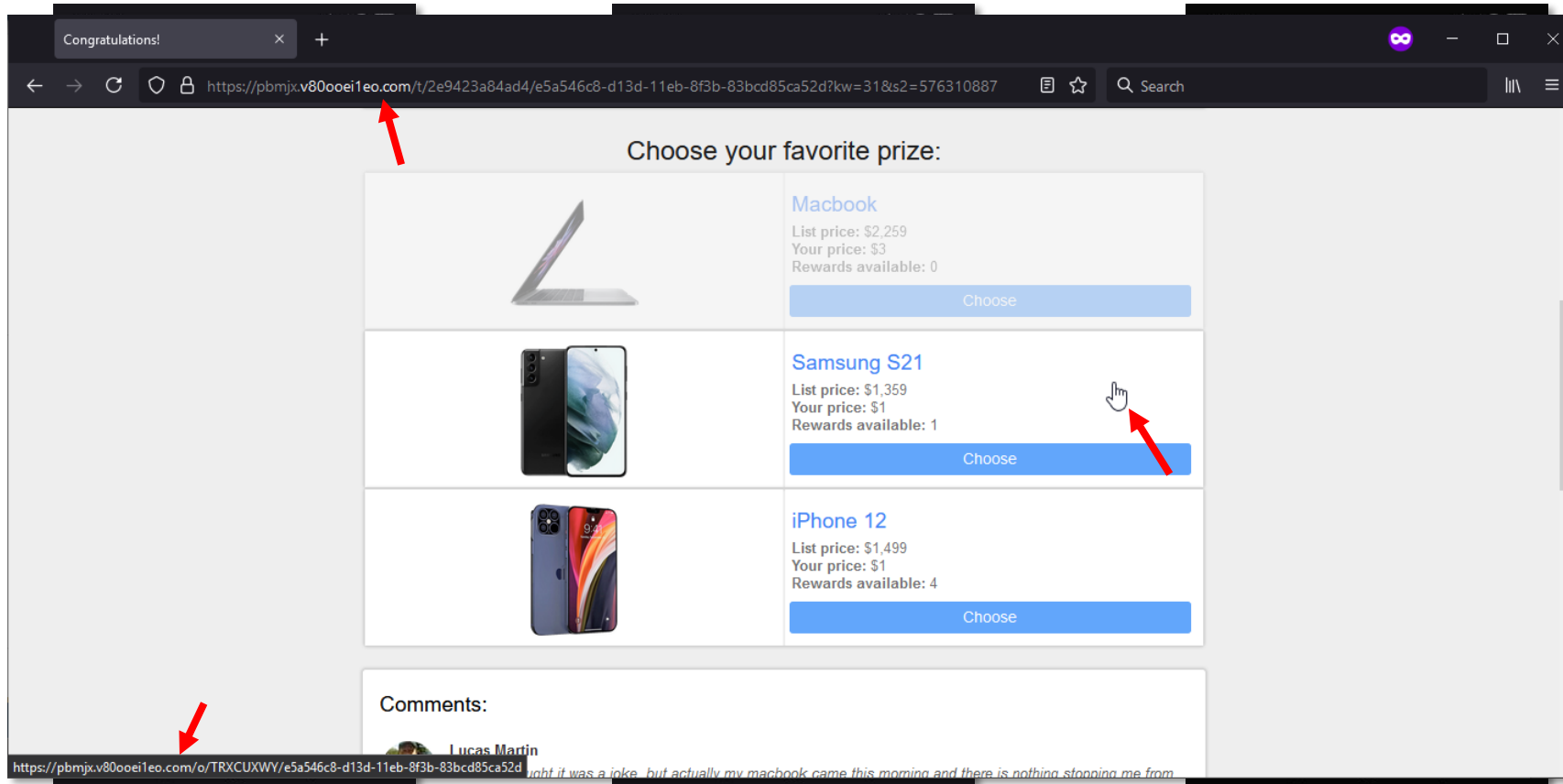
Phishing Awareness: Observing Intent

Phishing in 2021



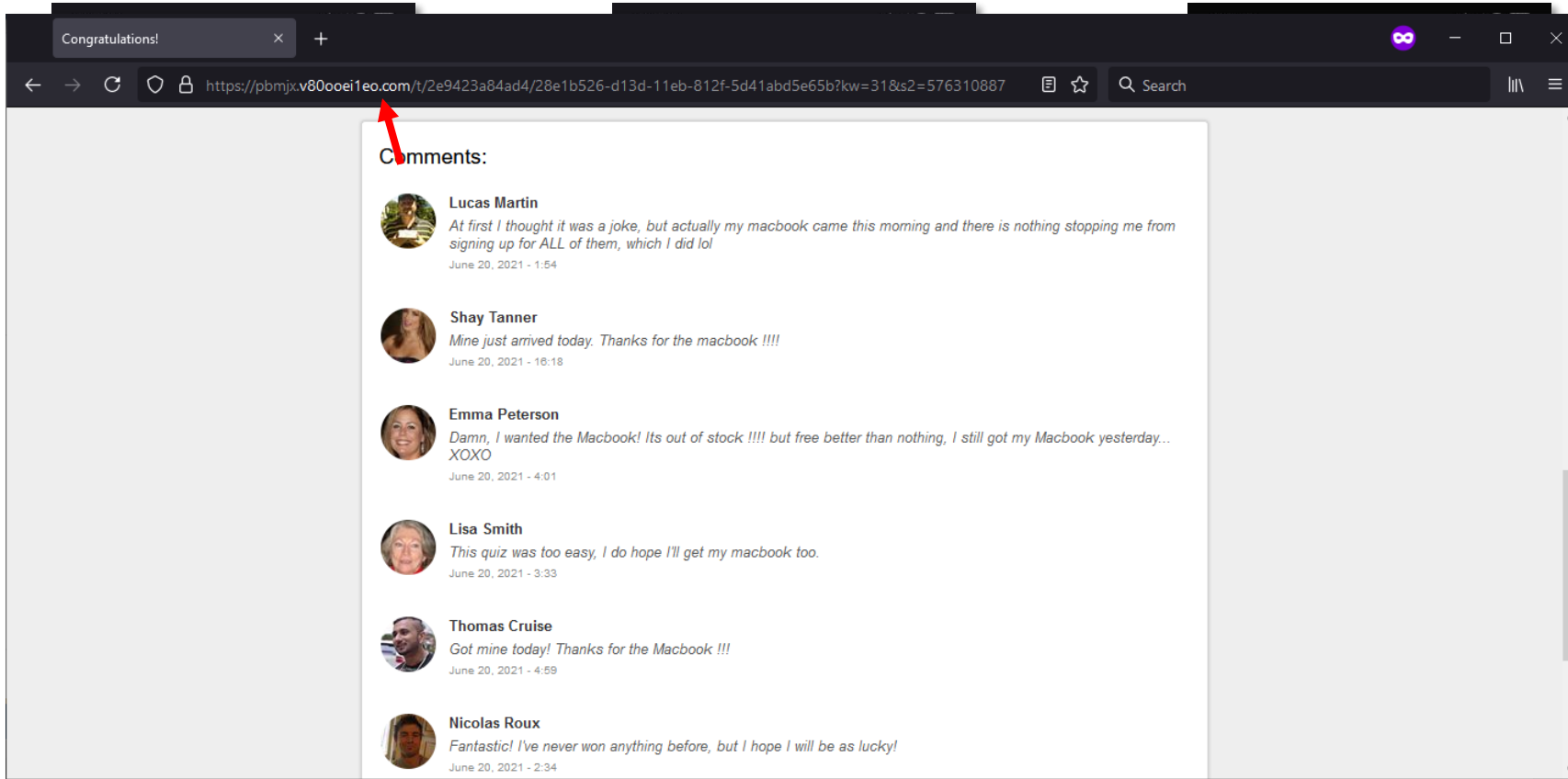
Phishing Awareness: Observing Intent

Phishing in 2021



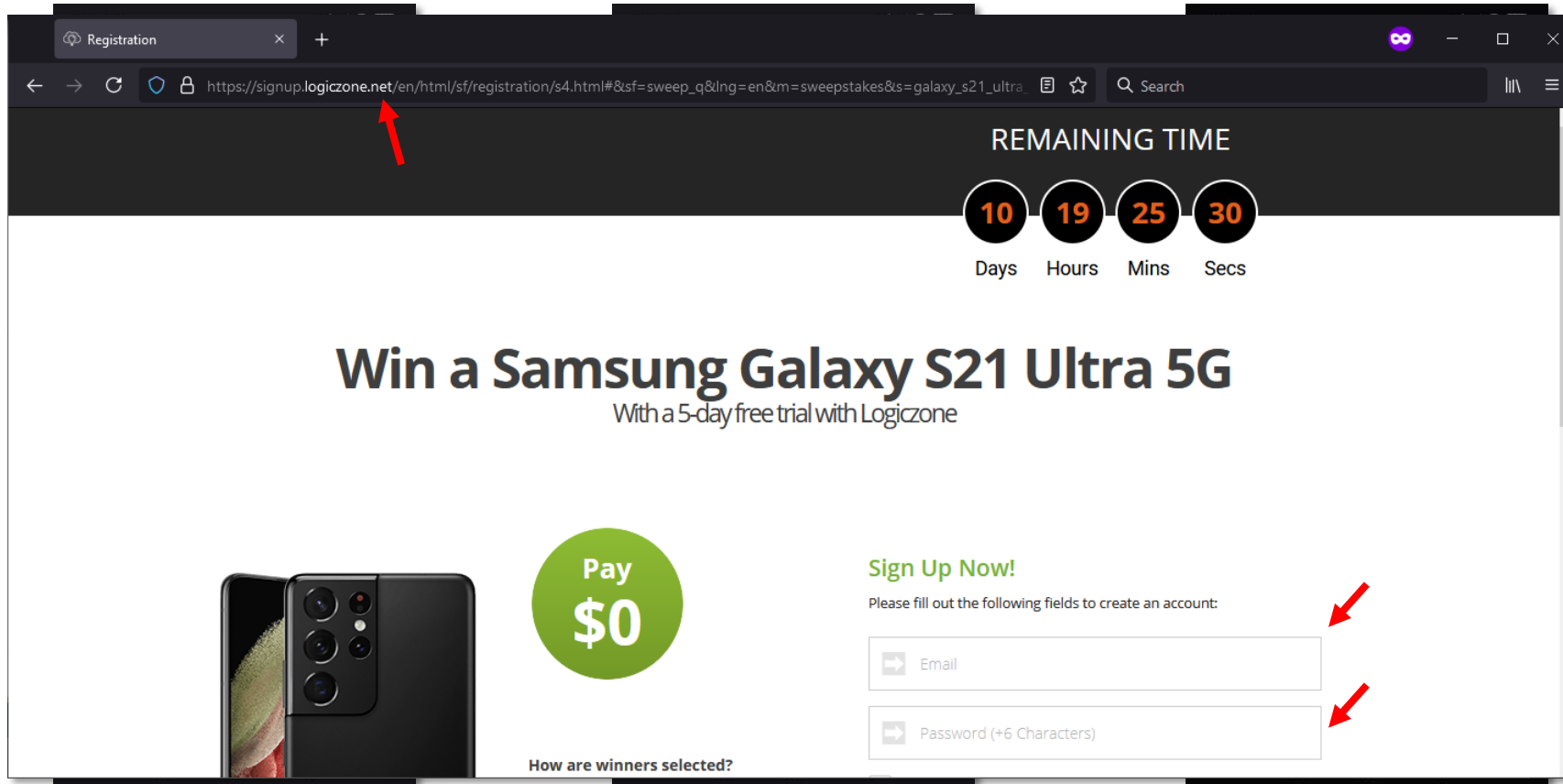
Phishing Awareness: Observing Intent

Phishing in 2021



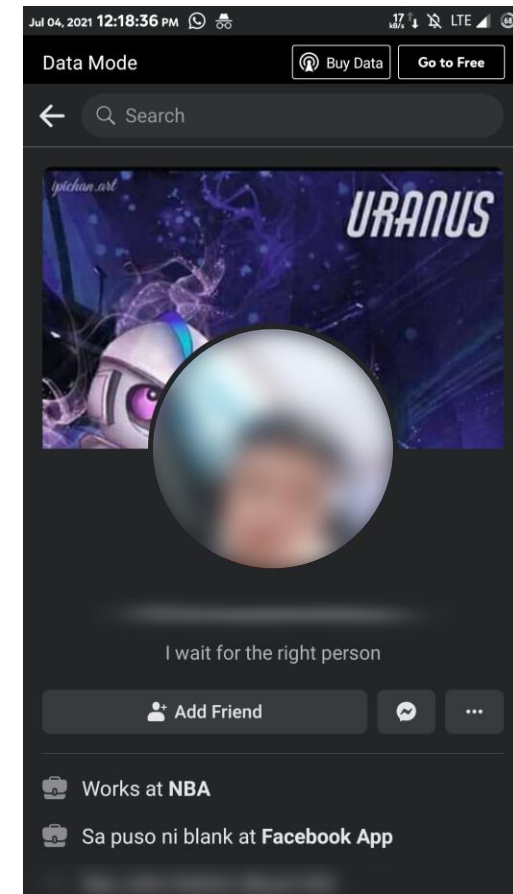
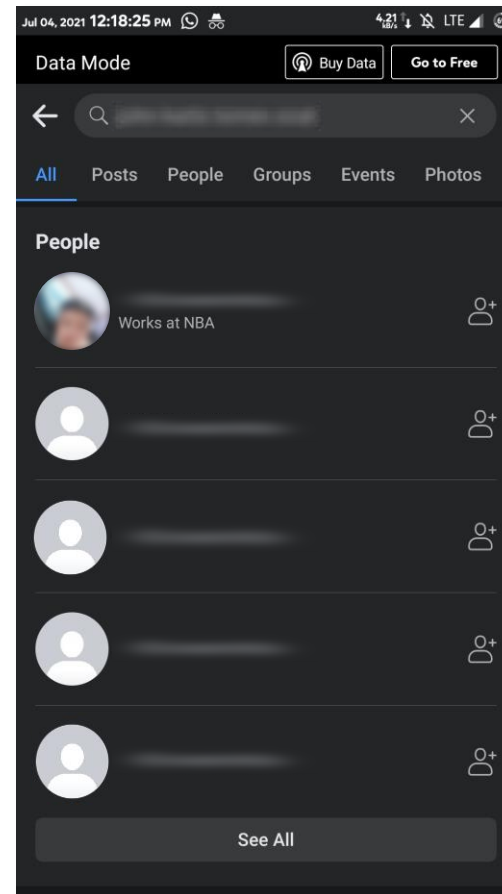
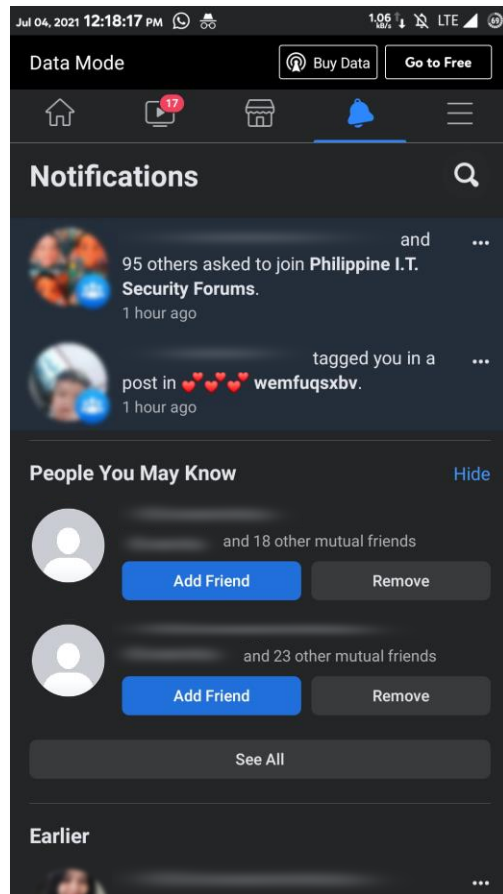
Phishing Awareness: Observing Intent

Phishing in 2021



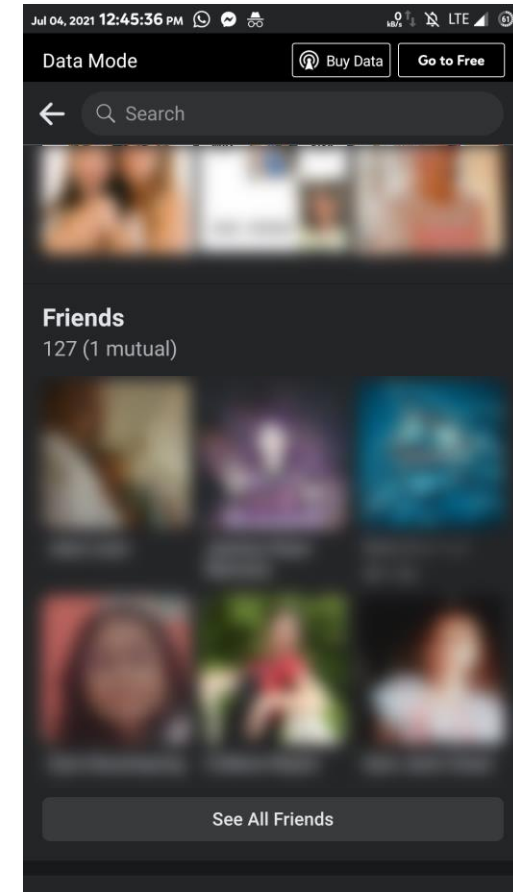
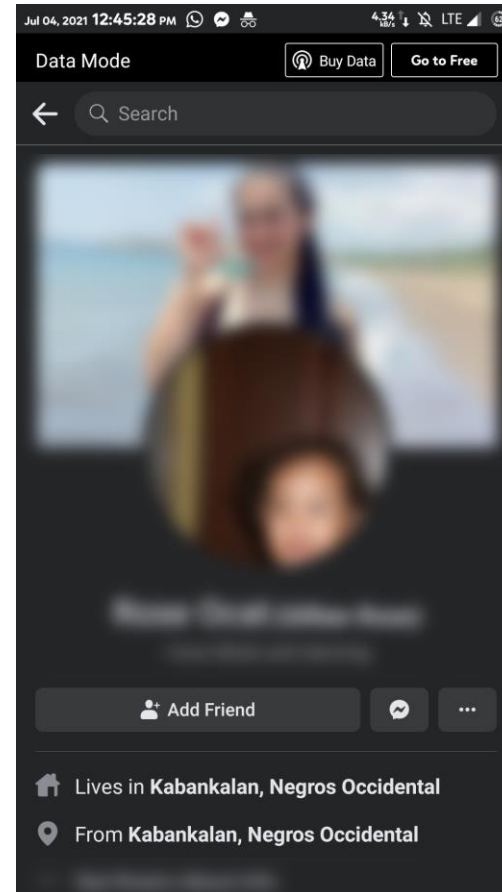
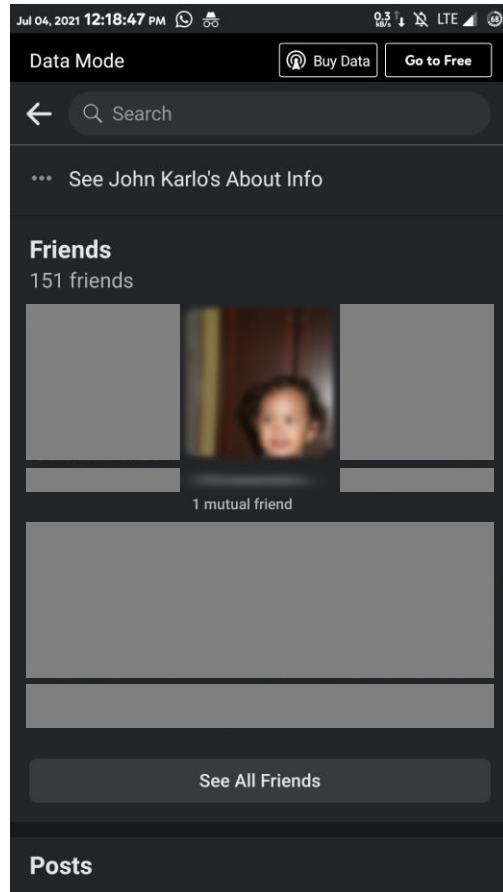
Phishing Awareness: Observing Intent

Phishing in 2021



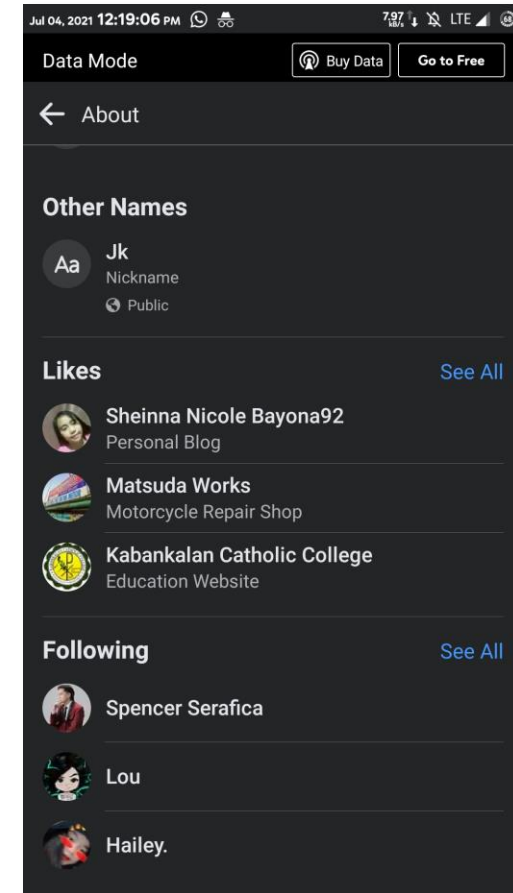
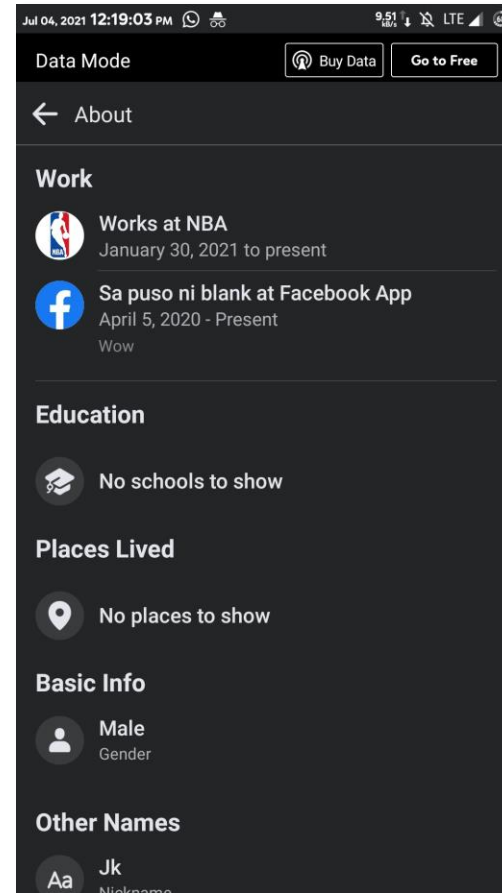
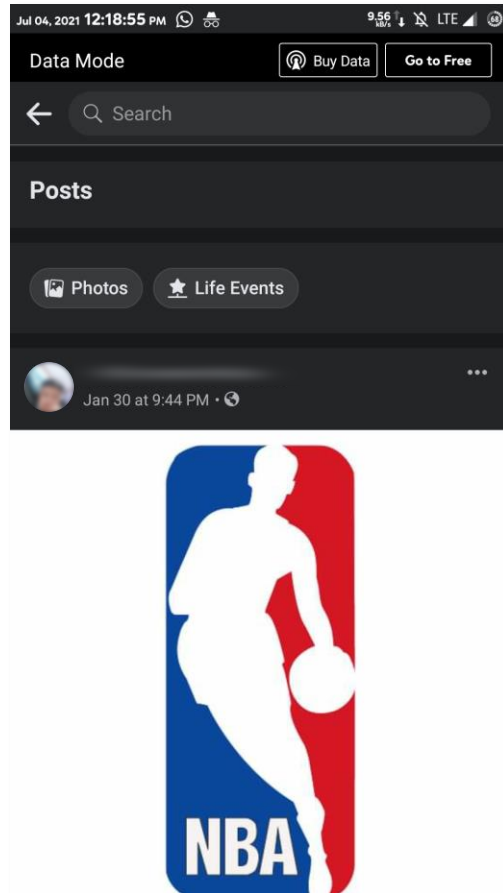
Phishing Awareness: Observing Intent

Phishing in 2021



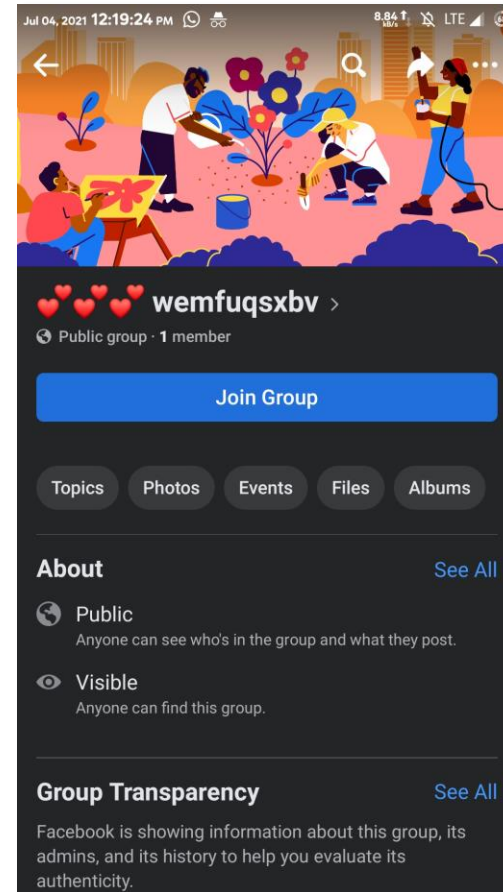
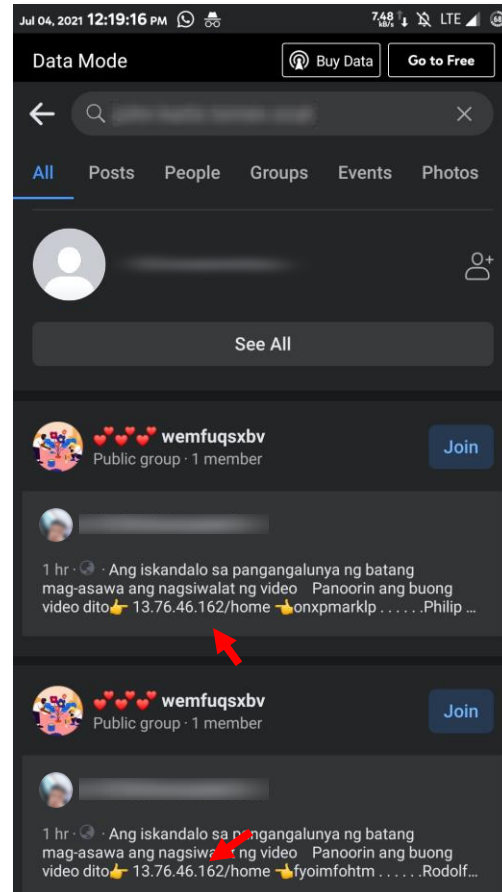
Phishing Awareness: Observing Intent

Phishing in 2021



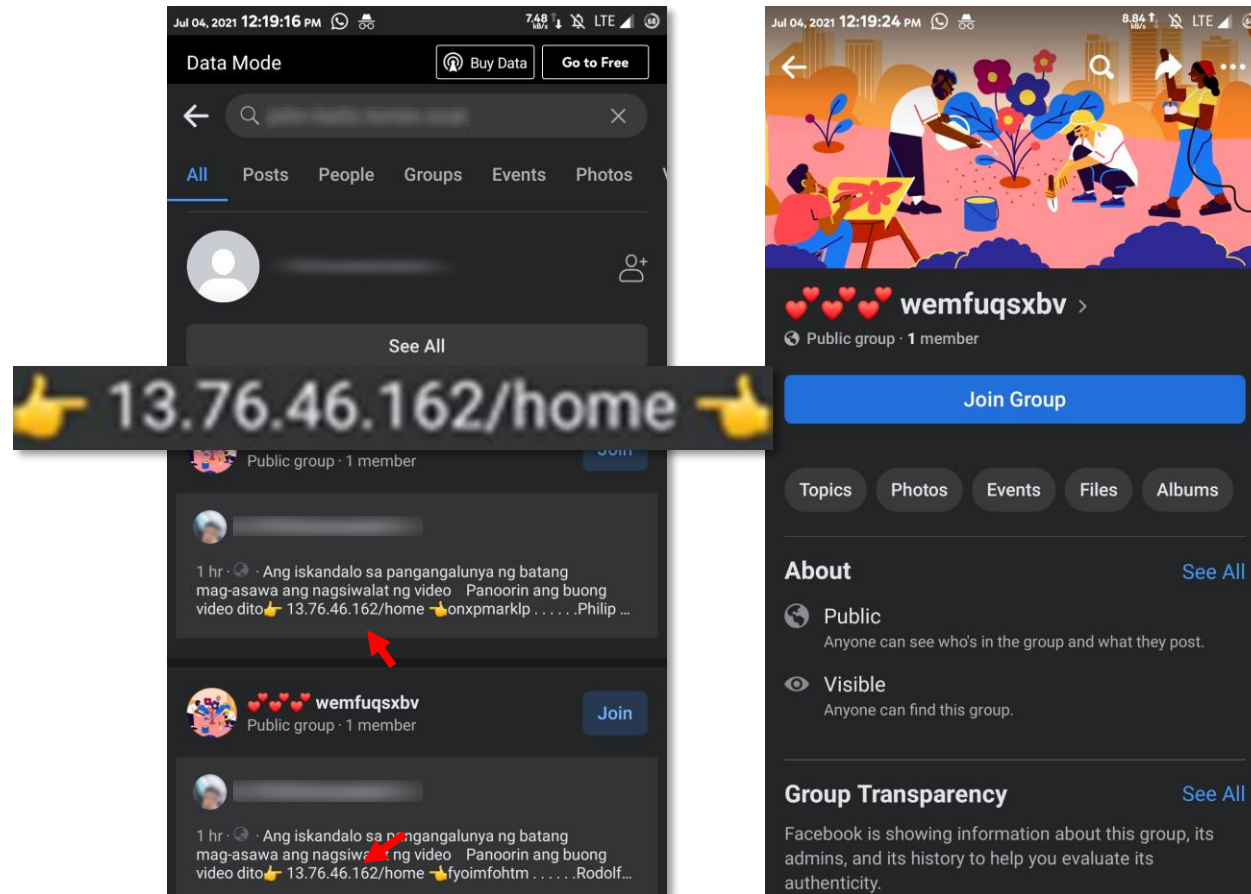
Phishing Awareness: Observing Intent

Phishing in 2021



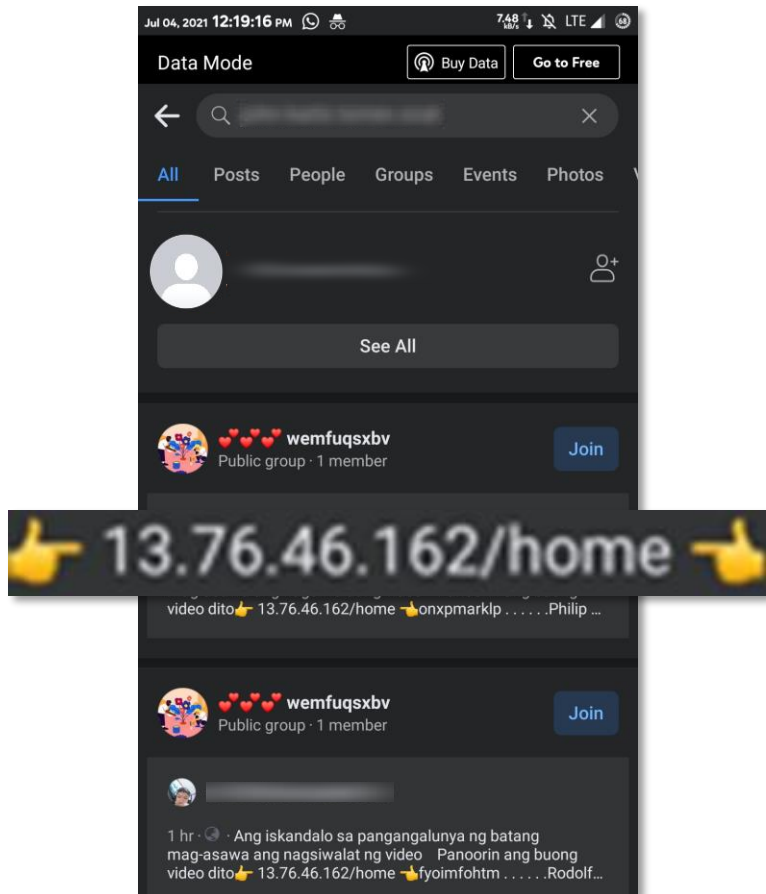
Phishing Awareness: Observing Intent

Phishing in 2021



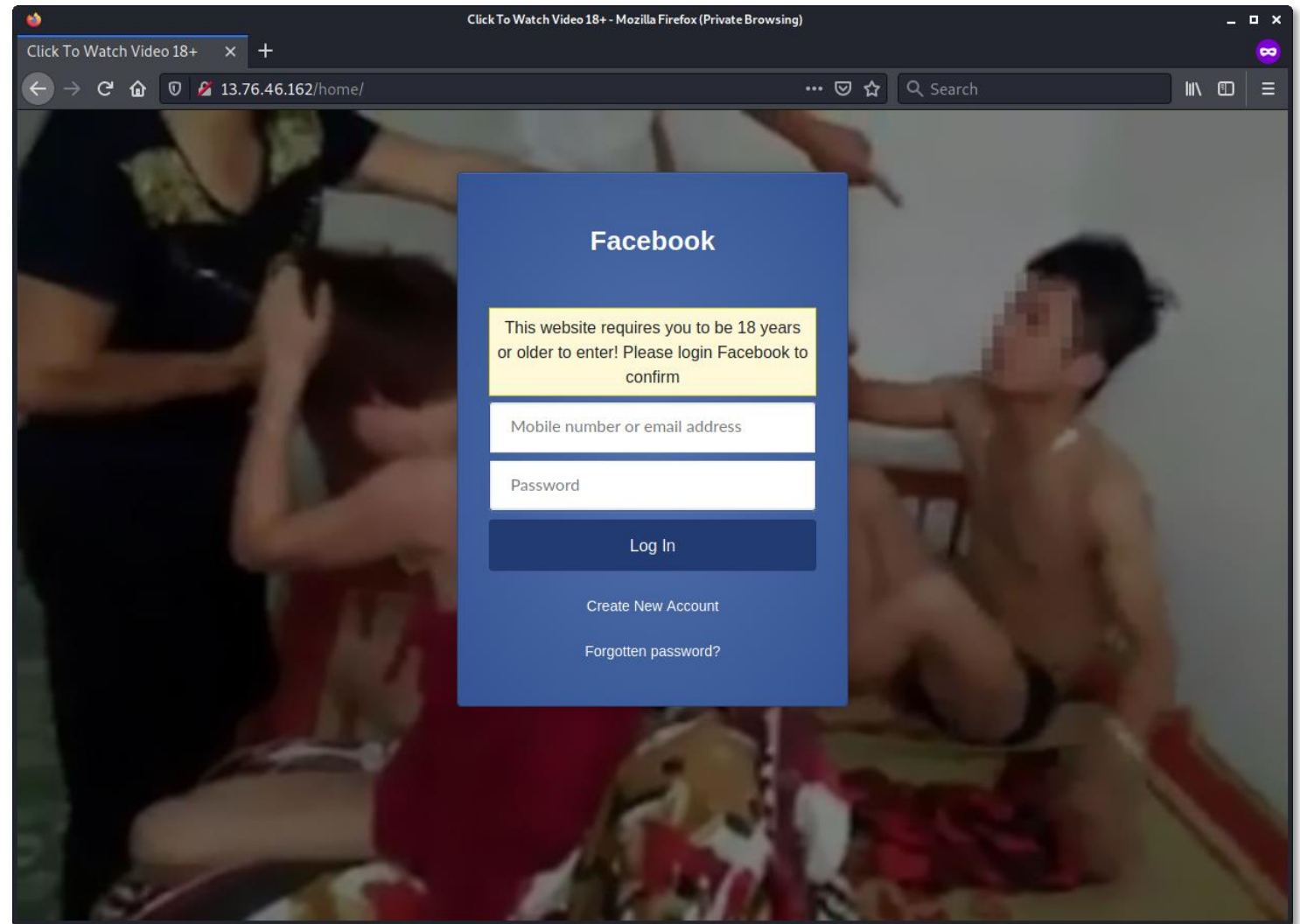
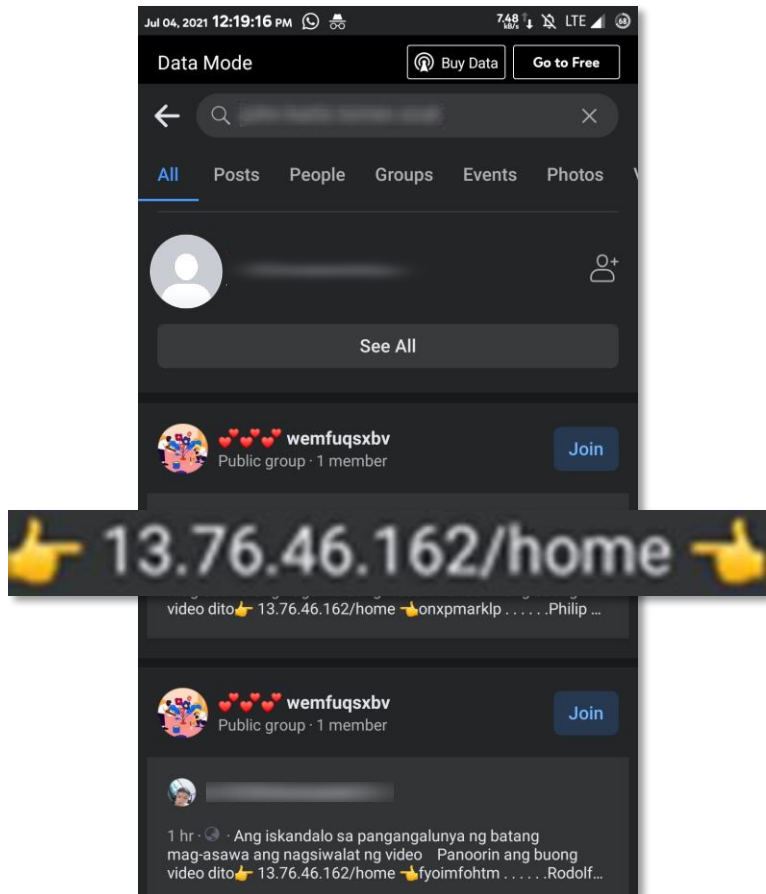
Phishing Awareness: Observing Intent

Phishing in 2021



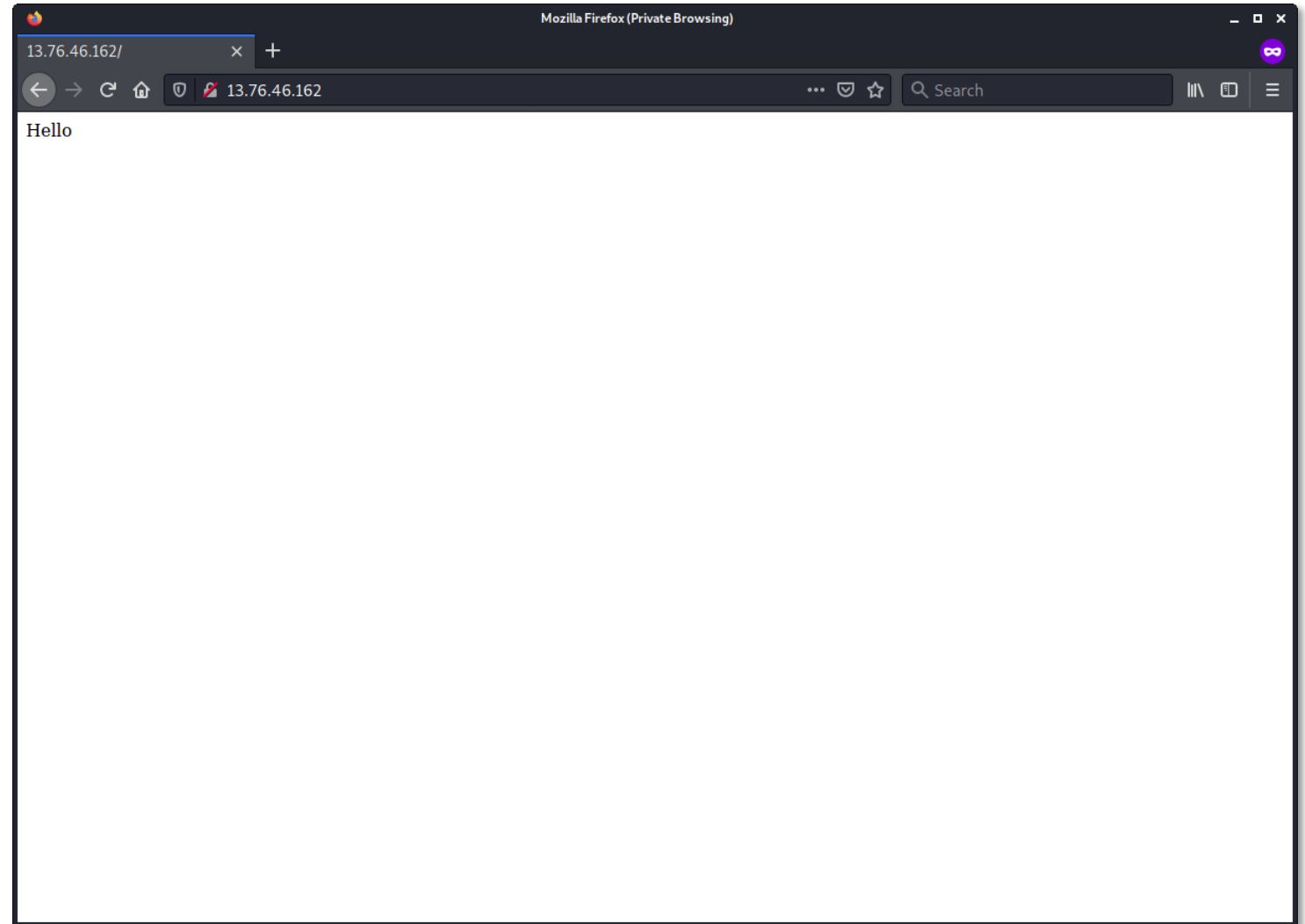
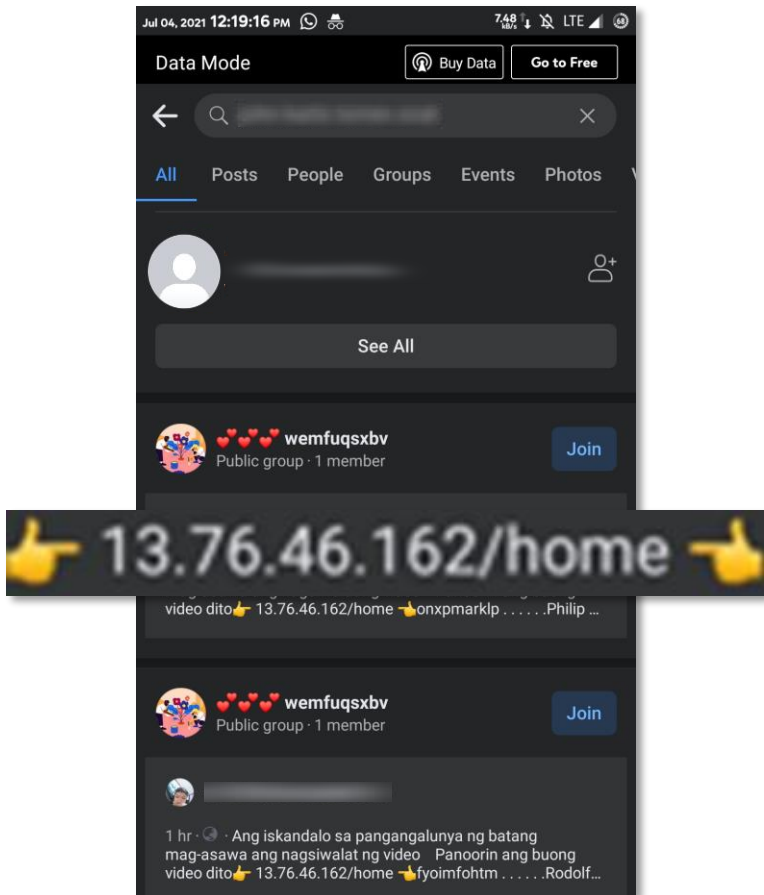
Phishing Awareness: Observing Intent

Phishing in 2021



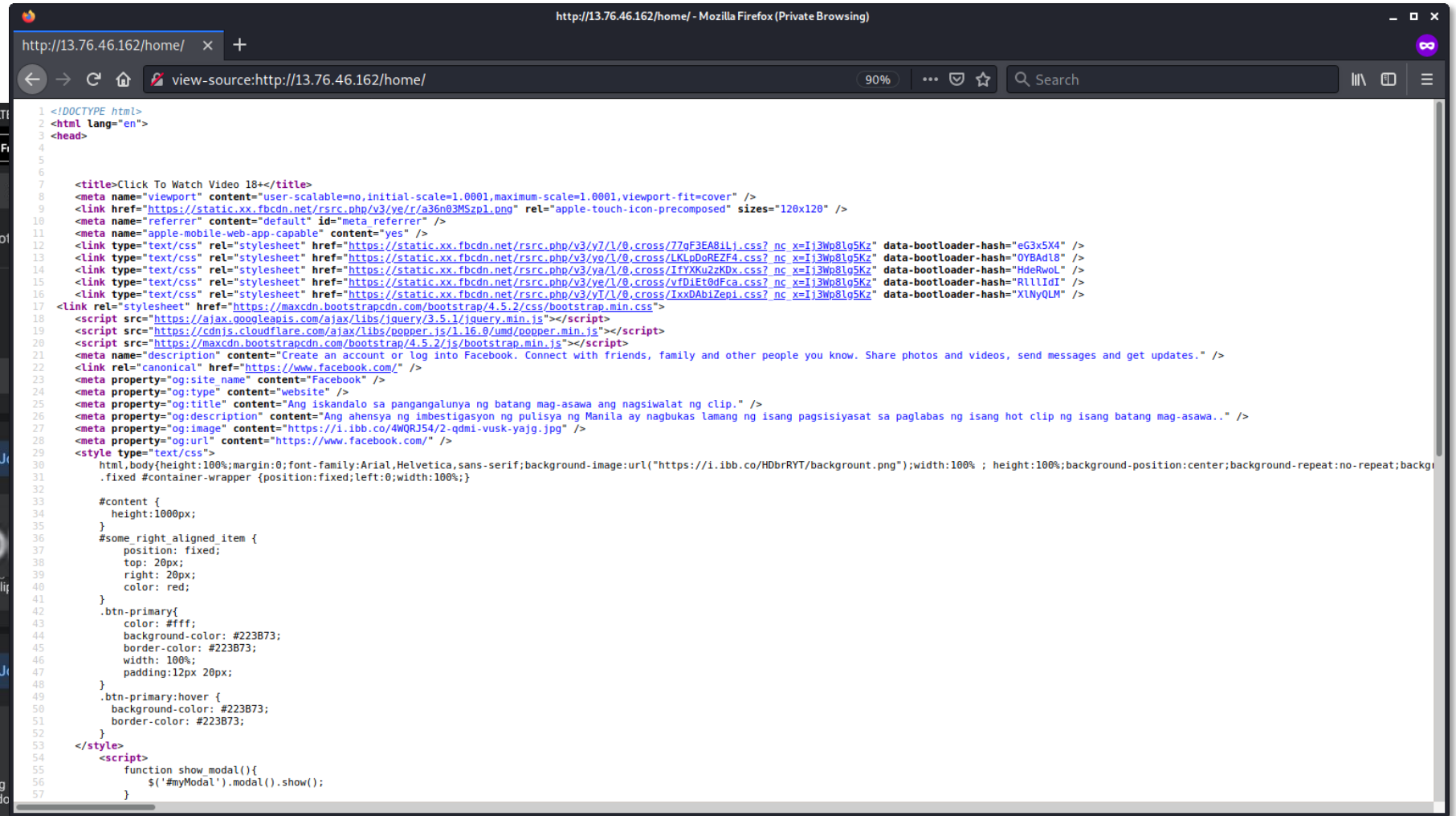
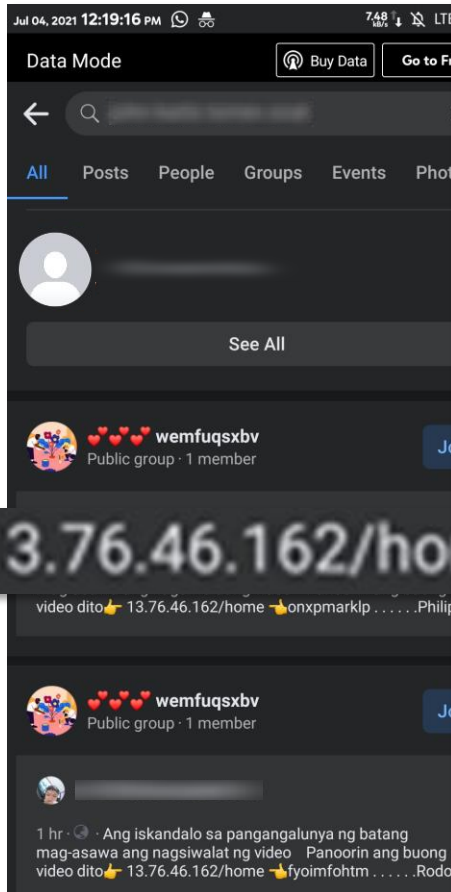
Phishing Awareness: Observing Intent

Phishing in 2021



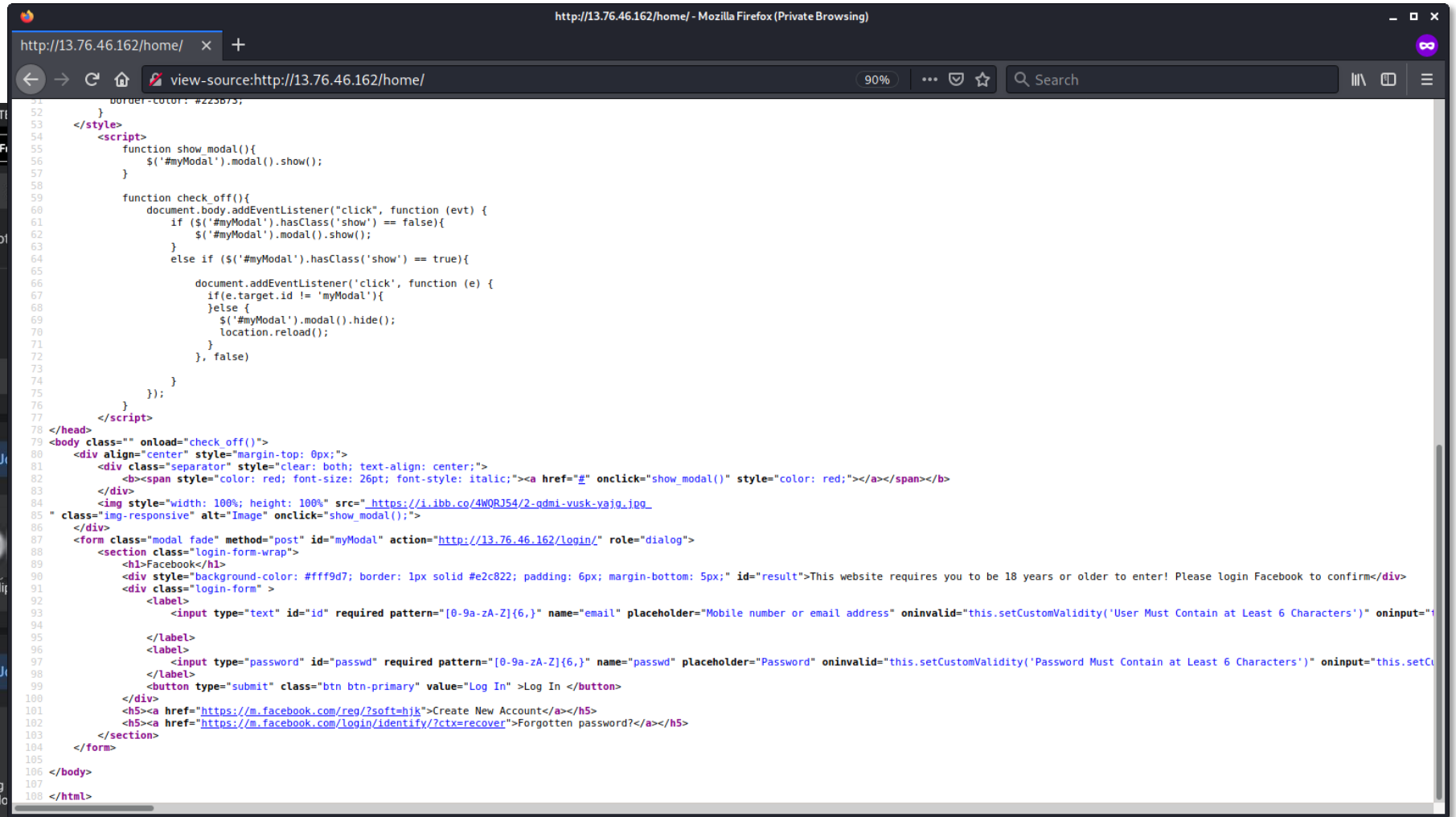
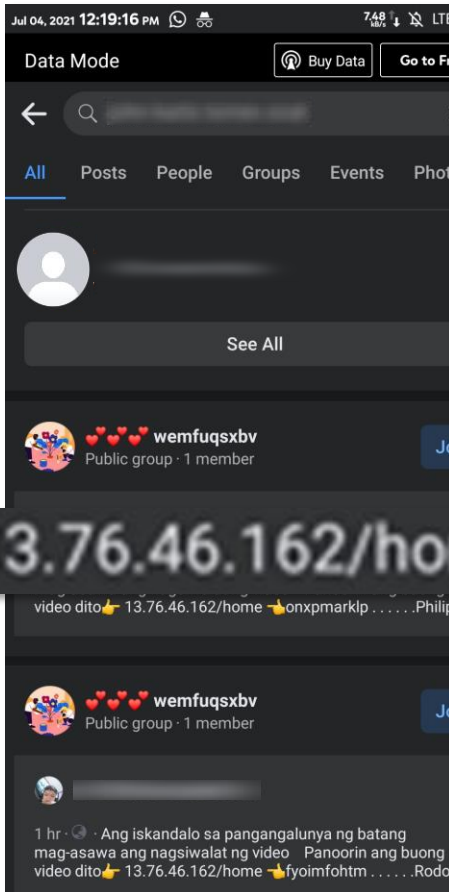
Phishing Awareness: Observing Intent

Phishing in 2021



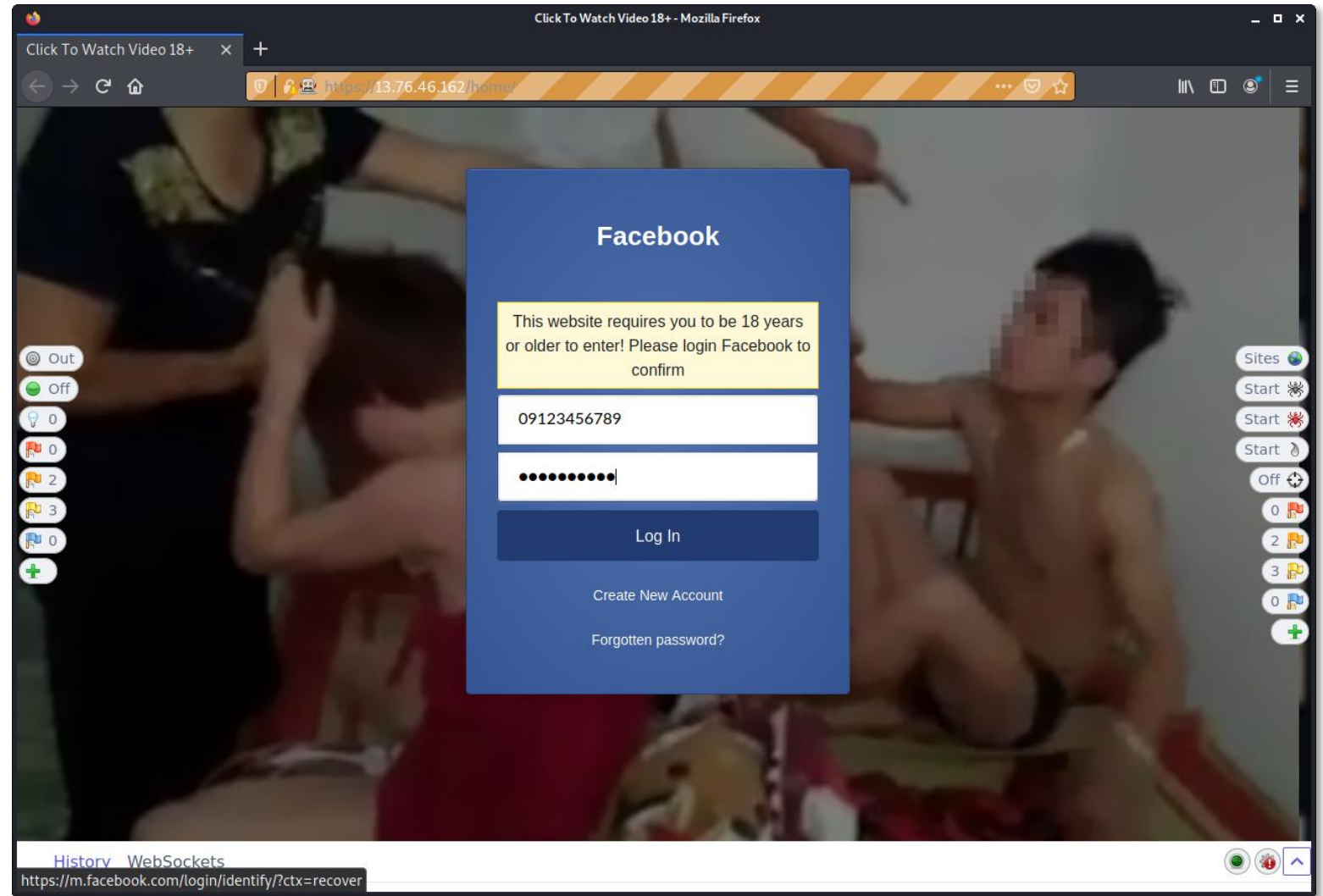
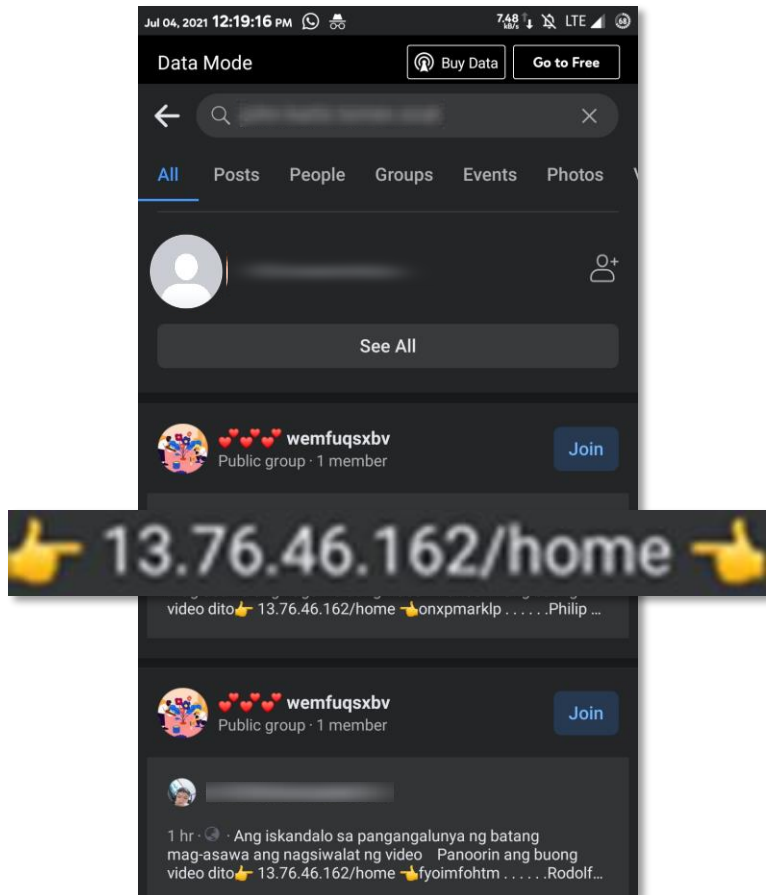
Phishing Awareness: Observing Intent

Phishing in 2021



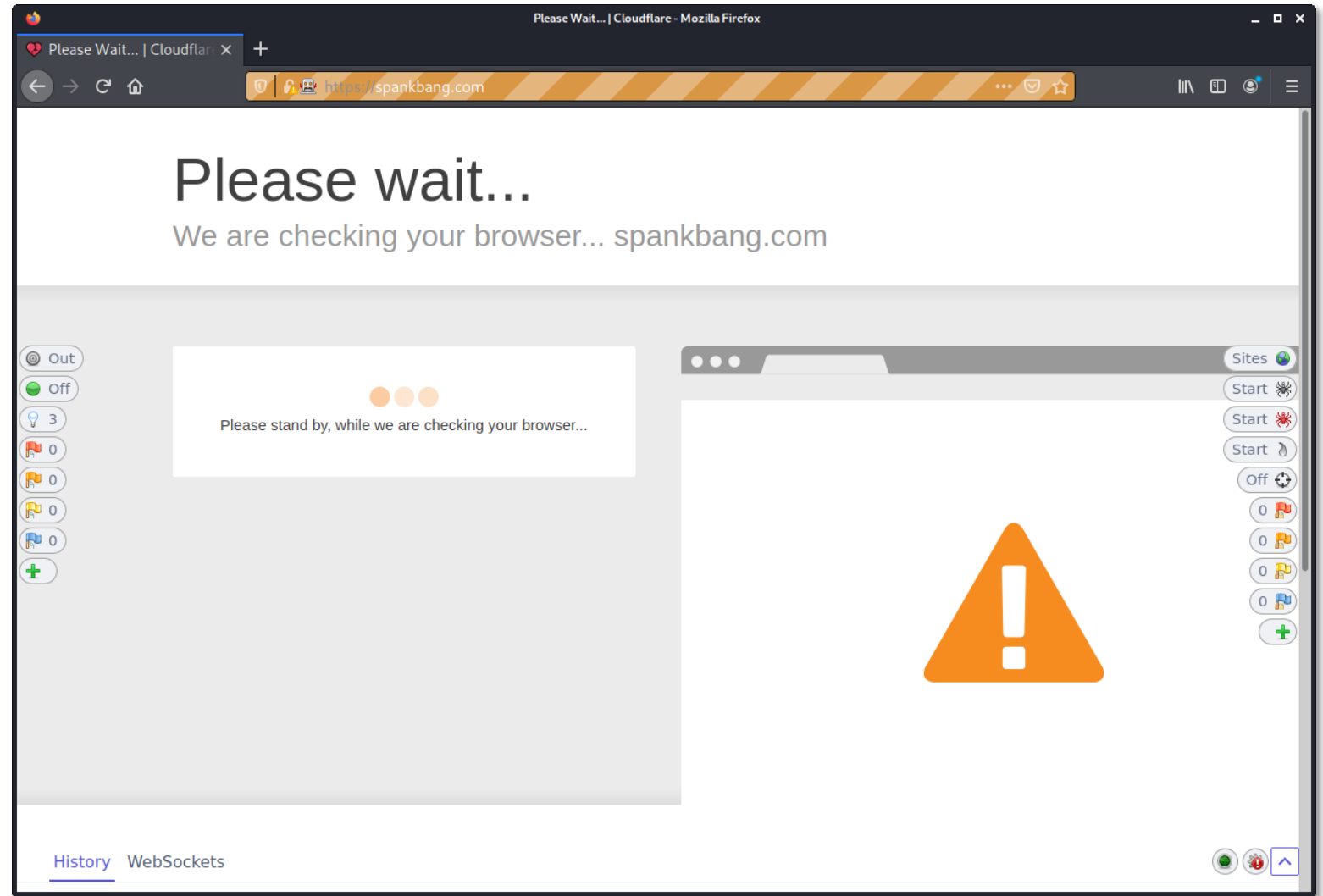
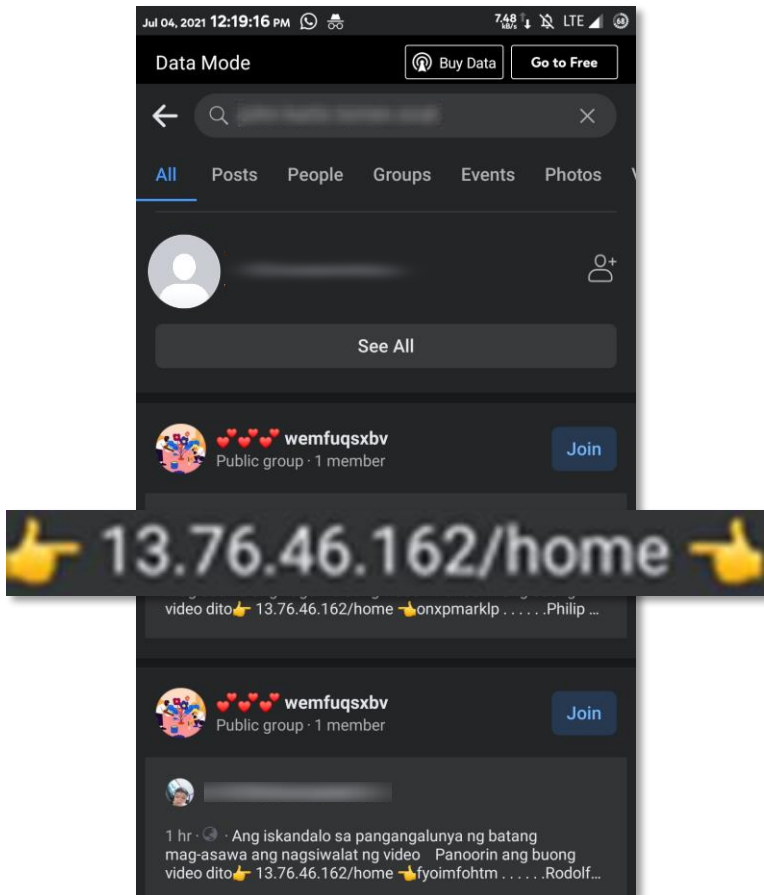
Phishing Awareness: Observing Intent

Phishing in 2021



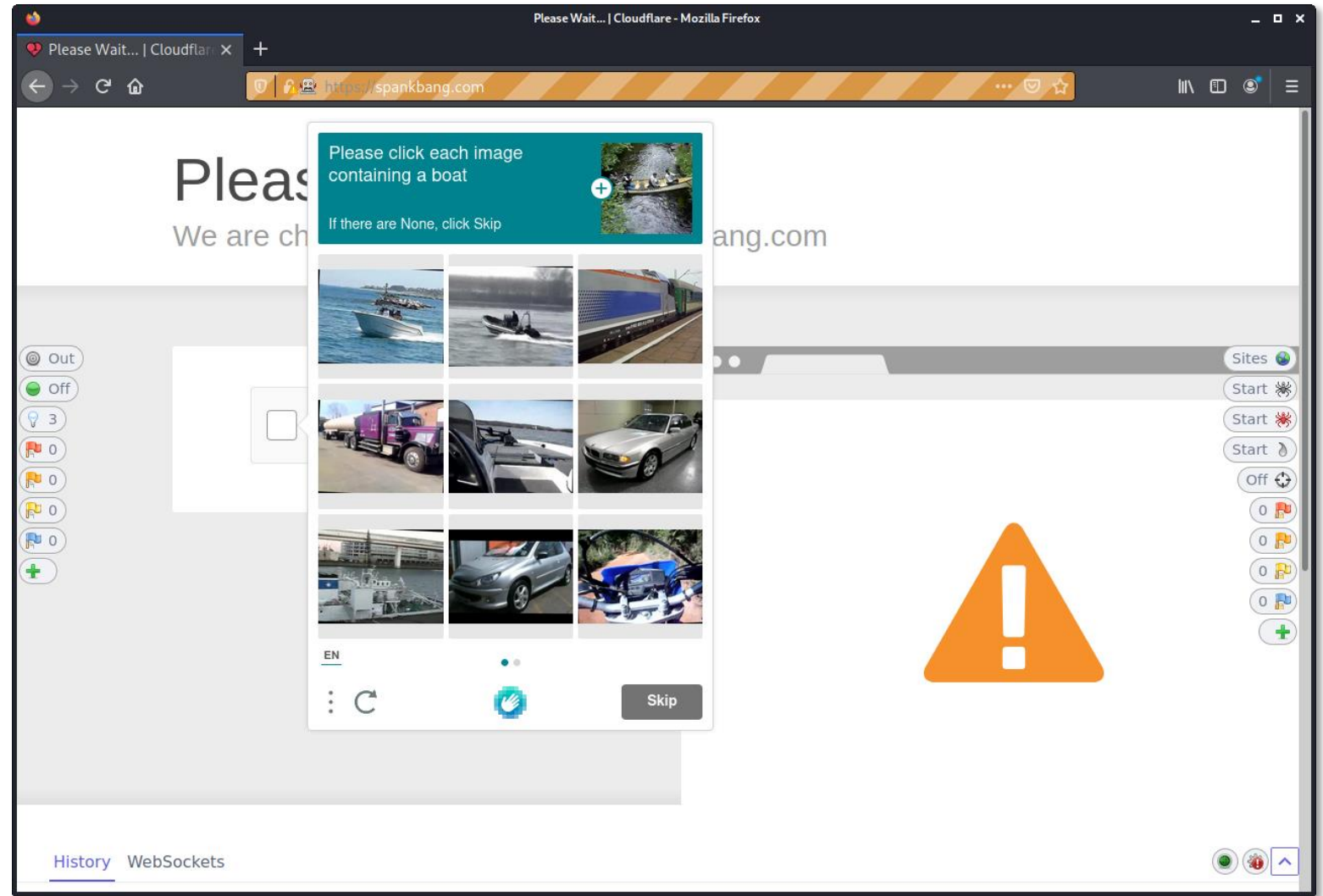
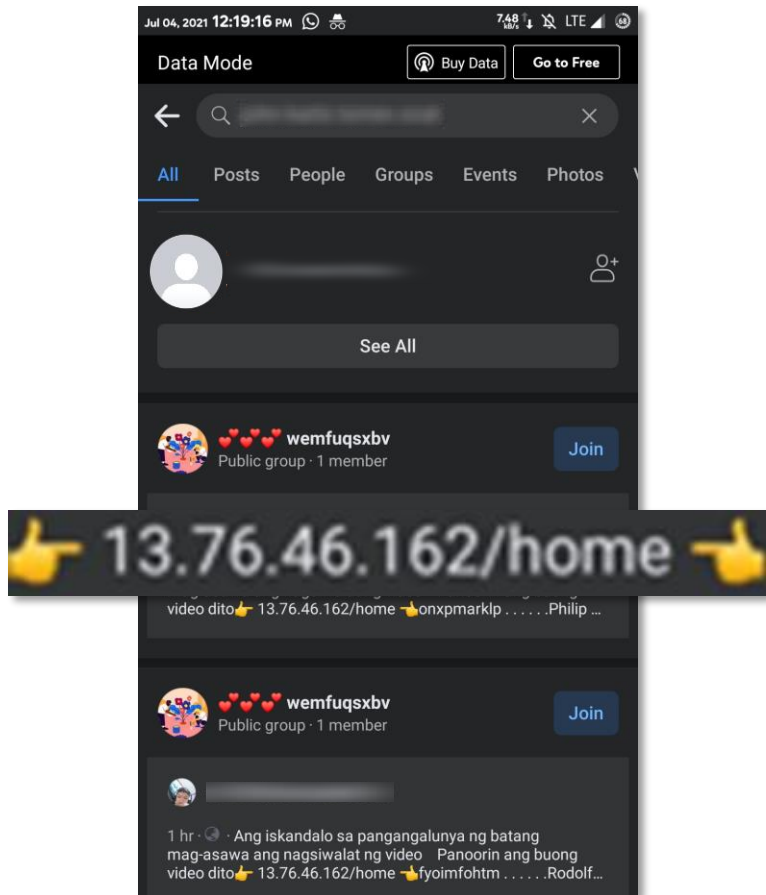
Phishing Awareness: Observing Intent

Phishing in 2021



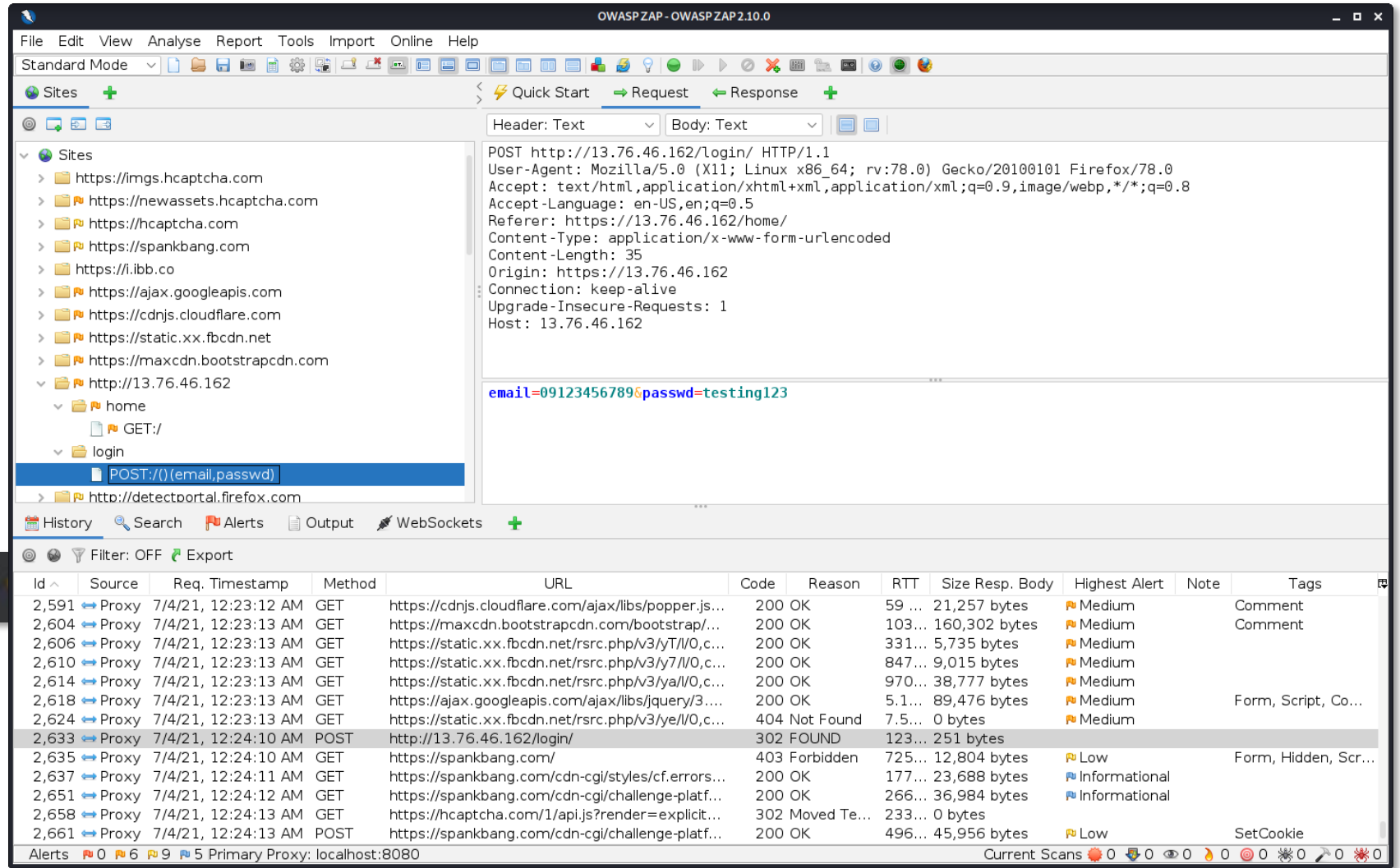
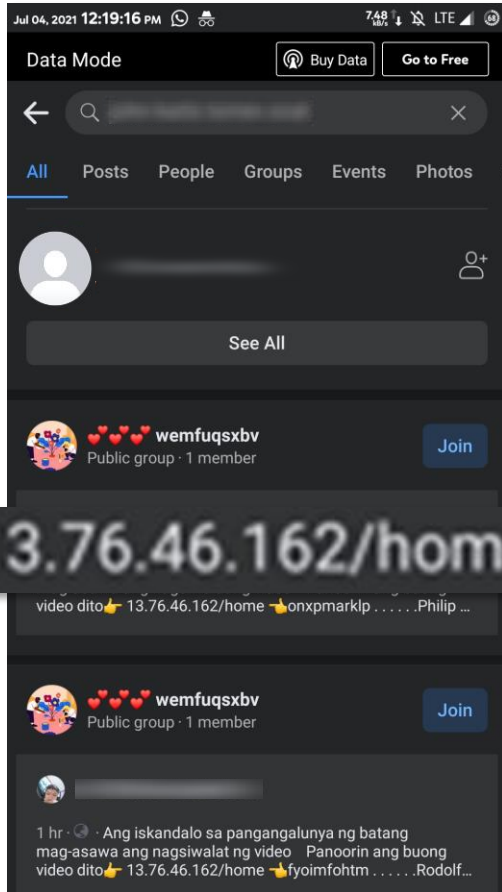
Phishing Awareness: Observing Intent

Phishing in 2021



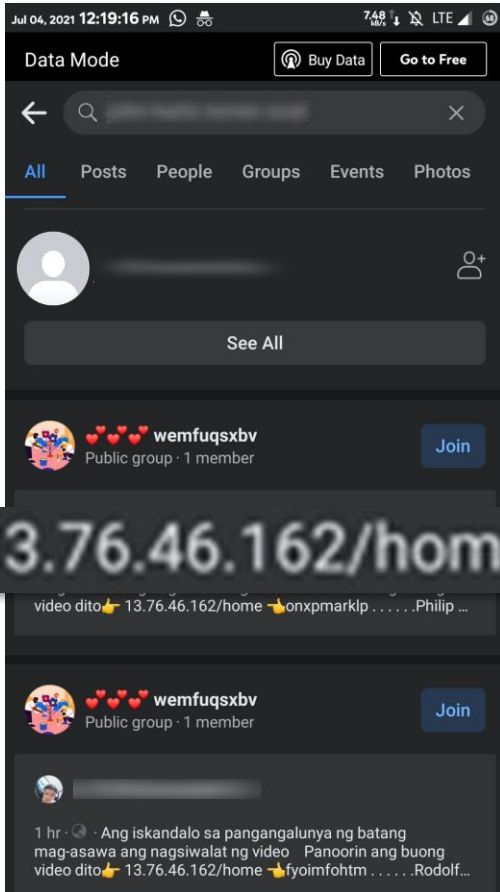
Phishing Awareness: Observing Intent

Phishing in 2021



Phishing Awareness: Observing Intent

Phishing in 2021



The screenshot shows the OWASP ZAP 2.10.0 web proxy tool interface. The top menu includes File, Edit, View, Analyse, Report, Tools, Import, and Online Help. The main window is divided into several sections:

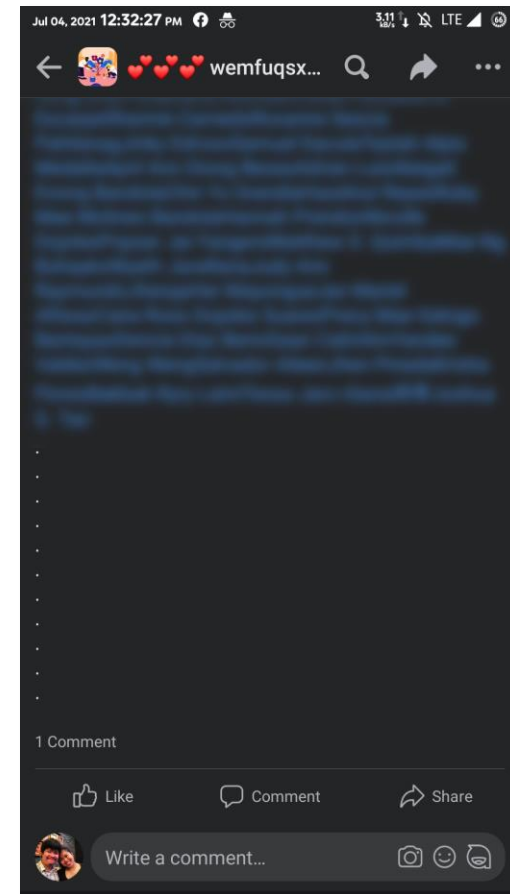
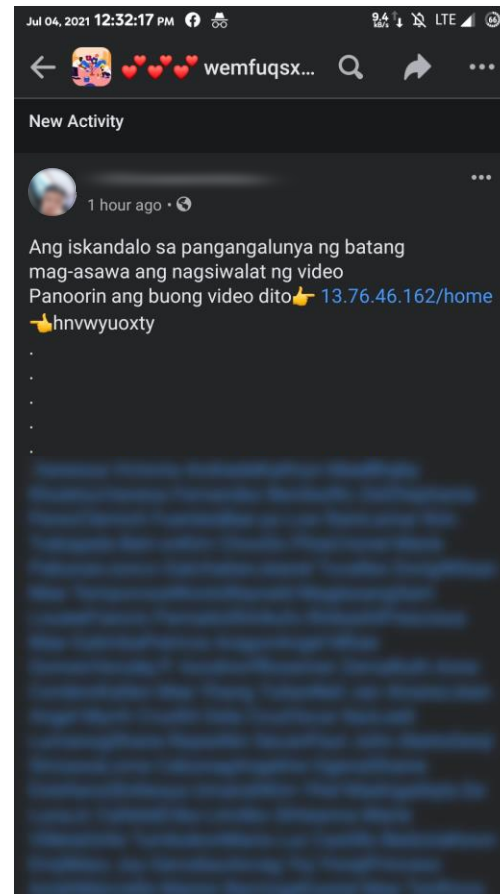
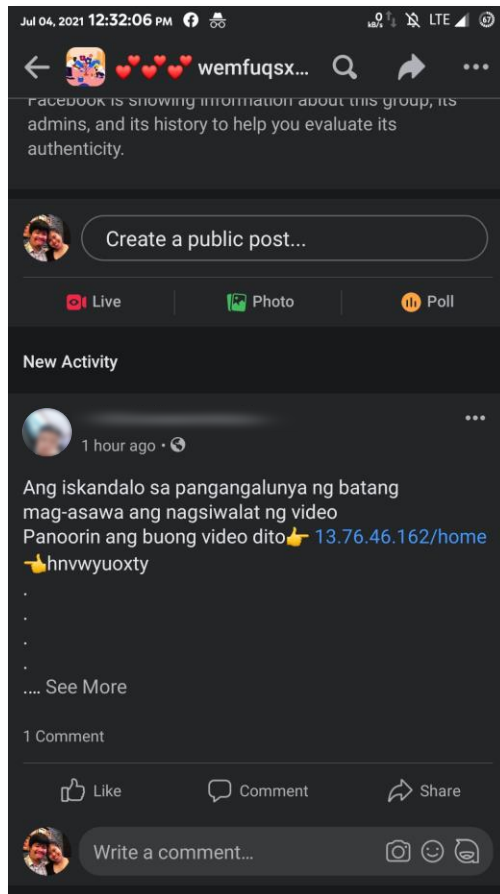
- Sites:** A list of sites being scanned, including https://irngs.hcaptcha.com, https://newassets.hcaptcha.com, https://hcaptcha.com, https://spankbang.com, https://fi.ibb.co, https://ajax.googleapis.com, https://cdnjs.cloudflare.com, https://static.xx.fbcdn.net, https://maxcdn.bootstrapcdn.com, and http://13.76.46.162.
- Request/Response:** A detailed view of a POST request to http://13.76.46.162/login/. The response is an HTTP 302 FOUND status with headers: Content-Type: text/html; charset=utf-8, Content-Length: 251, Location: https://spankbang.com/, Access-Control-Allow-Origin: https://13.76.46.162, Vary: Origin, Server: Werkzeug/1.0.1 Python/3.8.8, Date: Sun, 04 Jul 2021 04:24:12 GMT. The body contains HTML code for a redirect: `<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><title>Redirecting...</title><h1>Redirecting...</h1><p>You should be redirected automatically to target URL: https://spankbang.com/. If not click the link.</p>`
- History:** A table of request history with columns: Id, Source, Req. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Body, Highest Alert, Note, and Tags.

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
2,591	Proxy	7/4/21, 12:23:12 AM	GET	https://cdnjs.cloudflare.com/ajax/libs/popper.js...	200	OK	59 ...	21,257 bytes	Medium		Comment
2,604	Proxy	7/4/21, 12:23:13 AM	GET	https://maxcdn.bootstrapcdn.com/bootstrap/...	200	OK	103...	160,302 bytes	Medium		Comment
2,606	Proxy	7/4/21, 12:23:13 AM	GET	https://static.xx.fbcdn.net/rsrc.php/v3/yT/IV0,c...	200	OK	331...	5,735 bytes	Medium		
2,610	Proxy	7/4/21, 12:23:13 AM	GET	https://static.xx.fbcdn.net/rsrc.php/v3/yT/IV0,c...	200	OK	847...	9,015 bytes	Medium		
2,614	Proxy	7/4/21, 12:23:13 AM	GET	https://static.xx.fbcdn.net/rsrc.php/v3/ya/IV0,c...	200	OK	970...	38,777 bytes	Medium		
2,618	Proxy	7/4/21, 12:23:13 AM	GET	https://ajax.googleapis.com/ajax/libs/jquery/3...	200	OK	5.1...	89,476 bytes	Medium		Form, Script, Co...
2,624	Proxy	7/4/21, 12:23:13 AM	GET	https://static.xx.fbcdn.net/rsrc.php/v3/ye/IV0,c...	404	Not Found	7.5...	0 bytes	Medium		
2,633	Proxy	7/4/21, 12:24:10 AM	POST	http://13.76.46.162/login/	302	FOUND	123...	251 bytes			
2,635	Proxy	7/4/21, 12:24:10 AM	GET	https://spankbang.com/	403	Forbidden	725...	12,804 bytes	Low		Form, Hidden, Scr...
2,637	Proxy	7/4/21, 12:24:11 AM	GET	https://spankbang.com/cdn-cgi/styles/cf.errors...	200	OK	177...	23,688 bytes	Informational		
2,651	Proxy	7/4/21, 12:24:12 AM	GET	https://spankbang.com/cdn-cgi/challenge-platf...	200	OK	266...	36,984 bytes	Informational		
2,658	Proxy	7/4/21, 12:24:13 AM	GET	https://hcaptcha.com/1/api.js?render=explicit...	302	Moved Te...	233...	0 bytes			
2,661	Proxy	7/4/21, 12:24:13 AM	POST	https://spankbang.com/cdn-cgi/challenge-platf...	200	OK	496...	45,956 bytes	Low		SetCookie



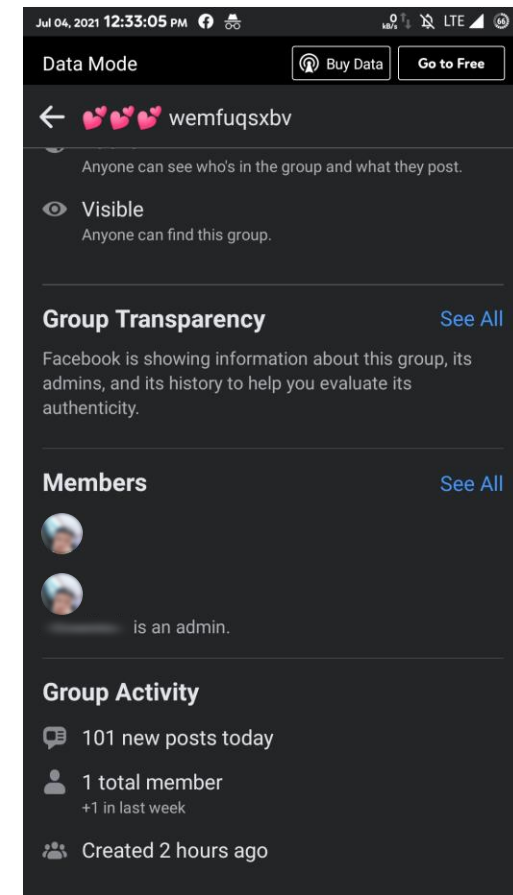
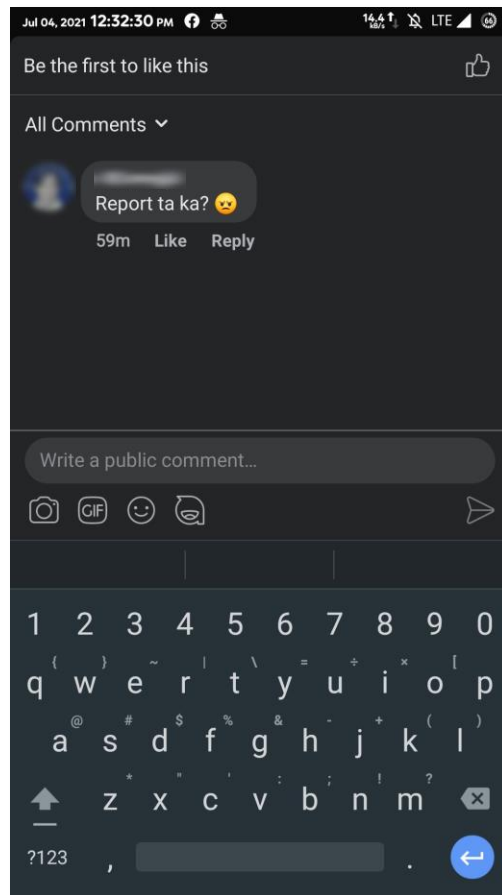
Phishing Awareness: Observing Intent

Phishing in 2021



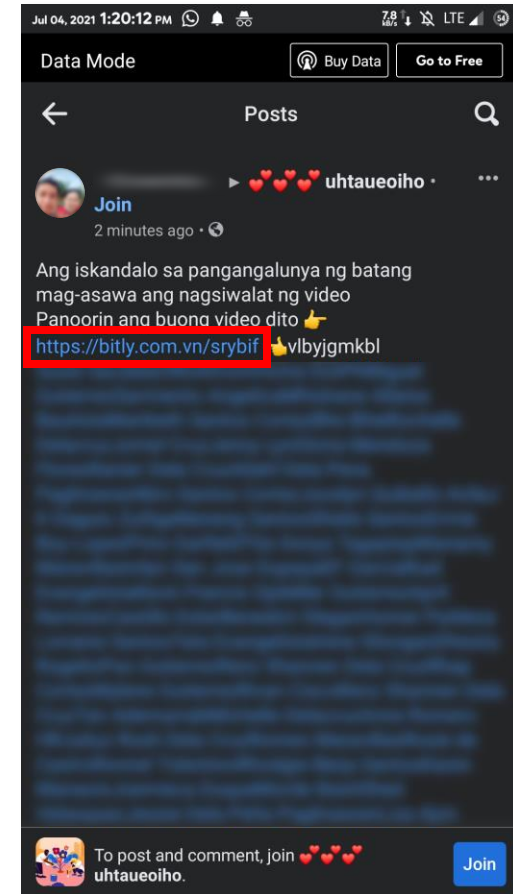
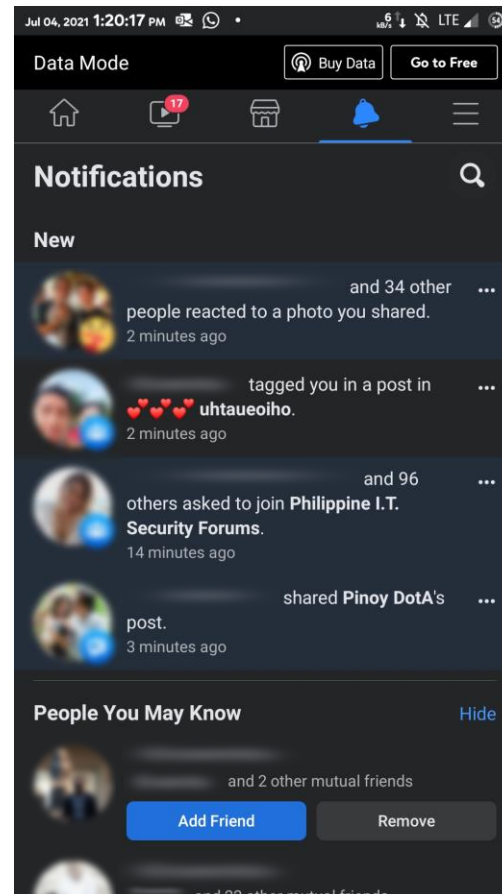
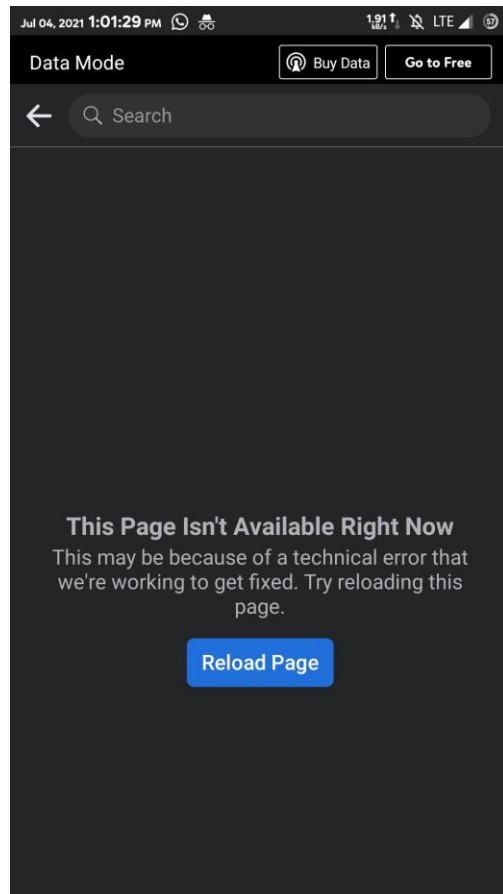
Phishing Awareness: Observing Intent

Phishing in 2021



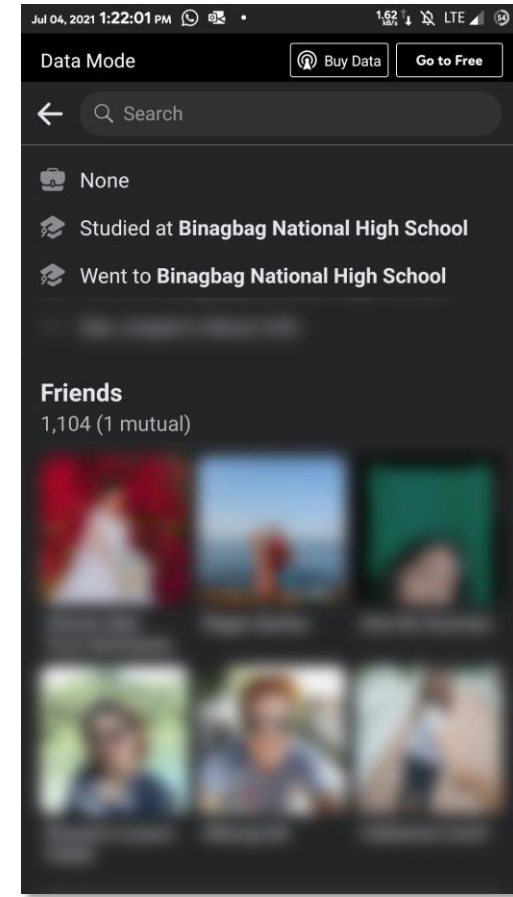
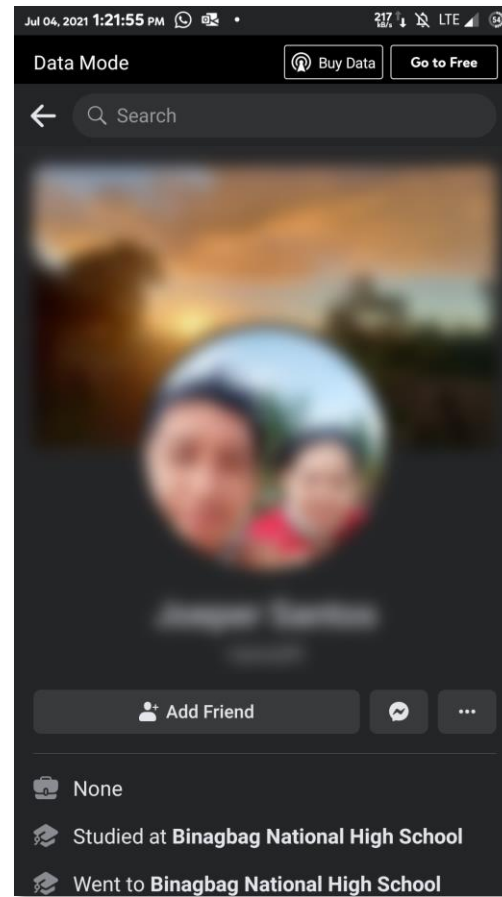
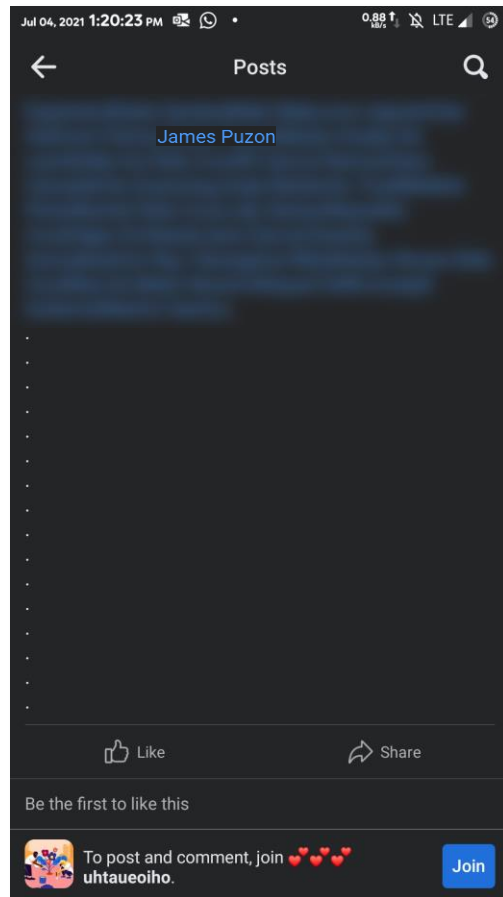
Phishing Awareness: Observing Intent

Phishing in 2021



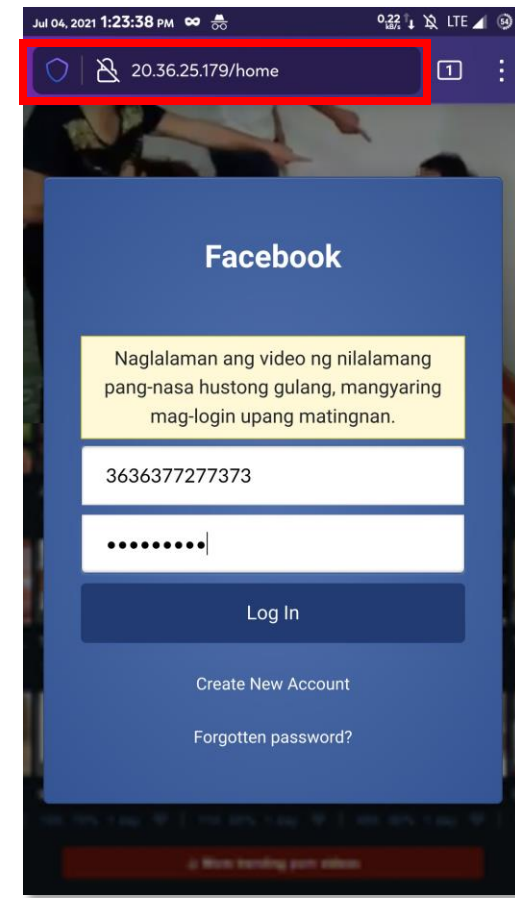
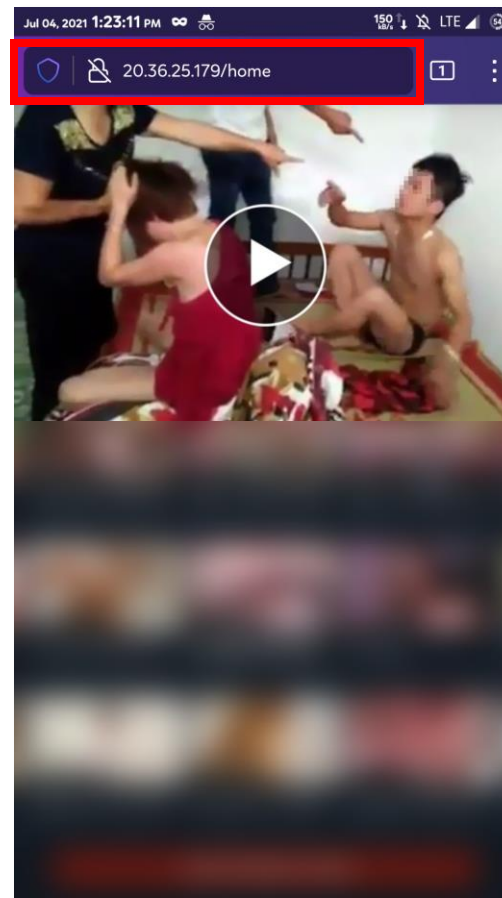
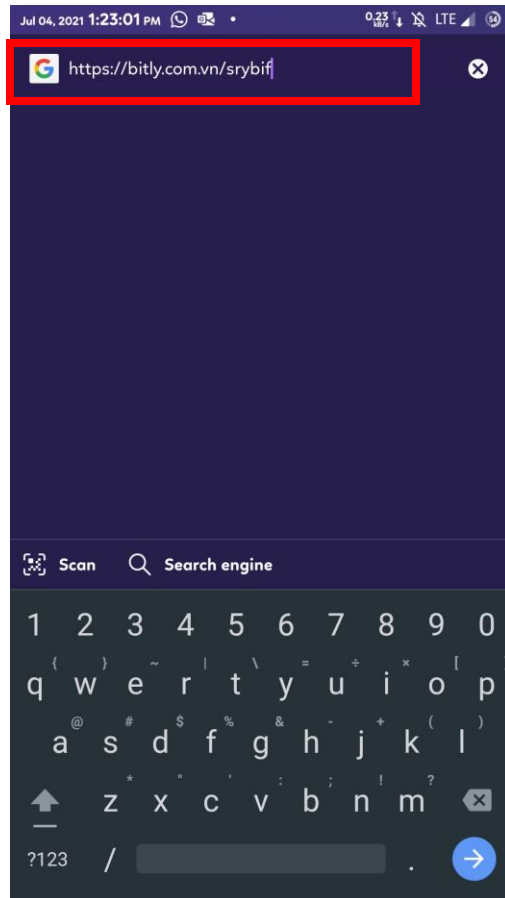
Phishing Awareness: Observing Intent

Phishing in 2021



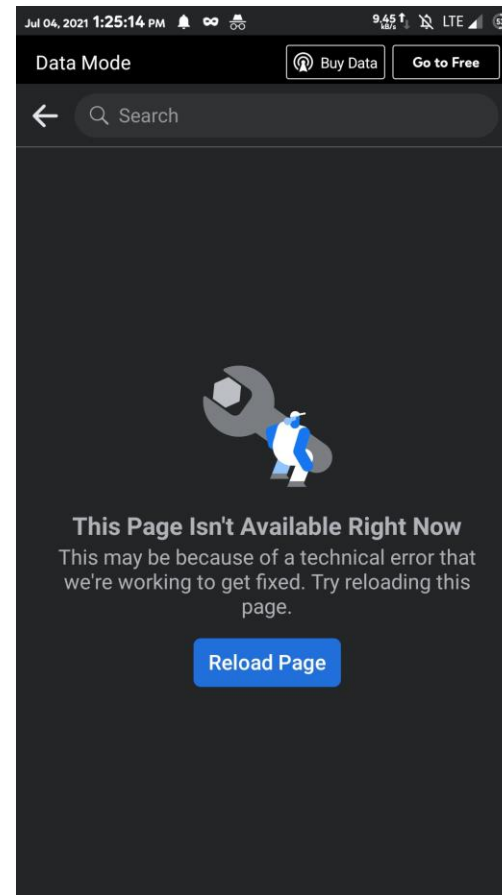
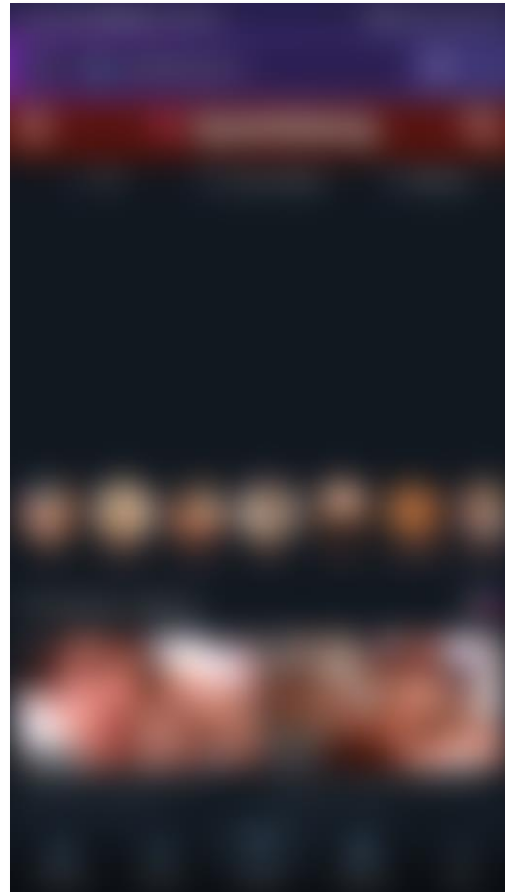
Phishing Awareness: Observing Intent

Phishing in 2021



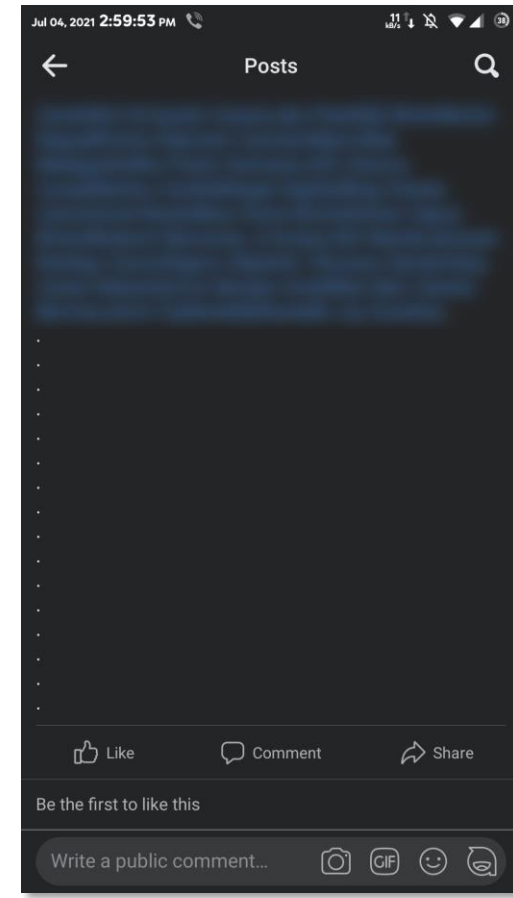
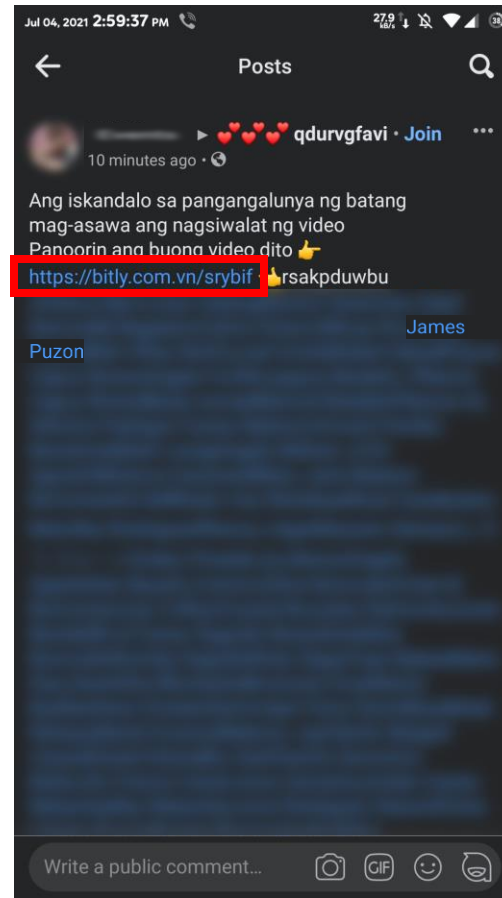
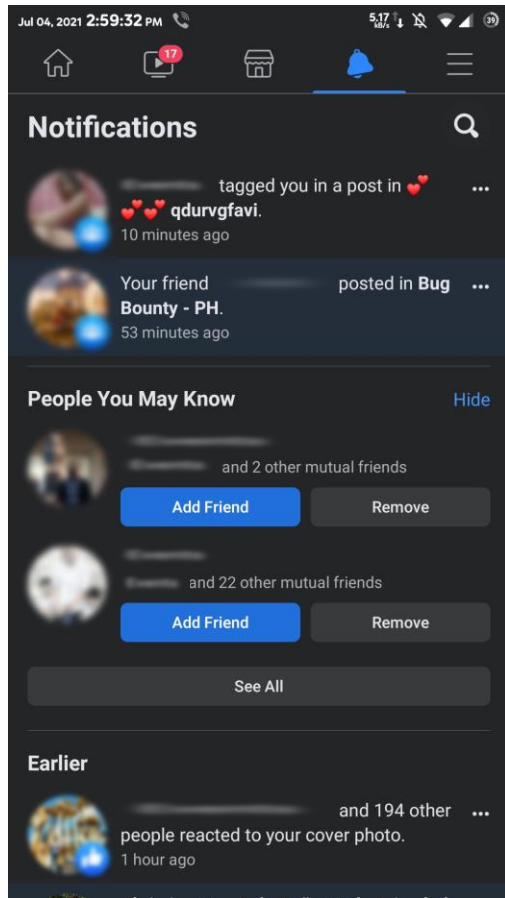
Phishing Awareness: Observing Intent

Phishing in 2021



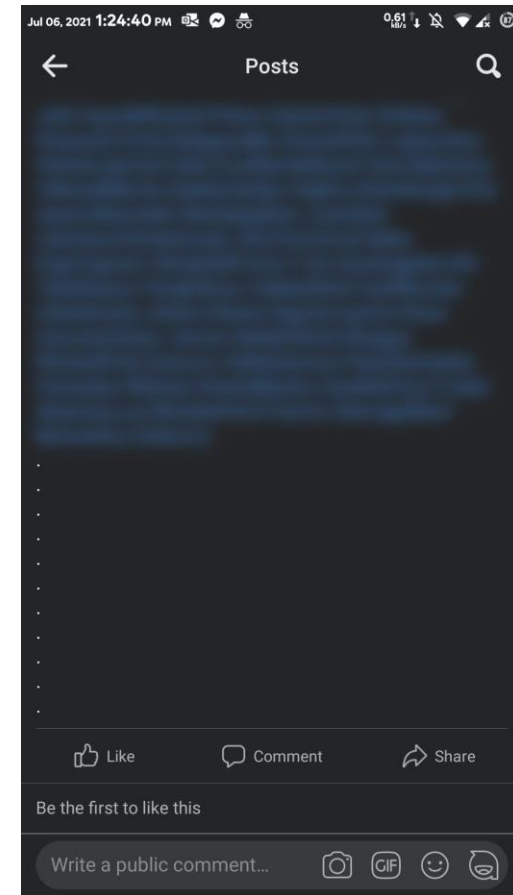
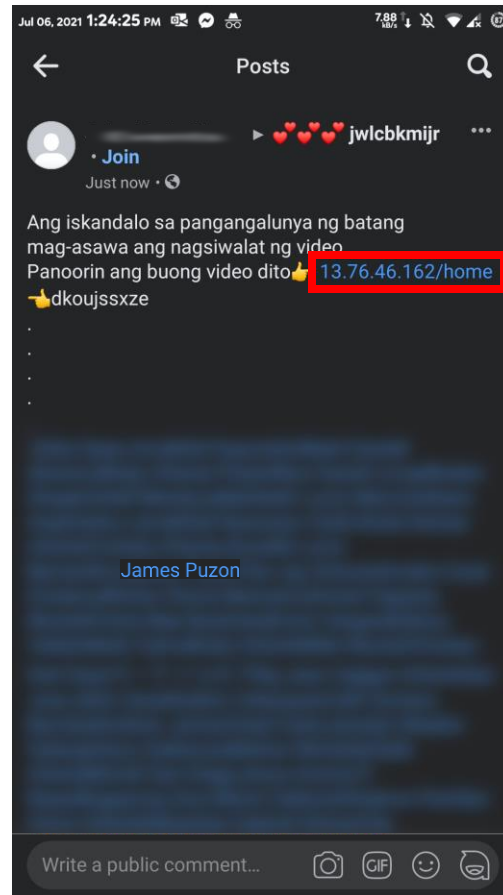
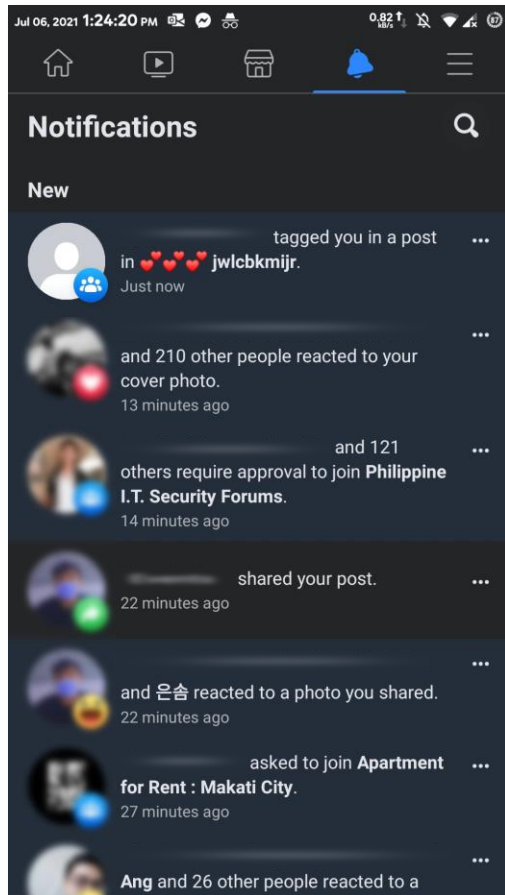
Phishing Awareness: Observing Intent

Phishing in 2021



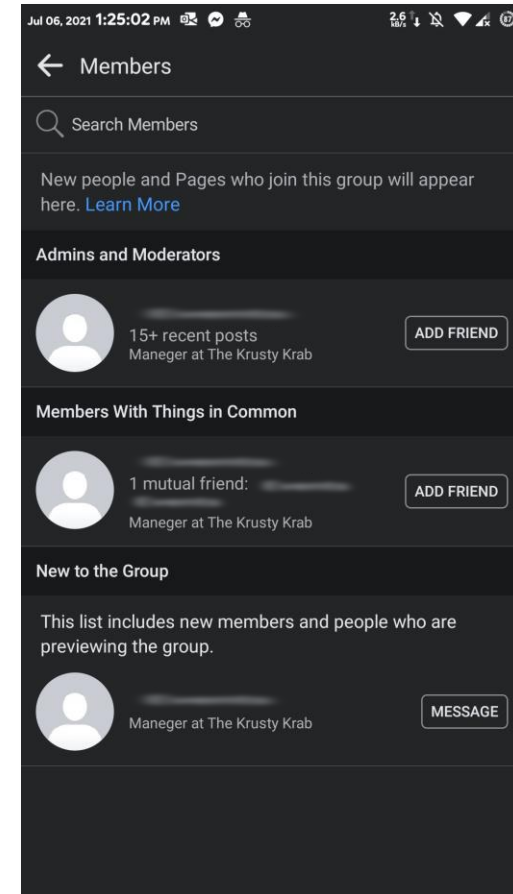
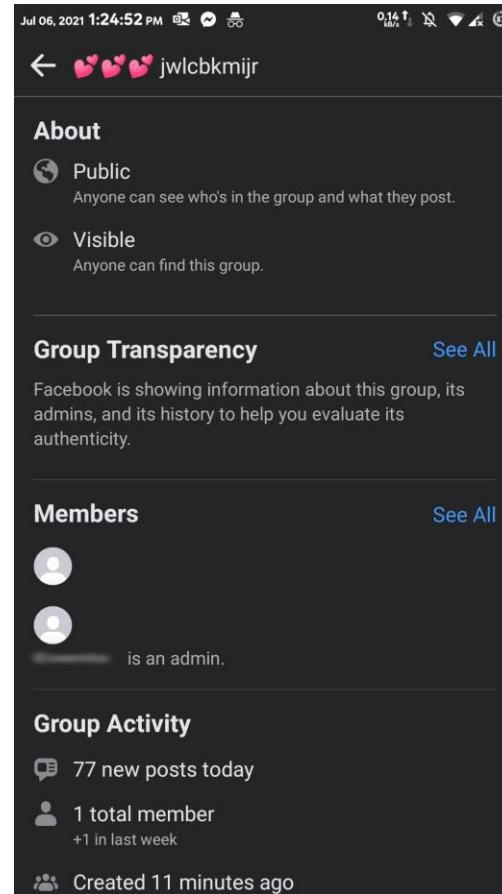
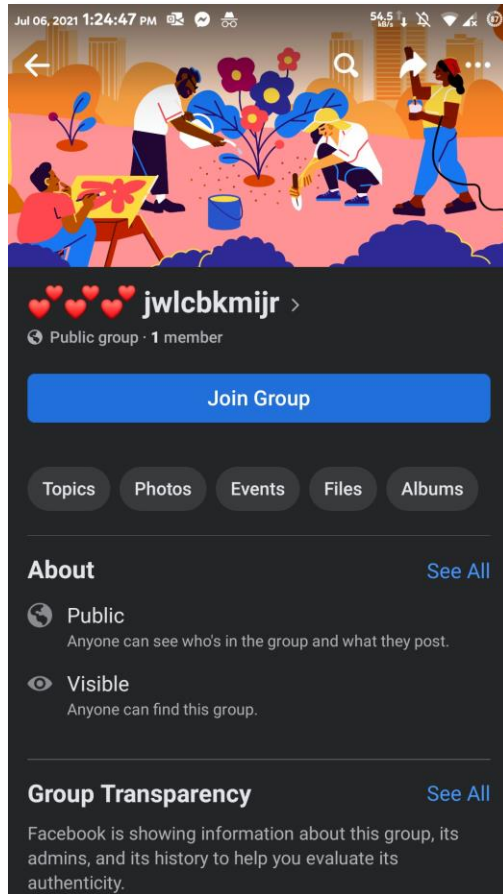
Phishing Awareness: Observing Intent

Phishing in 2021



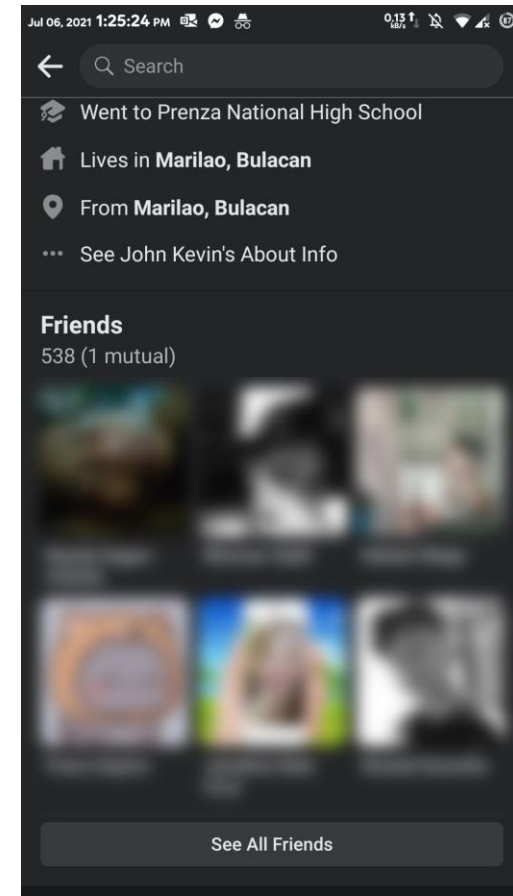
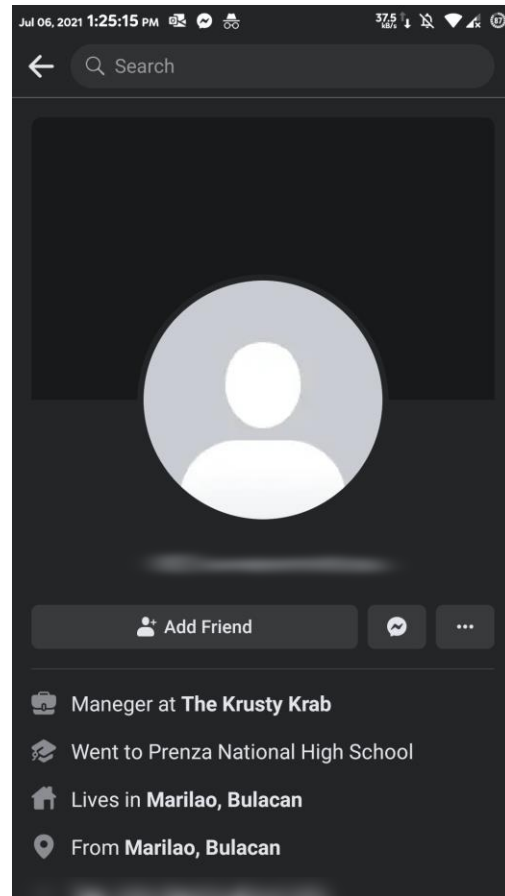
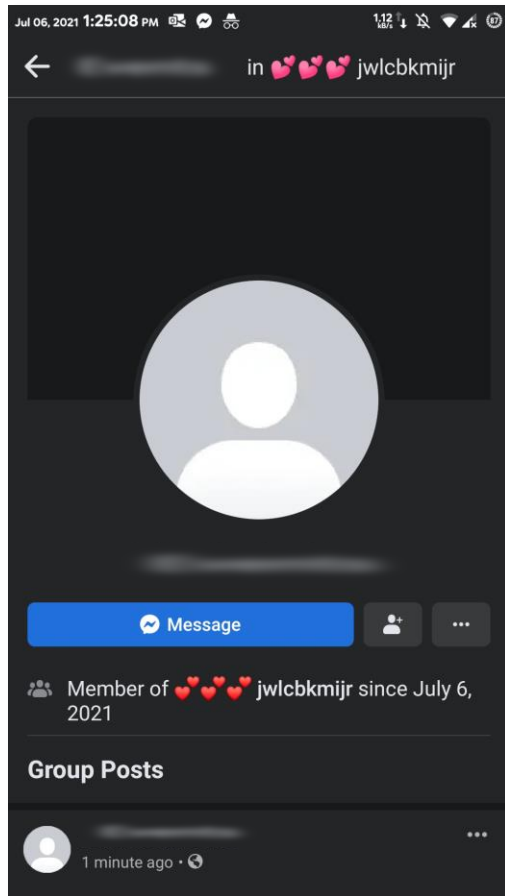
Phishing Awareness: Observing Intent

Phishing in 2021



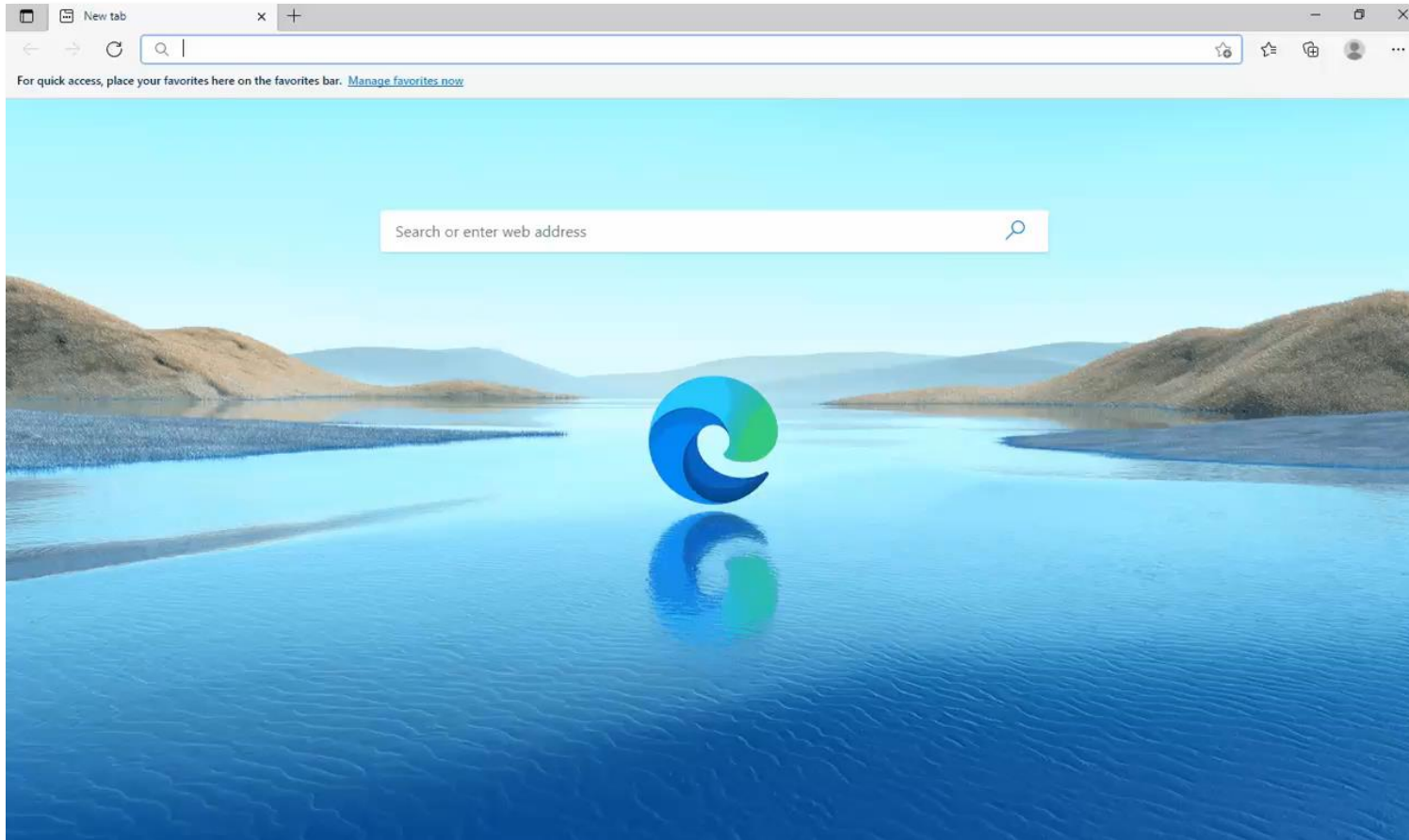
Phishing Awareness: Observing Intent

Phishing in 2021



Phishing Awareness: Old is New again

Phishing in 2021 (and beyond?)



References:

- <https://twitter.com/jq0904/status/1436155700212744211>



Phishing Awareness: Dealing with Phishing as an individual

They exploit our vulnerable nature (More brazenly in 2021)

- **Our lack of**
 - *Awareness*
 - *Knowledge*
 - *Discipline*
 - *Self-control*

- **Our vices**
 - *Greed*
 - *Envy*
 - *Impatience*

- **Etc.**

- **Our natural desires to**
 - *Help others*
 - *Feel good about ourselves*
 - *Be curious*
 - *Be Independent*



Phishing Awareness: Dealing with Phishing as an individual

They exploit our vulnerable nature (More brazenly in 2021)

- **Our lack of**
 - *Awareness*
 - *Knowledge*
 - *Discipline*
 - *Self-control*

 - **Our vices**
 - *Greed*
 - *Envy*
 - *Impatience*

 - **Etc.**
- **Our natural desires to**
 - *Help others*
 - *Feel good about ourselves*
 - *Be curious*
 - *Be Independent*

**What is happening
(personal observation)**

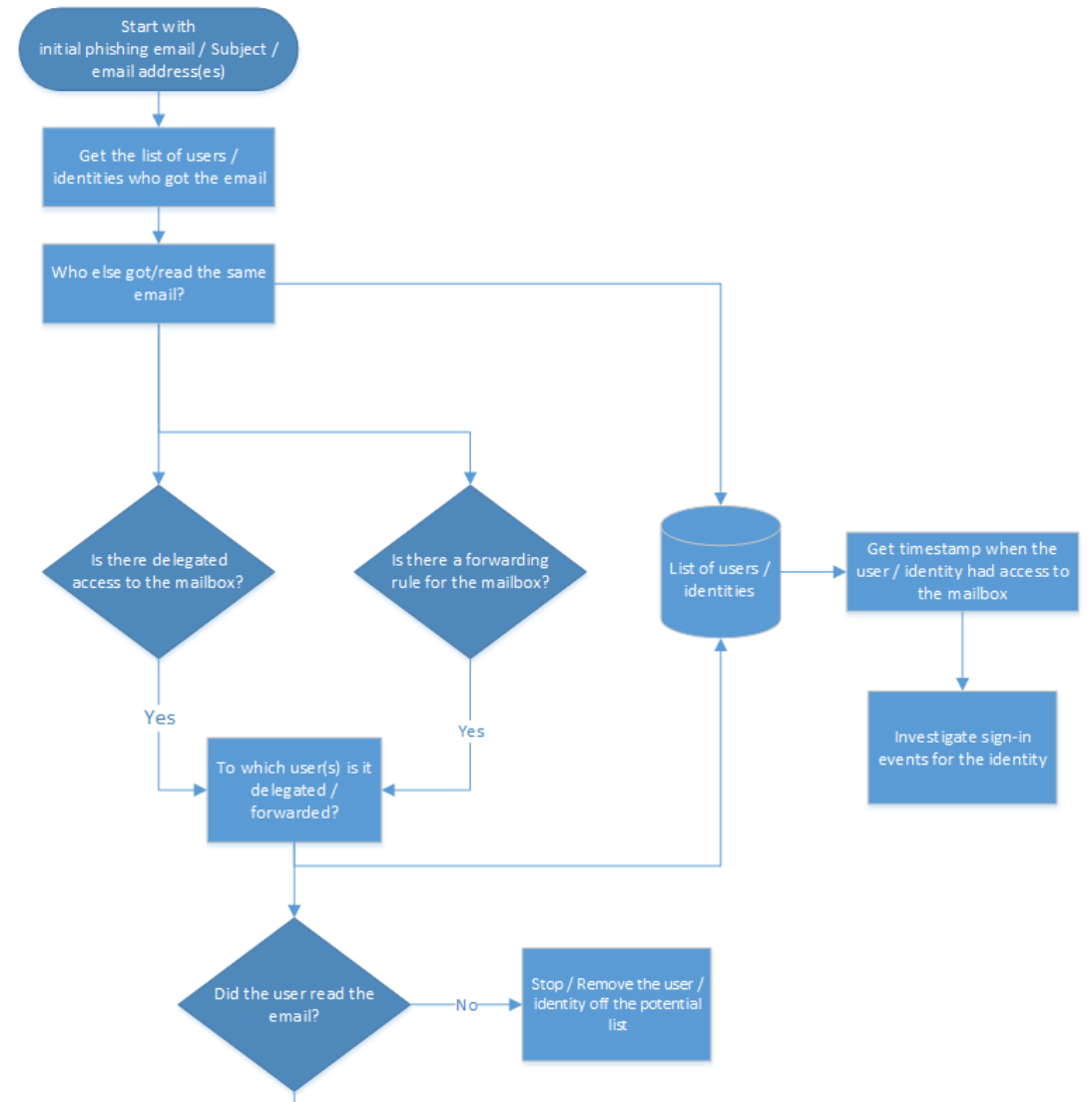
- *Eager blaming of victims*
- *No action after the fact*
- *No improvement*



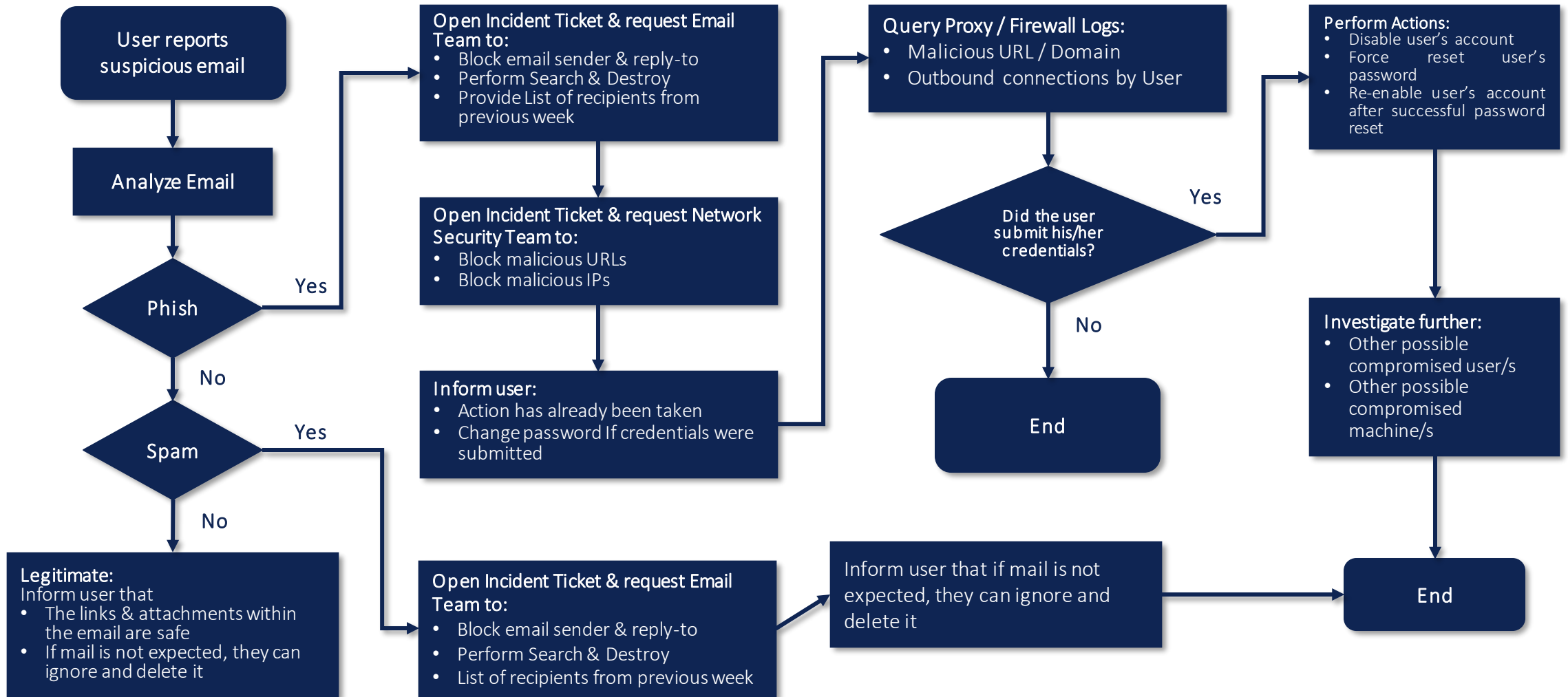
Phishing Awareness: Dealing with Phishing as an Organization

Incident Response Playbooks

- <https://docs.microsoft.com/en-us/security/compass/incident-response-playbooks>
- **Phishing**
 - <https://docs.microsoft.com/en-us/security/compass/incident-response-playbook-phishing>
 - <https://www.incidentresponse.com/playbooks/phishing>
 - <https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-phishing.md>



Phishing Awareness: Dealing with Phishing as an Organization



Phishing Awareness: Dealing with Phishing as an Organization

Standard Operating Procedure (from personal experience & understanding)

1. Perform Email Content Analysis (Mail Body & Mail Headers)
2. Preserve evidence (.eml/.msg file of report & phishing email, take hashes of both)
3. Block malicious Mail Sender
4. Block malicious URL
5. Check if other users were compromised within the organization
6. Perform forced password-reset & disable account/s of compromised user/s
7. Perform "Search & Destroy" of phishing emails

Dealing with criminal-hosted domains (from personal experience & understanding)

1. Determine WHOIS information (Is the information protected by WHOIS protection or not?)
2. Determine Domain Registrar (Do they require a Subpoena to process legal cases?)
3. Ensure evidence is preserved
4. Request that victim fill-up an incident report
5. Coordinate with Legal Department
6. File a Subpoena



Phishing Awareness: Dealing with Phishing as an Organization

Standard Operating Procedure (from personal experience & understanding)

1. Perform Email Content Analysis (Mail Body & Mail Headers)
2. Preserve evidence (.eml/.msg file of report & phishing email, take hashes of both)
3. Block malicious Mail Sender
4. Block malicious URL
5. Check if other users were compromised within the organization
6. Perform forced password-reset & disable account/s of compromised user/s
7. Perform "Search & Destroy" of phishing emails

Dealing with criminal-hosted domains (from personal experience & understanding)

1. Determine WHOIS information (Is the information protected by WHOIS protection or not?)
2. Determine Domain Registrar (Do they require a Subpoena to process legal cases?)
3. Ensure evidence is preserved
4. Request that victim fill-up an incident report
5. Coordinate with Legal Department
6. File a Subpoena
7. **Go to a corner and cry**



Phishing Awareness: Dealing with Phishing as an Organization

Standard Operating Procedure

1. Perform Email Content
2. Preserve evidence (.e
3. Block malicious Mail Se
4. Block malicious URL
5. Check if other users w
6. Perform forced passwo
7. Perform "Search & De

Dealing with criminal-ho

1. Determine WHOIS info
2. Determine Domain Re
3. Ensure evidence is pre
4. Request that victim fill
5. Coordinate with Legal
6. File a Subpoena
7. **Go to a corner and cry**

What Attackers are doing today	What your defenders will do today
1. Breach your network	1. Four hours of meetings
2. Monetize	2. Status Updates
	3. Add notes to tickets
	4. Timesheets
	5. HR mandated training
	6. close tickets as "False Positive"
	7. update slide decks
	8. update policies + KBs
	9. 23 minutes of Infosec work
Who will win?	

(Understanding)

(as of both)

er/s

(Understanding)

(protection or not?)

(legal cases?)



Phishing Awareness: Dealing with Phishing as an Organization

Ensure people are aware of legitimate references to your brand (organization) – Make them know *it's really you!*

Ensure people understand how you do business

Transparency is important

Be more proactive in enforcing policies



Phishing Awareness: Dealing with Phishing as an Organization

RFC 920 – Domain Requirements – Initial Set of Top Level Domains (1984)

GOV = Government, (e.g.: *.gov, *.gov.ph, *.gov.my, *.gov.sg, *.gov.uk, etc.)

EDU = Education, (e.g.: *.edu, *.edu.ph, *.edu.my, *.edu.sg, *.edu.hk, etc.)

COM = Commercial, (e.g.: *.com, *.com.ph, *.com.my, *.com.sg, *.com.hk, etc.)

MIL = Military, (e.g.: *.mil, *.mil.ph, *.mil.my, *.mil.tw, *.mil.uk, etc.)

ORG = Organization, any other domains meeting the second level requirements.

Countries = The English two letter code (alpha-2) identifying a country according to the ISO Standard for "Codes for the Representation of Names of Countries"



Phishing Awareness: Dealing with Phishing as an Organization

Consider the following:

- NLRC is currently a subdomain of DOLE – <https://nlrc.dole.gov.ph/>
- The DNS Admin of dole.gov.ph is the only one capable of managing nlrc.dole.gov.ph
 - Does DOLE & NLRC have an internal process for handling administration of nlrc.dole.gov.ph subdomain?
- Maybe NLRC can register & setup nlrc.gov.ph for themselves?
 - Does NLRC have personnel to manage their own web server / site?

Nag-share si [redacted] ng post.
Hunyo 17 nang 1:06 AM · 🌐

All hail Gmail.

 National Labor Relations Commission
NCR Arbitration Branch
Bookman Building, Quezon Avenue, Quezon City (near Banawe St.)
Sheriffs' Unit : 8740-7736 Public Assistance Center: 8781-7861

SHERIFF	EMAIL ADDRESS
1. ADRIANNE LOUISE L. ALDOVER	sheriffalldover@gmail.com
2. EDUARDO F. ARPON II	sheriffarpon@gmail.com
3. KENNETH A. ARTAJO	sheriffartajo@gmail.com
4. CHRISTIANSEN S. CASTEN	sheriffcasten@gmail.com
5. MARC CYRUS P. CRUZ	sheriffmarccruz@gmail.com
6. ANTONIO T. DATU, JR.	sheriffdatu@gmail.com
7. FERDINAND B. DELA CRUZ	sheriffdelacruz@gmail.com
8. HENRY O. GAGALANG, JR.	sheriffgagalang@gmail.com
9. EDMUND M. GUMBAN	sheriffgumban@gmail.com
10. JOHANN S. GUTIERREZ	sheriffgutierrez@gmail.com
11. REYMOND C. LOMUGDANG	sherifflomugdang@gmail.com
12. CARLOS G. MANUEL	sheriffcmanuel@gmail.com
13. MANOLITO G. MANUEL	sheriffmanolitomanuel@gmail.com
14. RYAN JESUS R. MARIANO	sheriffmariano@gmail.com
15. JONIE ANTHONY C. MONTES	sheriffjmontes@gmail.com
16. ARNOLD D. MUÑOZ	sheriffamunoz@gmail.com
17. NOLI S. NICDAO	sheriffnicdao@gmail.com
18. ALFREDO R. PAMBUAN	sheriffpambuan@gmail.com
19. JHON RAY P. PEREYRA	sheriffjhonraypereyra@gmail.com
20. JAMES B. POSADA	sheriffposada@gmail.com
21. VICENTE M. RAMOS, JR.	sheriffvramos@gmail.com
22. CHRISTOPHER D. ROMARATE	sheriffromarate@gmail.com
23. SHERWIN O. SINDAYEN	sheriffsindayen@gmail.com
24. TEOFILO BUTCH A. TAVERA	sheriffaverabutch@gmail.com
25. MANUEL T. TORRES, JR.	sheriffmtorres@gmail.com
26. JESUS G. VIDAL, JR.	sheriffvidal@gmail.com

facebook.com/nlrc.gov nlrcc.dole.gov.ph

NLRC
Hunyo 17 nang 12:44 AM · 🌐

Sheriffs. Email Addresses.

👍 550 46 na Comment 57 (na) Pagbabahagi



Phishing Awareness: Dealing with Phishing as an Organization

Consider the following:

- NLRC is currently a subdomain of DOLE – <https://nlrc.dole.gov.ph/>
- The DNS Admin of dole.gov.ph is the only one capable of managing nlrc.dole.gov.ph
 - Does DOLE & NLRC have an internal process for handling administration of nlrc.dole.gov.ph subdomain?
- Maybe NLRC can register & setup nlrc.gov.ph for themselves?
 - Does NLRC have personnel to manage their own web server / site?

Nag-share si [redacted] ng post.
Hunyo 17 nang 1:06 AM · 🌐

All hail Gmail.

National Labor Relations Commission
NCR Arbitration Branch
Bookman Building, Quezon Avenue, Quezon City (near Banawe St.)
Sheriffs' Unit : 8740-7736 · Public Assistance Center: 8781-7861

SHERIFF	EMAIL ADDRESS
1. ADRIANNE LOUISE L. ALDOVER	sheriffal Dover@gmail.com
2. EDUARDO F. ARPON II	sheriffarpon@gmail.com
3. KENNETH A. ARTAJA	sheriffartaj@gmail.com
4. CHRISTIANSEN S. CASTEN	sheriffcasten@gmail.com
5. MARC CYRUS P. CRUZ	sheriffmarccruz@gmail.com
6. ANTONIO T. DATU, JR.	sheriffdatu@gmail.com
7. FERDINAND B. DELA CRUZ	sheriffdelacruz@gmail.com
8. HENRY O. GAGALANG, JR.	sheriffgagalang@gmail.com
9. EDMUND M. GUMBAN	sheriffgumban@gmail.com
10. JOHANN S. GUTIERREZ	sheriffgutierrez@gmail.com
11. REYMOND C. LOMUGDANG	sherifflomugdang@gmail.com
12. CARLOS G. MANUEL	sheriffcmanuel@gmail.com
13. MANOLITO G. MANUEL	sheriffmanolitomanuel@gmail.com
14. RYAN JESUS R. MARIANO	sheriffmariano@gmail.com
15. JONIE ANTHONY C. MONTES	sheriffmontes@gmail.com
16. ARNOLD D. MUÑOZ	sheriffarnoldmuñoz@gmail.com
17. NOLI S. NICDAO	sheriffnicdao@gmail.com
18. ALFREDO R. PAMBUAN	sheriffpambuan@gmail.com
19. JHON RAY P. PEREYRA	sheriffjohnraypereyra@gmail.com
20. JAMES B. POSADA	sheriffposada@gmail.com
21. VICENTE M. RAMOS, JR.	sherifframosjr@gmail.com
22. CHRISTOPHER D. ROMARATE	sheriffromarate@gmail.com
23. SHERWIN O. SINDAYEN	sheriffsindayen@gmail.com
24. TEOFILO BUTCH A. TAVERA	sheriffbutchtavera@gmail.com
25. MANUEL T. TORRES, JR.	sheriffmtorresjr@gmail.com
26. JESUS G. VIDAL, JR.	sheriffvidaljr@gmail.com

facebook.com/nlrc.gov · nlrc.dole.gov.ph

NLRC
Hunyo 17 nang 12:44 AM · 🌐

Sheriffs. Email Addresses.

👍 550 46 na Comment 57 (na) Pagbabahagi



Phishing Awareness: Dealing with Phishing as an Organization

Consider the following:

- NLRC is currently a subdomain of DOLE – <https://nlrc.dole.gov.ph/>
- The DNS Admin of dole.gov.ph is the only one capable of managing nlrc.dole.gov.ph
 - Does DOLE & NLRC have an internal process for handling administration of nlrc.dole.gov.ph subdomain?
- Maybe NLRC can register & setup nlrc.gov.ph for themselves?
 - Does NLRC have personnel to manage their own web server / site?
- What about other government agencies with a similar issue?



Phishing Awareness: Dealing with Phishing as an Organization



Phishing Awareness: Dealing with Phishing as an Organization

Nag-share si ng post.
Hunyo 17 nang 1:06 AM -

All hail Gmail.

National Labor Relations Commission
NCR Arbitration Branch
Bookman Building, Quezon Avenue, Quezon City (near Banawe St.)
Sheriffs' Unit : 8740-7736 Public Assistance Center: 8781-7861

SHERIFF	EMAIL ADDRESS
1. ADRIANNE LOUISE L. ALDOVER	sheriffalcover@gmail.com
2. EDUARDO F. ARPON II	sheriffarpon@gmail.com
3. KENNETH A. ARTAJA	sheriffartajo@gmail.com
4. CHRISTIANSEN S. CASTEN	sheriffcasten@gmail.com
5. MARC CYRUS P. CRUZ	sheriffmrcruz@gmail.com
6. ANTONIO T. DATU, JR.	sheriffdatu@gmail.com
7. FERDINAND B. DELA CRUZ	sheriffdelacruz@gmail.com
8. HENRY O. GAGALANG, JR.	sheriffgagalang@gmail.com
9. EDMUND M. GUMBAN	sheriffgumban@gmail.com
10. JOHANN S. GUTIERREZ	sheriffgutierrez@gmail.com
11. REYMOND C. LOMUGDANG	sherifflomugdang@gmail.com
12. CARLOS G. MANUEL	sheriffcmanuel@gmail.com
13. MANOLITO G. MANUEL	sheriffmanolitomanuel@gmail.com
14. RYAN JESUS R. MARIANO	sheriffmriano@gmail.com
15. JONIE ANTHONY C. MONTES	sheriffmontes@gmail.com
16. ARNOLD D. MUÑOZ	sheriffmunoz@gmail.com
17. NOLI S. NICDAO	sheriffnicdao@gmail.com
18. ALFREDO R. PAMBUAN	sheriffpambuan@gmail.com
19. JHON RAY P. PEREYRA	sheriffjhraypereyra@gmail.com
20. JAMES B. POSADA	sheriffposada@gmail.com
21. VICENTE M. RAMOS, JR.	sheriffvramos@gmail.com
22. CHRISTOPHER D. ROMARATE	sheriffromarate@gmail.com
23. SHERWIN O. SINDAYEN	sheriffsindayen@gmail.com
24. TEOFILO BUTCH A. TAVERA	sheriffataverabutch@gmail.com
25. MANUEL T. TORRES, JR.	sheriffmtorres@gmail.com
26. JESUS G. VIDAL, JR.	sheriffvidal@gmail.com

facebook.com/nlrc.gov nlrc.dole.gov.ph

NLRC
Hunyo 17 nang 12:44 AM -

Sheriffs. Email Addresses.

550 46 na Comment 57 (na) Pagbabahagi



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY



.gov.ph Domain Registration

Philippine Standard Time:
Sunday, June 20, 2021, 1:49:31 AM

1. Download the appropriate form for your concern.

- [NEW .gov.ph Domain Application](#)

For new applications, the requesting agency is required to submit by email, written in the agency's letterhead, an official letter stating that you are given permission to register the particular domain name for that agency. The letter should be duly signed by any of the following: Agency Head, Chief Information Officer, or the MIS Head. The request letter should be addressed to:

.gov.ph Administrator
Department of Information and Communications Technology
DICT Bldg., C.P. Garcia, Diliman, Quezon City
PHILIPPINES 1101

- [.gov.ph Domain Registry Modification](#)
- [.gov.ph Domain Deactivation](#)

2. Accomplish the form. Details in the form should be specific and correct and should be written legibly.

3. Send the accomplished form to dns@dict.gov.ph and wait for an email notification from the .gov.ph Domain Administrator.

Please read the [DNS Naming Policy](#) to know if you are qualified for a .gov.ph domain sub-delegation

References:

- <https://dns.gov.ph/>
- <https://www.facebook.com/nlrc.gov/posts/4249646861722243>



Phishing Awareness: Dealing with Phishing as an Organization

Consider the following:

- NLRC is currently a subdomain of DOLE – <https://nlrc.dole.gov.ph/>
- The DNS Admin of dole.gov.ph is the only one capable of managing nlrc.dole.gov.ph
 - Does DOLE & NLRC have an internal process for handling administration of nlrc.dole.gov.ph subdomain?
- Maybe NLRC can register & setup nlrc.gov.ph for themselves?
 - Does NLRC have personnel to manage their own web server / site?
- What about other government agencies with a similar issue?
- What about educational institutions with a similar issue?

Nag-share si [redacted] ng post.
Hunyo 17 nang 1:06 AM · 🌐

All hail Gmail.

 National Labor Relations Commission
NCR Arbitration Branch
Bookman Building, Quezon Avenue, Quezon City (near Banawe St.)
Sheriffs' Unit : 8740-7736 · Public Assistance Center: 8781-7861

SHERIFF	EMAIL ADDRESS
1. ADRIANNE LOUISE L. ALDOVER	sheriffalover@gmail.com
2. EDUARDO F. ARPON II	sheriffarpon@gmail.com
3. KENNETH A. ARTAJO	sheriffartajo@gmail.com
4. CHRISTIANSEN S. CASTEN	sheriffcasten@gmail.com
5. MARC CYRUS P. CRUZ	sheriffmascruz@gmail.com
6. ANTONIO T. DATU, JR.	sheriffdatu@gmail.com
7. FERDINAND B. DELA CRUZ	sheriffdelacruz@gmail.com
8. HENRY O. GAGALANG, JR.	sheriffgagalang@gmail.com
9. EDMUND M. GUMBAN	sheriffgumban@gmail.com
10. JOHANN S. GUTIERREZ	sheriffgutierrez@gmail.com
11. REYMOND C. LOMUGDANG	sherifflomugdang@gmail.com
12. CARLOS G. MANUEL	sheriffcmanuel@gmail.com
13. MANOLITO G. MANUEL	sheriffmanolitomanuel@gmail.com
14. RYAN JESUS R. MARIANO	sheriffmariano@gmail.com
15. JONIE ANTHONY C. MONTES	sheriffmontes@gmail.com
16. ARNOLD D. MUÑOZ	sheriffarnoldmuñoz@gmail.com
17. NOLI S. NICDAO	sheriffnicdao@gmail.com
18. ALFREDO R. PAMBUAN	sheriffpambuan@gmail.com
19. JHON RAY P. PEREYRA	sheriffjohnraypereyra@gmail.com
20. JAMES B. POSADA	sheriffposada@gmail.com
21. VICENTE M. RAMOS, JR.	sherifframosjr@gmail.com
22. CHRISTOPHER D. ROMARATE	sheriffromarate@gmail.com
23. SHERWIN O. SINDAYEN	sheriffsindayen@gmail.com
24. TEOFILO BUTCH A. TAVERA	sheriffbutchtavera@gmail.com
25. MANUEL T. TORRES, JR.	sheriffmtorresjr@gmail.com
26. JESUS G. VIDAL, JR.	sheriffvidaljr@gmail.com

facebook.com/nlrc.gov · nlrc.dole.gov.ph

NLRC
Hunyo 17 nang 12:44 AM · 🌐
Sheriffs. Email Addresses.

👍 550 46 na Comment 57 (na) Pagbabahagi



Phishing Awareness: Dealing with Phishing as an Organization



EDU.PH Registration Form

1. Read the [Service Agreement](#) which governs this service. If you agree with it, proceed to the next steps.
2. Ensure that the domain you wish to register is still available. You may [check](#) it here.
3. Fill up the [registration form](#) below to generate a request. Our system immediately email a Verification Form to **Your Email Address** found in this form. Do not use a Yahoo- or a Microsoft-based email address. Their email systems modify our Verification Form. Please make sure that you only use English letters in the form (e.g. do not use "enye (n~)") because our Verification System will reject your form later on.
4. Reply to the Verification Form emailed to you. Do **not** make any modifications to the Form. Be sure that your email client does not make any modifications to the Form. The slightest modification will invalidate the Form. After we receive this reply, we will mark the new DNS registration as "PENDING." You then have one (1) week to comply with all of the following requirements:
 1. Show proof that the school is an educational/training institution recognized by the government. As proof, we will accept an emailed copy of the school's DepEd/CHED/TESDA recognition paper(s) or Republic Act (for SUCs).
 2. Show proof that the school has given you permission to register the particular domain name for the school. Please email a letter from the school's president or principal, written on the school's letterhead, authorizing the registration of the domain name.
 3. Pay the DNS registration fee **after** you have completed the online registration. You will received an email from our system stating that your registration is "PENDING" when you have completed the online registration.

A "PENDING" registration which fails to meet all of the above requirements after the one week (seven calendar days) period is automatically deleted from our databases without any notice.

A "PENDING" registration is activated usually on the same work day when all the requirements are fulfilled. The notice of activation is then emailed to the domain's administrative and technical contacts. If your registration is not activated on the same day, please email our tech support to call our attention.

All emails must not exceed 2MB in size and must be sent to support AT ph.net

Our tech support can not provide you a tutorial on how the DNS works. Please take the time to read this Wikipedia [article](#) on how the DNS works.

Visit <http://services.ph.net/payment.html> for the payment details. Confused? Visit the [FAQ Page](#) for more information.

EDU.PH DNS Registration

Note: DNS servers are limited to 65 chars. All others are 50 characters.

General Information (Required)

Your Email Address	<input type="text"/> <small>After you successfully complete this form, the generated form will be automatically emailed to this address for verification together with further instructions. New registrants must double-check that they can receive email through this address. Do not use a Yahoo or a MS-based email address. (e.g. yourname@yourisp.com)</small>
Complete Domain Name	<input type="text"/> <small>The complete domain name you intend to register (e.g. school.edu.ph)</small>

References:

- <http://services.ph.net/dns/registration.pl>



Phishing Awareness: Dealing with Phishing as an Organization

Consider the following:

- NLRC is currently a subdomain of DOLE – <https://nlrc.dole.gov.ph/>
- The DNS Admin of dole.gov.ph is the only one capable of managing nlrc.dole.gov.ph
 - Does DOLE & NLRC have an internal process for handling administration of nlrc.dole.gov.ph subdomain?
- Maybe NLRC can register & setup nlrc.gov.ph for themselves?
 - Does NLRC have personnel to manage their own web server / site?
- What about other government agencies with a similar issue?
- What about educational institutions with a similar issue?
- What about private entities with a similar issue?

Nag-share si [redacted] ng post.
Hunyo 17 nang 1:06 AM · 🌐

All hail Gmail.

National Labor Relations Commission
NCR Arbitration Branch
Bookman Building, Quezon Avenue, Quezon City (near Banawe St.)
Sheriffs' Unit : 8740-7736 Public Assistance Center: 8781-7861

SHERIFF	EMAIL ADDRESS
1. ADRIANNE LOUISE L. ALDOVER	sheriffalldover@gmail.com
2. EDUARDO F. ARPON II	sheriffarpon@gmail.com
3. KENNETH A. ARTAJO	sheriffartajo@gmail.com
4. CHRISTIANSEN S. CASTEN	sheriffcasten@gmail.com
5. MARC CYRUS P. CRUZ	sheriffmarccruz@gmail.com
6. ANTONIO T. DATU, JR.	sheriffdatu@gmail.com
7. FERDINAND B. DELA CRUZ	sheriffdelacruz@gmail.com
8. HENRY O. GAGALANG, JR.	sheriffgagalang@gmail.com
9. EDMUND M. GUMBAN	sheriffgumban@gmail.com
10. JOHANN S. GUTIERREZ	sheriffgutierrez@gmail.com
11. REYMOND C. LOMUGDANG	sherifflomugdang@gmail.com
12. CARLOS G. MANUEL	sheriffcmanuel@gmail.com
13. MANOLITO G. MANUEL	sheriffmanolitomanuel@gmail.com
14. RYAN JESUS R. MARIANO	sheriffmariano@gmail.com
15. JONIE ANTHONY C. MONTES	sheriffjmontes@gmail.com
16. ARNOLD D. MUÑOZ	sheriffamunoz@gmail.com
17. NOLI S. NICDAO	sheriffnicdao@gmail.com
18. ALFREDO R. PAMBUAN	sheriffpambuan@gmail.com
19. JHON RAY P. PEREYRA	sheriffjhonraypereyra@gmail.com
20. JAMES B. POSADA	sheriffposada@gmail.com
21. VICENTE M. RAMOS, JR.	sheriffvramos@gmail.com
22. CHRISTOPHER D. ROMARATE	sheriffromarate@gmail.com
23. SHERWIN O. SINDAYEN	sheriffsindayen@gmail.com
24. TEOFILO BUTCH A. TAVERA	sheriffaverabutch@gmail.com
25. MANUEL T. TORRES, JR.	sheriffmtorres@gmail.com
26. JESUS G. VIDAL, JR.	sheriffvidal@gmail.com

facebook.com/nlrc.gov nlrcc.dole.gov.ph

NLRC
Hunyo 17 nang 12:44 AM · 🌐

Sheriffs. Email Addresses.

👍 550 46 na Comment 57 (na) Pagbabahagi



There will never be a Solution until people acknowledge there is a Problem




There will never be a Solution until people acknowledge there is a Problem

At times people listen not to what is said, but on how, when & where it was said



Phishing Awareness: Eschewing Ambiguity

Pinned Tweet

 **Kevin Beaumont** @GossiTheDog · Jul 3

I realise this was a long read and almost nobody read it, but I do feel like a career in cybersecurity is basically standing on a bridge watching it burn down, which feels like being quite a lonely voice.

The situation is not sustainable.

doublepulsar.com/the-hard-truth...

With ransomware gangs running around with multi-million dollar budgets, it gives them the ability to buy exploits and tools from exploit brokers at a scale normally reserved for states and nation states. While states take calculated risks in cyber intrusion operations — for example, covert spying — ransomware gangs are driven by operational impacts.

In short, it is like giving rocket launchers to teenagers. This problem is not going to suddenly, magically stop. It is going to get worse. The recruitment cycle for more capabilities is accelerating, to the point where small groups of gangs are finding ways around security controls and exploring zero day exploits, which vendors have always struggled to realistically detect.

50 357 927

[Show this thread](#)

The hard truth about ransomware: we aren't prepared, it's a battle with new rules, and it hasn't near reached peak impact.




References:

- <https://twitter.com/GossiTheDog/status/1411316938182205441>
- <https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasn-t-a93ad3030a54>

Phishing Awareness: Eschewing Ambiguity

Pinned Tweet

 **Kevin Beaumont** @GossiTheDog · Jul 3

I realise this was a long read and almost nobody read it, but I do feel like a career in cybersecurity is basically standing on a bridge watching it burn down, which feels like being quite a lonely voice.

The situation is not sustainable.

doublepulsar.com/the-hard-truth...

With ransomware gangs running around with multi-million dollar budgets, it gives them the ability to buy exploits and tools from exploit brokers at a scale normally reserved for states and nation states. While states take calculated risks in cyber intrusion operations — for example, covert spying — ransomware gangs are driven by operational impacts.

In short, it is like giving rocket launchers to teenagers. This problem is not going to suddenly, magically stop. It is going to get worse. The recruitment cycle for more capabilities is accelerating, to the point where small groups of gangs are finding ways around security controls and exploring zero day exploits, which vendors have always struggled to realistically detect.

50 357 927

Show this thread

The hard truth about ransomware: we aren't prepared, it's a battle with new rules, and it hasn't near reached peak impact.



References:

- <https://twitter.com/GossiTheDog/status/1411316938182205441>
- <https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasn-t-a93ad3030a54>



Phishing Awareness: Eschewing Ambiguity

Pinned Tweet

Kevin Beaumont ✓
I realise this was a low point in my career in cybersecurity, which feels like I've been punched down, which feels like I've been punched down.

The situation is not so simple. It's a double-edged sword. doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasnt-reached-peak-impact/

With ransomware getting more sophisticated, it gives them the ability to do things on a scale normally reserved for nation states. The calculated risks in cyberspace — ransomware gangs — are increasing.

In short, it is like giving a person a gun and saying, "You're going to suddenly, magically stop. It is going to get worse. The recruitment cycle for more capabilities is accelerating, to the point where small groups of gangs are finding ways around security controls and exploring zero day exploits, which vendors have always struggled to realistically detect."

50 357 927

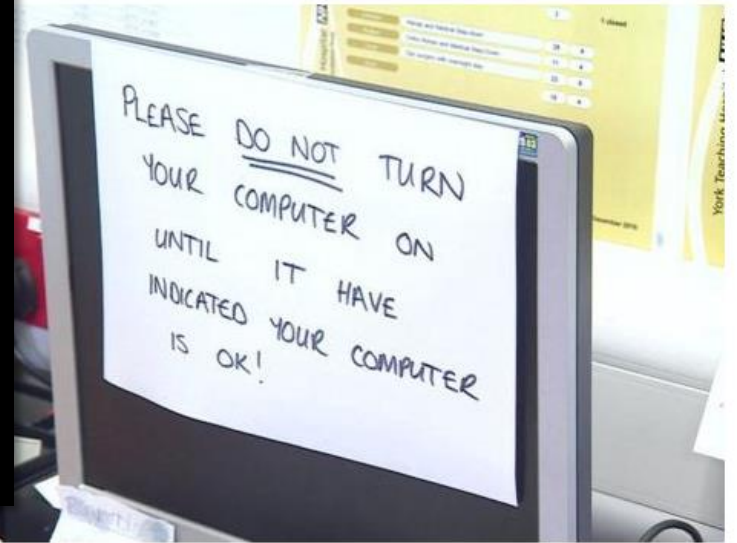
Show this thread

Kevin Beaumont ✓ @GossiTheDog · Jul 4
Btw this was never a manifesto for 'let's quit'; it's the opposite. It also wasn't a call for MS to be a charity. It's a '..we're getting into a mess, this is going to become a crisis for society, we need to lift people up'

Kevin Beaumont ✓ @GossiTheDog · Jul 4
Replying to @tinker_bell512
No. We double down. We press vendors and product owners to be more accountable and invest properly, not just in profits but customer protection. We press governments to do more, we take more action.

2 5 68

The hard truth about ransomware: we aren't prepared. It's a battle with new rules, and it hasn't reached peak impact.



References:

- <https://twitter.com/GossiTheDog/status/1411316938182205441>
- <https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasnt-reached-peak-impact/>



Phishing Awareness: Eschewing Ambiguity

Pinned Tweet

Kevin Beaumont ✓
I realise this was a low point in my career in cybersecurity, which feels like I've been let down, which feels like I've been let down.

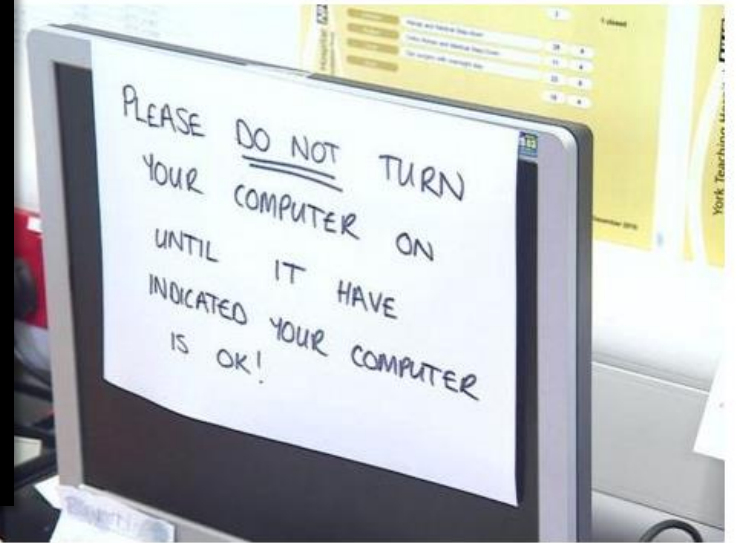
Kevin Beaumont ✓ @GossiTheDog · Jul 4
Btw this was never a manifesto for 'let's quit'; it's the opposite. It also wasn't a call for MS to be a charity. It's a '..we're getting into a mess, this is going to become a crisis for society, we need to lift ourselves out of it'.

Kevin Beaumont ✓ @GossiTheDog
Replying to @tinker_bell512
No. We double down. We press vendors and product owners to be more accountable and invest properly, not just in profits but customer protection. We press governments to do more, we take more action.

7:43 AM · Jul 4, 2021 · Twitter Web App

8 Retweets 2 Quote Tweets 50 Likes

The hard truth about ransomware: we aren't in a battle with new rules, and it has reached peak impact.



owners to be more accountable but customer protection more action.

- References:
- <https://twitter.com/GossiTheDog/status/1411316938182205441>
 - <https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasnt-reached-peak-impact/>





COVENANT OF GRACE INTEGRATED ACADEMY, INC.

Block 10 Lot 1 Aurora Pijuan St., corner Pilar Pilapil St., BF Resort Village, Talon 2, Las Piñas

Telephone Nos.: 8873-0629 / 7501-6033 E-mail: inquiry@cogia.edu.ph Website: <https://cogia.edu.ph>

Your Partner in Preparing Children for Life



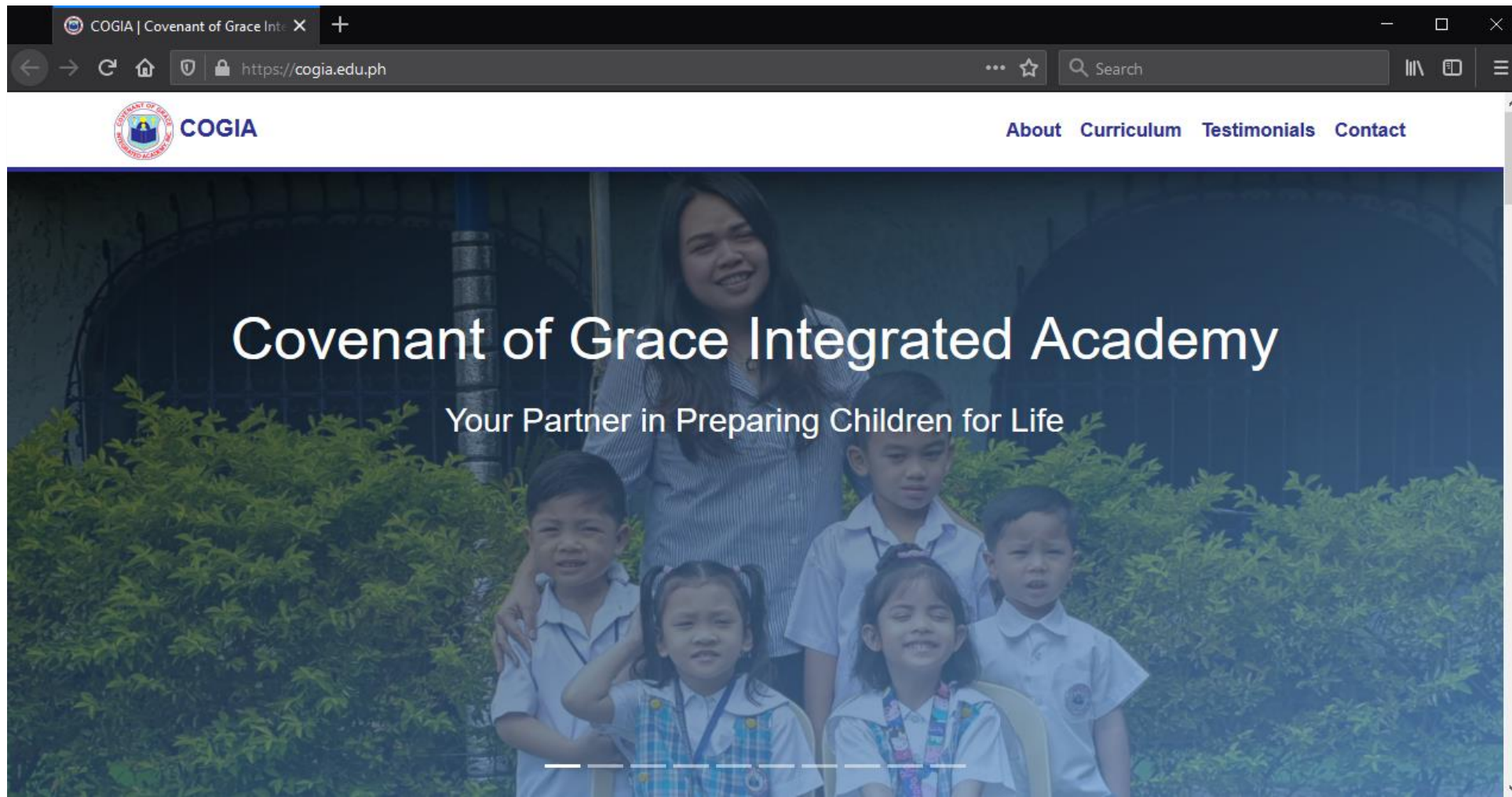


COVENANT OF GRACE INTEGRATED ACADEMY, INC.

Block 10 Lot 1 Aurora Pijuan St. corner Pilar Pilapil St., BF Resort Village, Talon 2, Las Piñas City
Telephone Nos.: 873-0629 / 501-6033 * E-mail: gracecovenant@globelines.com.ph

Your Partner in Preparing Children for Life

OLD WEBSITE OF COGIA



OLD WEBSITE OF COGIA

COGIA | Covenant of Grace Int. X +

https://cogia.edu.ph

Home About Curriculum and Program Contact Us

 **COGIA**

Covenant of Grace Integrated Academy

Your Partner in Preparing Children for Life

Preschool and Elementary School in BF Resort Village, Las Pinas City

Our children are growing in a complex, competitive world. As such, they should be properly guided and equipped in facing the challenges ahead of them. Helping children achieve confidence is indeed an overwhelming task. However, with the help of competent teachers, coupled with guidance from God, it can be achieved.

It is with this realization that Covenant of Grace Integrated Academy came into existence.

Covenant of Grace Integrated Academy was established to provide a balanced program that promotes intellectual, physical, social, emotional and spiritual developments. You now have hope for your children as they work together with us in developing their God-given potentials.

The school aims to provide your child with:

1. A healthy fear of the Lord resulting in faith in God and values transformation as well as growth in knowledge and wisdom.
2. A biblical concept of him/herself through Bible lessons to provide for a proper Christian outlook in life.
3. Awareness and development of traditional Filipino values that makes him/her unique in our now globalized community.
4. Love and concern for his/her family, friends, school, community and society.
5. Proficiency in academic skills especially in reading, grammar, math and the sciences.
6. Activities that promote physical, emotional and mental health.
7. Awareness of the importance of order and self-discipline.



BACKGROUND



RECOGNIZED

P-066 s.2012 / E-070 s.2012

About Covenant of Grace Integrated Academy

- A church-ministry founded by my Father and Mother
- Non-stock, Non-profit Corporation
- Small school started in 2005
 - 38 students for SY 2021 – 2022 (6 students with full scholarship, 4 students with partial scholarship)
 - 28 students for SY 2020 – 2021 (Due to pandemic)
 - 59 students for SY 2019 – 2020 (Regular number of students has been < 60 since inception in 2005)
 - Started with 5 students in SY 2005 – 2006
- Traditional school, minimal usage of technology
 - **Hands-on face-to-face interaction between teachers & students required**
- **Was not involved in the ministry until relatively recently**
 - **Not employed or officially part of the school**



BACKGROUND

About Covenant of Grace Integrated Academy

- A church-ministry founded by my Father and Mother
- Non-stock, Non-profit Corporation – **Not a charitable institution, but we do charitable work**
- Small school started in 2005
 - 38 students for SY 2021 – 2022 (6 students with full scholarship, 4 students with partial scholarship)
 - 28 students for SY 2020 – 2021 (Due to pandemic)
 - 59 students for SY 2019 – 2020 (Regular number of students has been < 60 since inception in 2005)
 - Started with 5 students in SY 2005 – 2006
- Traditional school, minimal usage of technology
 - **Hands-on face-to-face interaction between teachers & students required**
- **Was not involved in the ministry until relatively recently**
 - **Not employed or officially part of the school**

ASSUMED RESPONSIBILITIES & OBJECTIVES

- Enable Students and Faculty to engage in remote learning
- Ensure that Students, Faculty and Parents are well-informed of the requirements for remote learning
- Ensure that everything is running smoothly
- Ensure **DUE DILIGENCE** is performed for **IT**
 - **INFORMATION SECURITY** is a **BIG PART** of **DUE DILIGENCE** for **IT**
- Protect **IMPORTANT DATA** of Students, Faculty and Parents
- Create well-defined easy to understand/follow policies & procedures
- Ensure that IT-related issues are immediately resolved



ASSUMED RESPONSIBILITIES & OBJECTIVES

- Enable Students and Faculty to engage in remote learning
- Ensure that Students, Faculty and Parents are well-informed of the requirements for remote learning – **AVOID PROBLEMS IN REMOTE EDUCATION**
- Ensure that everything is running smoothly – **MAKE THINGS WORK AS INTENDED**
- Ensure **DUE DILIGENCE** is performed for **IT** – **MAKE THINGS OPERATE SECURELY**
 - **INFORMATION SECURITY** is a **BIG PART** of **DUE DILIGENCE** for **IT**
- Protect **IMPORTANT DATA** of Students, Faculty and Parents
- Create well-defined easy to understand/follow policies & procedures
- Ensure that IT-related issues are immediately resolved – **FIX PROBLEMS IMMEDIATELY**



ASSUMED RESPONSIBILITIES & OBJECTIVES

PARENTS BEWARE: Zoombombers insert obscene materials into grade school online class

Published September 18, 2020, 6:40 AM
by [Jane Kingsu-Cheng](#)

With almost everything done virtually, including classes and playdates, parents (and any guardian) should not let their guard down when it comes to children going online. Parents should remember that being at home doesn't mean your kids are safe from harm. The vast and unlimited online world is a scarier place that parents should watch over with a vigilant eye.

How it happened

On Sept. 17, people have been forwarding a screenshot of a Zoom class of grade five students. Among those in the class is a photo of what seemed to be a group of males who hacked into the class. *Manila Bulletin Lifestyle* got in touch with a parent from the said school whose child was in that class. The parent recounted that it happened around 10 a.m. and "someone was let into the Zoom meeting." The person drew a malicious photo and shared it on screen, opened the camera and showed his private body part.

This is referred to as Zoom bombing. According to How Stuff Works, this is "when strangers intrude on others' meetings on Zoom. Sometimes, these folks might just listen in without anyone knowing they're there. Other times, they totally disrupt the meetings in silly or even threatening ways."

ing

ed of the requirements for

ON

WORK AS INTENDED

OPERATE SECURELY

S

procedures

PROBLEMS IMMEDIATELY



ASSUMED RESPONSIBILITIES & OBJECTIVES

PARENTS BEWARE: Zoombo obscene materials into grad class

Published September 18, 2020, 6:40 AM
by [Jane Kingsu-Cheng](#)

With almost everything done virtually, including classes and playdate guard down when it comes to children going online. Parents should i kids are safe from harm. The vast and unlimited online world is a scarier place that parents should watch over with a

How it happened

On Sept. 17, people have been forwarding a screenshot of a Zoom cl class is a photo of what seemed to be a group of males who hacked touch with a parent from the said school whose child was in that cla 10 a.m. and “someone was let into the Zoom meeting.” The person d opened the camera and showed his private body part.

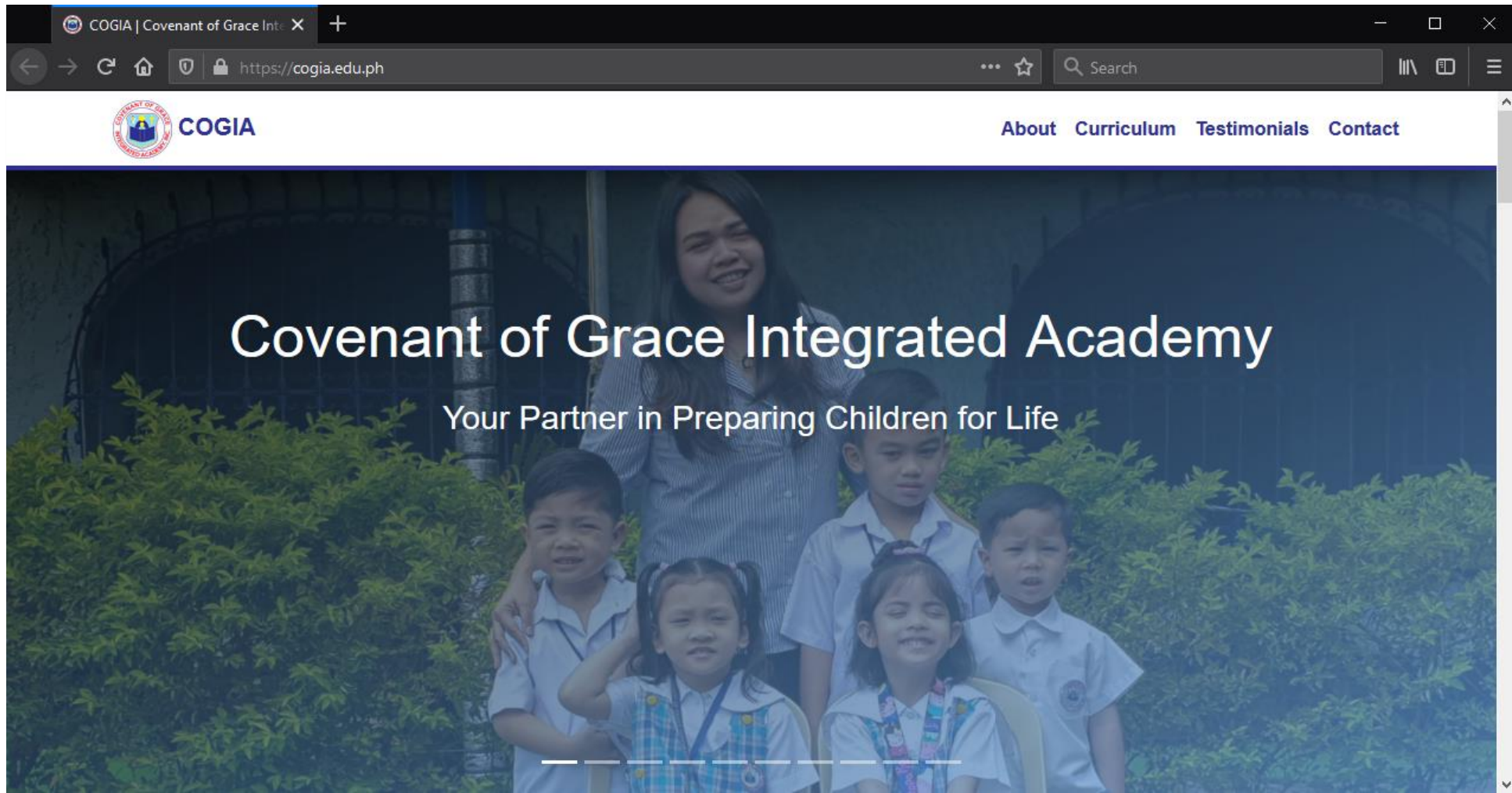
This is referred to as Zoom bombing. According to How Stuff Works, meetings on Zoom. Sometimes, these folks might just listen in with they totally disrupt the meetings in silly or even threatening ways.”

Under investigation

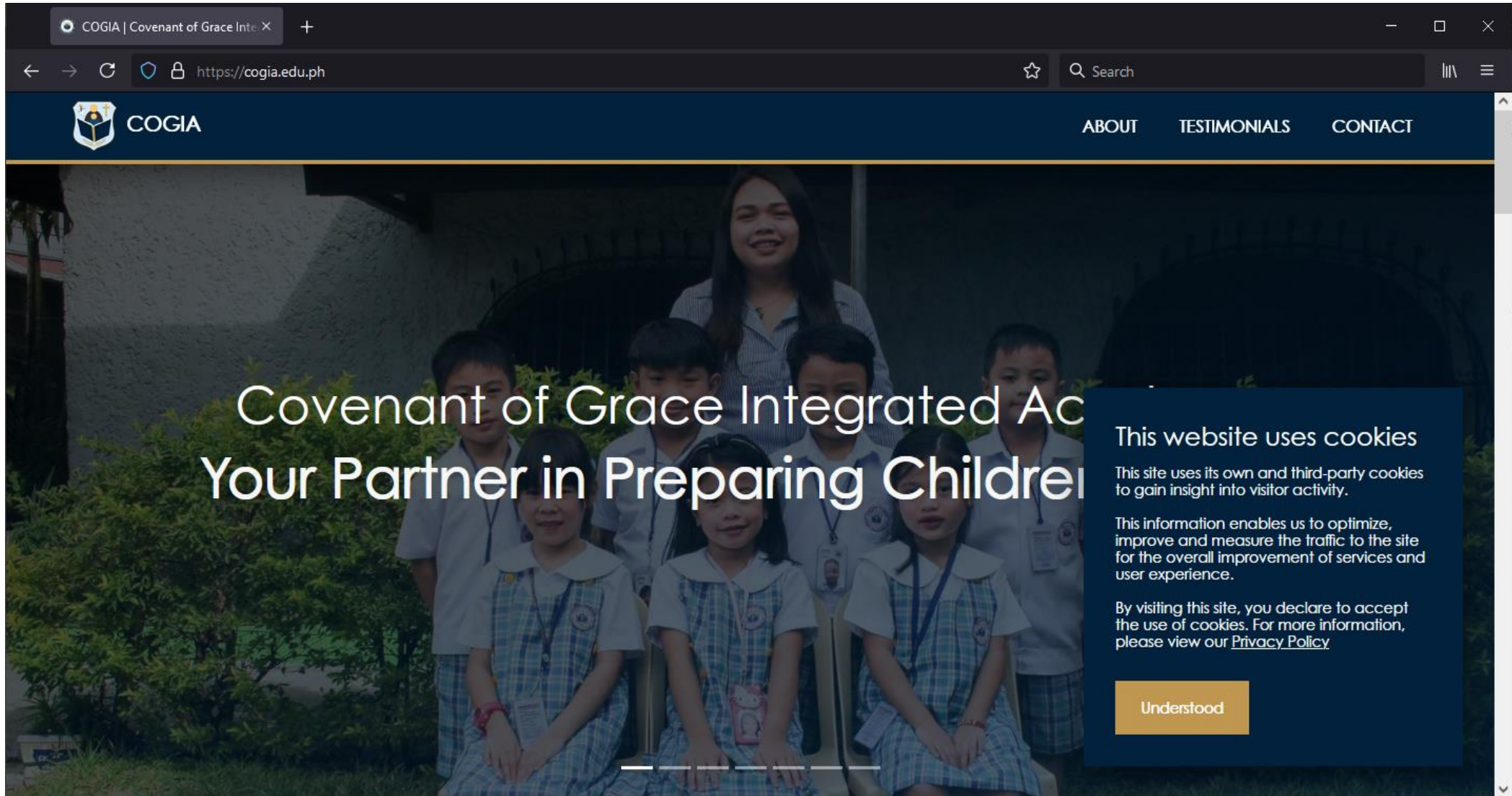
As to how that group got in, our source who wishes to remain anonymous revealed that “the teacher thought it was the IT (Information Technology department) checking on the classes or a student who got disconnected.” The teacher noticed it right away and was able to kick that person out.




APPLYING DUE DILIGENCE: WEBSITE DEVELOPMENT & OPERATIONS



APPLYING DUE DILIGENCE: WEBSITE DEVELOPMENT & OPERATIONS




APPLYING DUE DILIGENCE: WEBSITE MAINTENANCE & SECURITY

Security Headers Home About Donate
Sponsored by  **Report URI**

Scan your site now


Hide results Follow redirects

Security Report Summary

	Site:	https://cogia.edu.ph/
	IP Address:	2606:4700:3034::681b:8b4c
	Report Time:	30 Aug 2020 04:37:29 UTC
	Headers:	<input checked="" type="checkbox"/> X-Content-Type-Options <input checked="" type="checkbox"/> Content-Security-Policy <input checked="" type="checkbox"/> Strict-Transport-Security <input checked="" type="checkbox"/> Referrer-Policy <input checked="" type="checkbox"/> Feature-Policy <input checked="" type="checkbox"/> X-Frame-Options



APPLYING DUE DILIGENCE: WEBSITE MAINTENANCE & SECURITY


Security Headers
Sponsored by  Probely

Home About Donate

Scan your site now

Hide results Follow redirects

Security Report Summary

	Site:	https://cogia.edu.ph/
	IP Address:	2606:4700:3033::ac43:8ea9
	Report Time:	11 Jul 2021 15:50:44 UTC
	Headers:	<input checked="" type="checkbox"/> X-Content-Type-Options <input checked="" type="checkbox"/> Content-Security-Policy <input checked="" type="checkbox"/> Strict-Transport-Security <input checked="" type="checkbox"/> Referrer-Policy <input checked="" type="checkbox"/> Permissions-Policy <input checked="" type="checkbox"/> X-Frame-Options



APPLYING DUE DILIGENCE: WEBSITE MAINTENANCE & SECURITY

SSL Report: cogia.edu.ph

Assessed on: Sun, 30 Aug 2020 04:44:11 UTC | HIDDEN | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	Ready	Sun, 30 Aug 2020 04:40:23 UTC Duration: 36.131 sec	A
2	Ready	Sun, 30 Aug 2020 04:41:00 UTC Duration: 44.180 sec	A
3	Ready	Sun, 30 Aug 2020 04:41:44 UTC Duration: 44.223 sec	A
4	Ready	Sun, 30 Aug 2020 04:42:28 UTC Duration: 32.695 sec	A
5	Ready	Sun, 30 Aug 2020 04:43:01 UTC Duration: 34.236 sec	A
6	Ready	Sun, 30 Aug 2020 04:43:35 UTC Duration: 36.127 sec	A



APPLYING DUE DILIGENCE: WEBSITE MAINTENANCE & SECURITY



[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > cogia.edu.ph

SSL Report: cogia.edu.ph

Assessed on: Wed, 06 Oct 2021 14:19:23 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	2606:4700:3033:0:0:0:ac43:8ea9 Ready	Wed, 06 Oct 2021 14:16:17 UTC Duration: 45.263 sec	A+
2	2606:4700:3030:0:0:0:6815:3f1c Ready	Wed, 06 Oct 2021 14:17:03 UTC Duration: 45.729 sec	A+
3	104.21.63.28 Ready	Wed, 06 Oct 2021 14:17:48 UTC Duration: 49.526 sec	A+
4	172.67.142.169 Ready	Wed, 06 Oct 2021 14:18:38 UTC Duration: 45.341 sec	A+

SSL Report v2.1.8



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY

Enter domain
cogia.edu.ph

Check domain

Well done! Your domain is protected against abuse by phishers and spammers

Receivers are able to reliably separate and block fraudulent emails that mimic your email domain from your authentic emails. We can offer dedicated support to help manage DMARC-related incidents, regular data reviews, monitor ongoing compliance and help embed DMARC into your daily operations.

GET STARTED

 **DMARC**

Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

[Details](#)

 **SPF**

Your domain has a valid SPF record and the policy is sufficiently strict.

[Details](#)

 **DKIM**

Your DKIM record is valid.

[Details](#)



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY

Covenant of Grace Integrated Academy, Inc. ☀ Light mode

Active users

ⓘ Due to a recent increase in Teams usage, when you assign a Teams license to a user it may take around 24 hours before they'll be fully set up. Until then, you won't be able to assign Teams policies to them, and they might not have access to some Teams features like calling and audio conferencing. [Check status](#)

[Add a user](#) [User templates](#) [Add multiple users](#) [Multi-factor authentication](#) [Delete a user](#) [Refresh](#) [Reset password](#) [Export users](#) [Filter](#) [Choose columns](#)

Display name ↑	Username	Licenses	Title	Department	Choose columns
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for students			
⋮	@cogia.edu.ph	Office 365 A1 for faculty			



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY

Azure Active Directory admin center

Dashboard > Users

Users | Sign-ins

Covenant of Grace Integrated Academy, Inc. - Azure Active Directory

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date: **Last 7 days** Show dates as: **Local** Add filters

Date	Request ID	User	Application	Status	IP address	Location	Conditional access
8/30/2020, 1:14:44 PM	2762ab27-f677-4519-aa5f...		Azure Portal	Interrupted	180.191.99.61		Not Applied
8/30/2020, 11:17:38 AM	afef3b00-7452-48ee-859a...	Juan Dela Cruz	Outlook Mobile	Success	180.191.99.61	San Juan Del Monte, Nati...	Success
8/30/2020, 7:14:27 AM	c987f7a1-5057-40d6-b48...		Outlook Mobile	Success	180.191.99.61	San Juan Del Monte, Nati...	Success
8/30/2020, 7:12:02 AM	be579140-3b72-4aab-8d9...		Outlook Mobile	Failure	180.191.99.61	San Juan Del Monte, Nati...	Not Applied
8/29/2020, 10:07:09 PM	467b818f-9e69-4f2b-9d2...		Microsoft Teams Web Clie...	Success	112.206.42.202	Sampaloc, National Capit...	Success
8/29/2020, 10:07:09 PM	1b01a54b-6546-4c98-bd4...		Microsoft Teams Web Clie...	Success	112.206.42.202	Sampaloc, National Capit...	Success
8/29/2020, 9:56:41 PM	0037207f-8938-4c47-903a...		Microsoft Teams Web Clie...	Success	112.206.42.202	Sampaloc, National Capit...	Success
8/29/2020, 9:55:11 PM	1242407a-fd6e-45fa-8d28...		Microsoft Teams Web Clie...	Success	112.206.42.202	Sampaloc, National Capit...	Success
8/29/2020, 9:54:38 PM	aa11d0a7-130b-4ebd-a48...		Microsoft Teams Web Clie...	Success	112.206.42.202	Sampaloc, National Capit...	Success



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY

Azure Active Directory admin center

Dashboard > Users

Users | Sign-ins

Covenant of Grace Integrated Academy, Inc. - Azure Active Directory

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date: Last 7 days Show dates as: Local Add filters

Date	Request ID	User	Application	Status	IP address	Location	Conditional access
8/30/2020, 1:14:44 PM	2762ab27-f677-4519-aa5f...		Azure Portal	Interrupted	180.191.99.61		Not Applied
8/30/2020, 11:17:38 AM	afef3b00-7452-48ee-859a...	Juan Dela Cruz	Outlook Mobile	Success	180.191.99.61	San Juan Del Monte, Nati...	Success

Exchange admin center

Message trace > Message trace search results

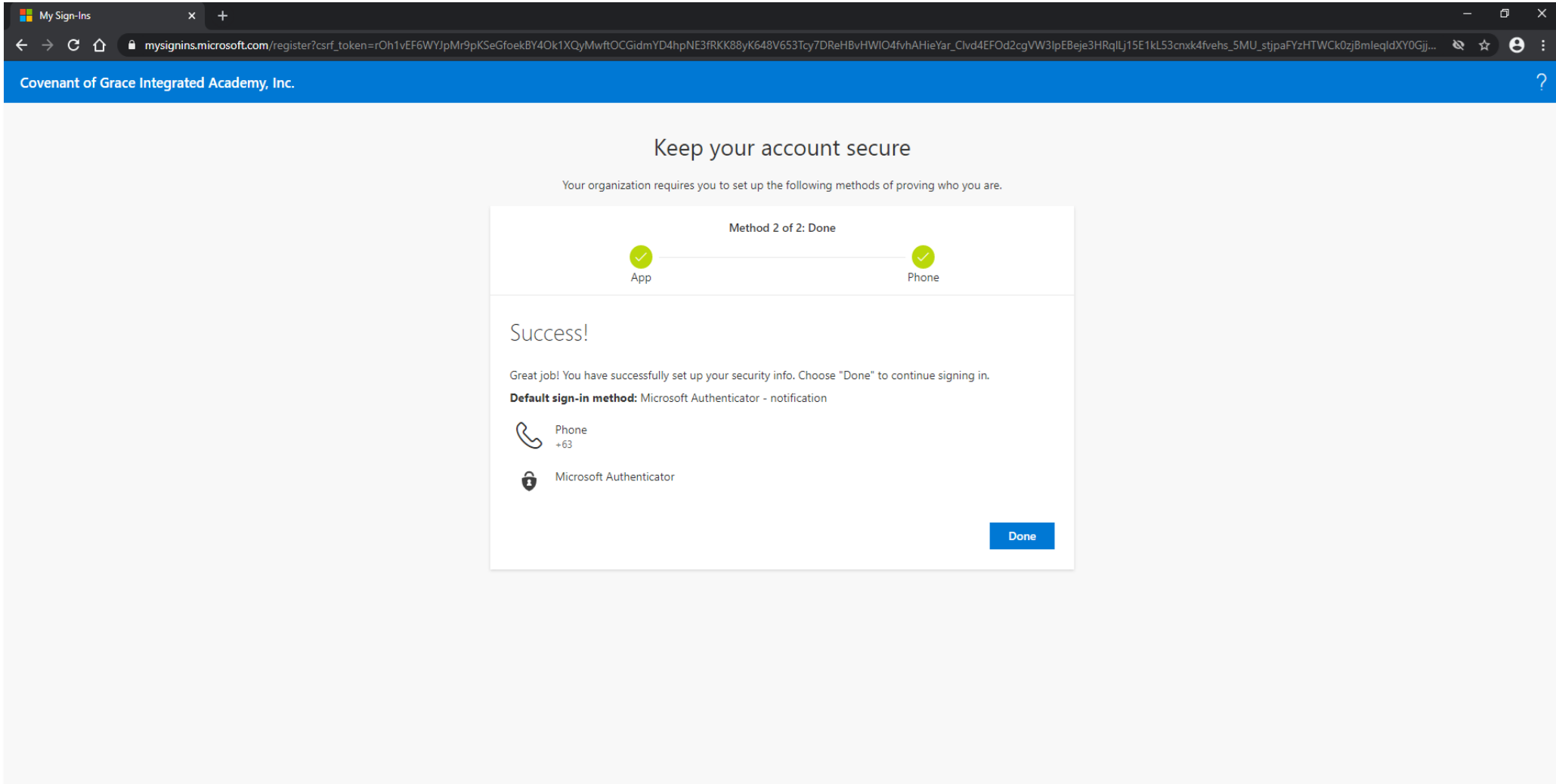
Export results Edit message trace Refresh

55 items Search

Date (UTC-08:00) ↓	Sender	Recipient	Subject	Status
7/11/2021, 9:01 AM	msonlineservicesteam@microsoftonline.com	@cogia.edu.ph	Your Covenant of Grace Integrated Academy, Inc. password ...	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for students subscription is renewing soon	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for students subscription is renewing soon	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for students subscription is renewing soon	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for faculty subscription is renewing soon	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for faculty subscription is renewing soon	Delivered
7/11/2021, 8:27 AM	microsoft-noreply@microsoft.com	@cogia.edu.ph	Your Office 365 A1 for faculty subscription is renewing soon	Delivered



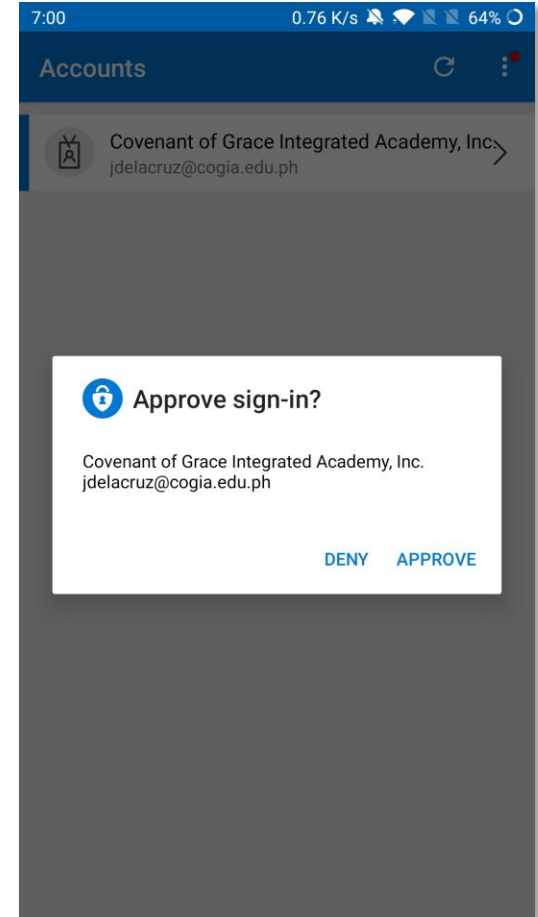
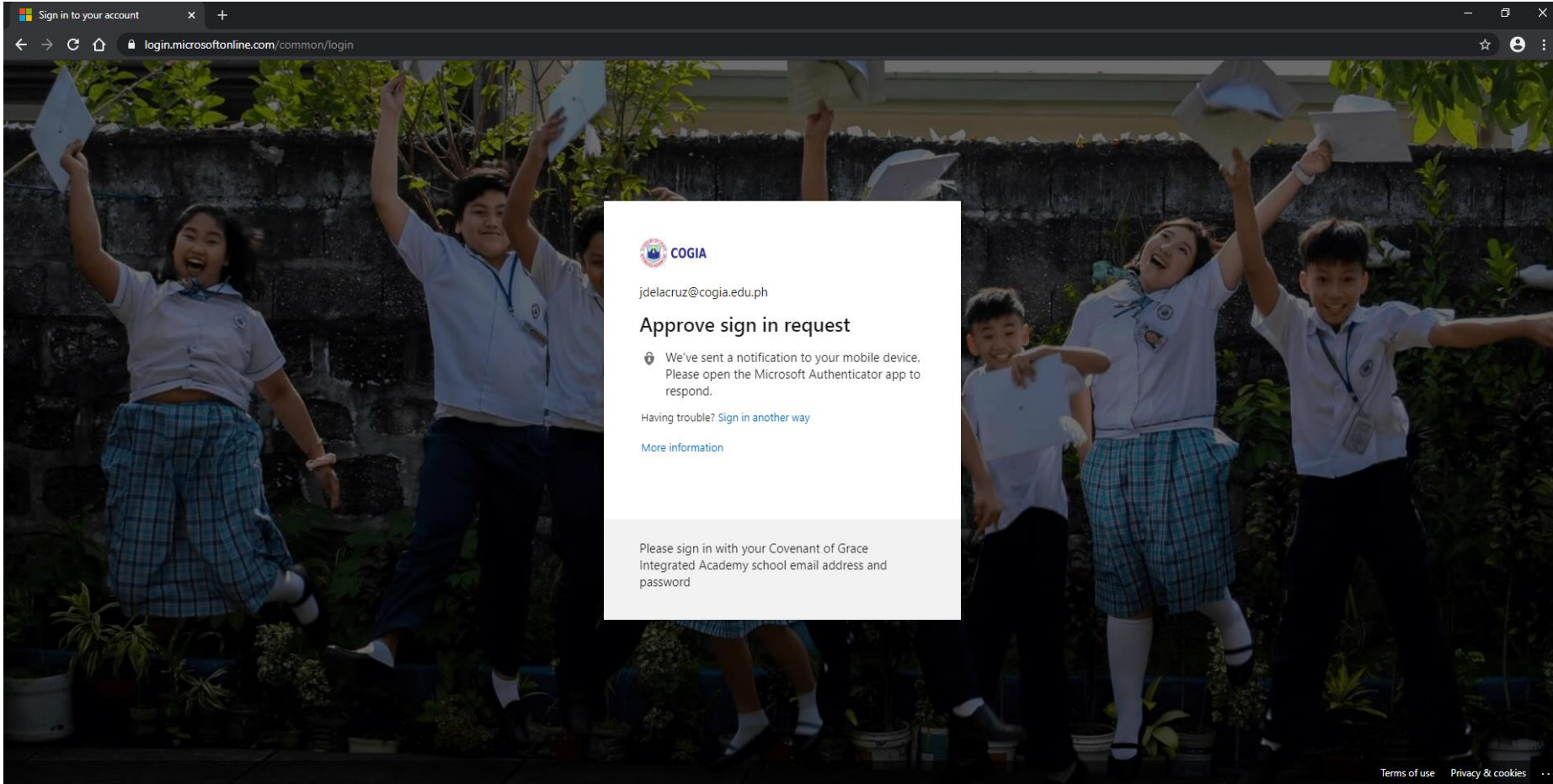
APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY



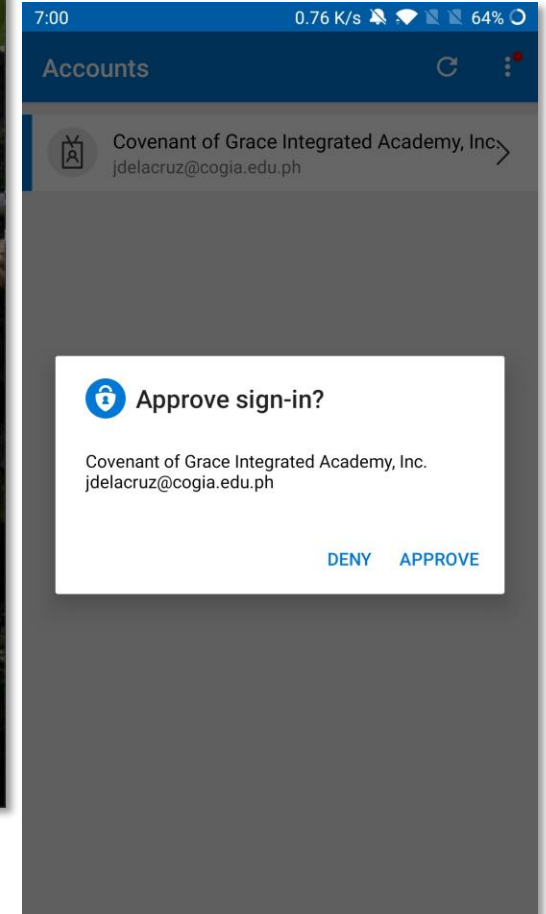
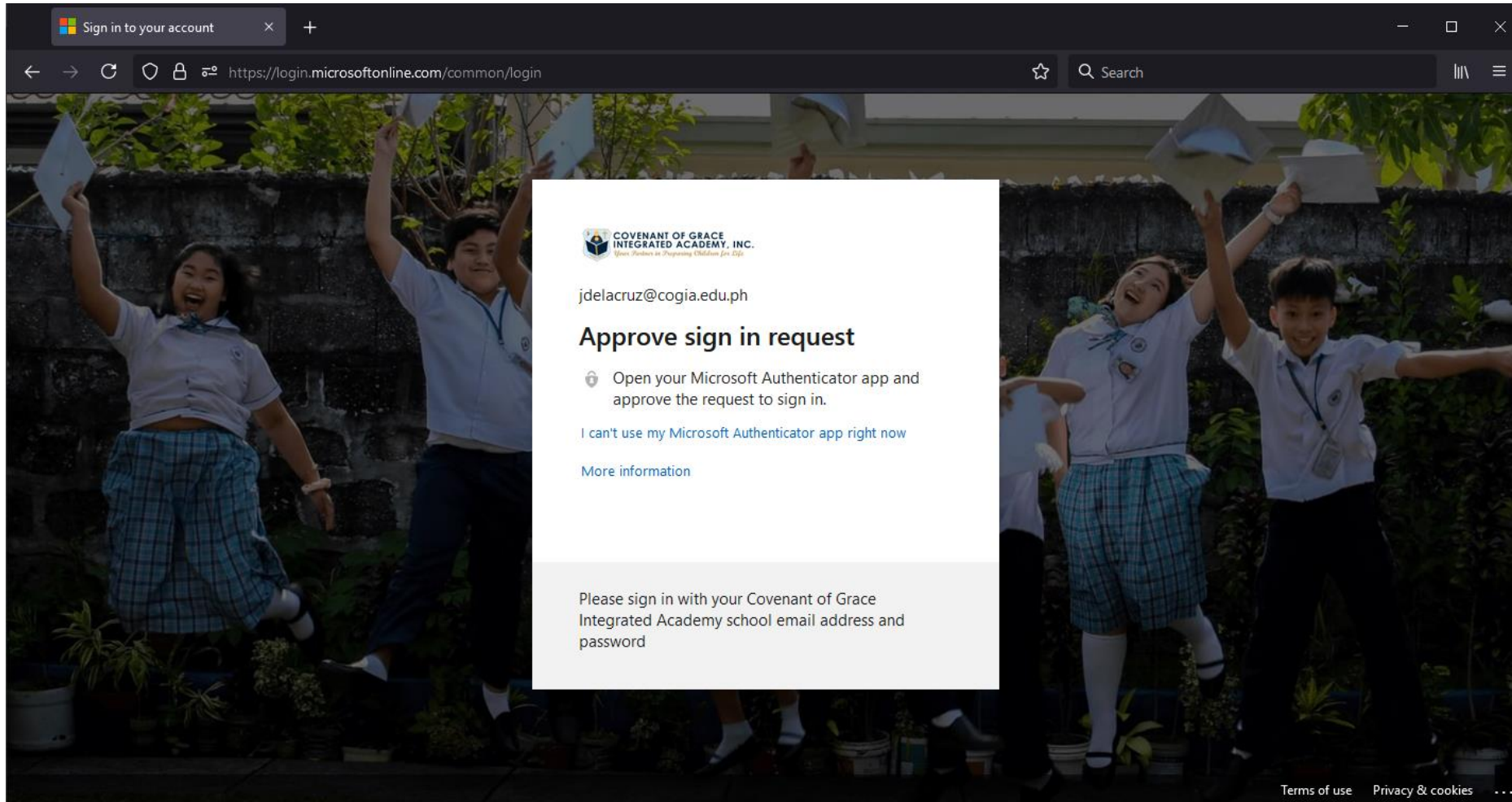
The screenshot shows a web browser window with the address bar displaying `mysignins.microsoft.com/register?csrf_token=rOh1vEF6WYJpMr9pKSeGfoekBY4Ok1XQyMwftOCGidmYD4hpNE3fRKK88yK648V653Tcy7DRvHBvHWIO4fvhAHieYar_Clv4EFOD2cgVW3lpEBeje3HRqLj15E1kL53cnxk4fvehs_5MU_stjpaFYzHTWCK0zjBmleqldXY0Gjj...`. The page title is "Covenant of Grace Integrated Academy, Inc.". The main heading is "Keep your account secure". Below this, a message states: "Your organization requires you to set up the following methods of proving who you are." A progress bar shows "Method 2 of 2: Done" with green checkmarks for "App" and "Phone". A "Success!" message follows: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Below this, the "Default sign-in method" is listed as "Microsoft Authenticator - notification". Two options are shown: "Phone +63" and "Microsoft Authenticator". A blue "Done" button is located at the bottom right of the success message box.



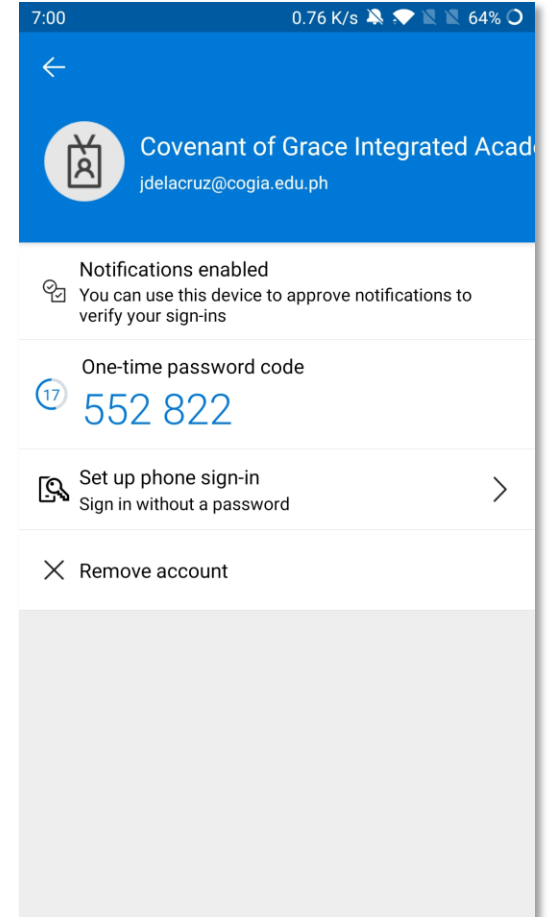
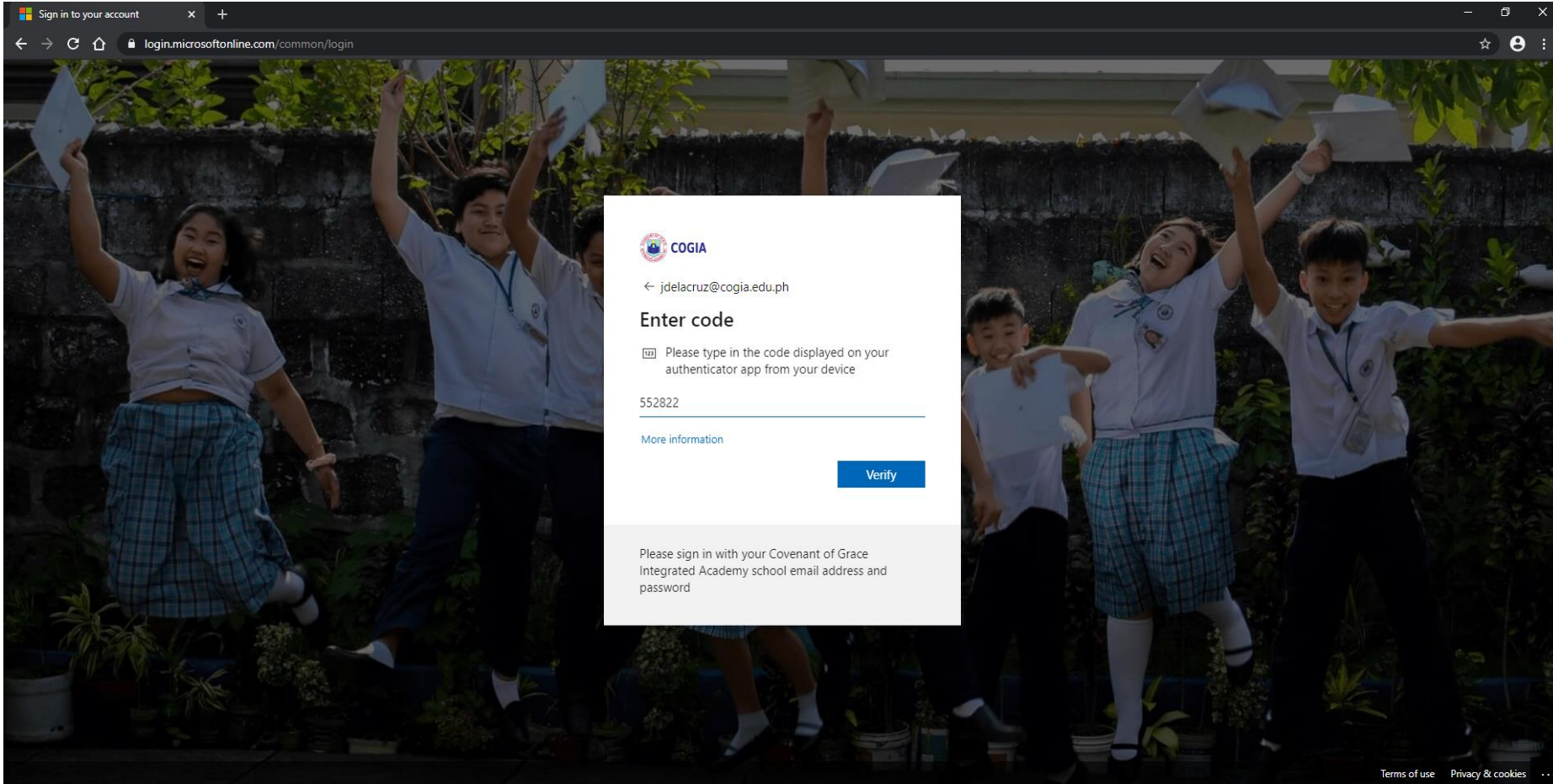
APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY

Sign in to your account

https://login.microsoftonline.com/common/login

COVENANT OF GRACE INTEGRATED ACADEMY, INC.
Your Pathway to Preparing Children for Life

← jdelacruz@cogia.edu.ph

Enter code

Please type in the code displayed on your authenticator app from your device

969508

Send an identity verification request to my Microsoft Authenticator app.

[More information](#)

Verify

Please sign in with your Covenant of Grace Integrated Academy school email address and password

Terms of use Privacy & cookies ...

7:00 0.76 K/s 64%

←

Covenant of Grace Integrated Acad
jdelacruz@cogia.edu.ph

Notifications enabled
You can use this device to approve notifications to verify your sign-ins

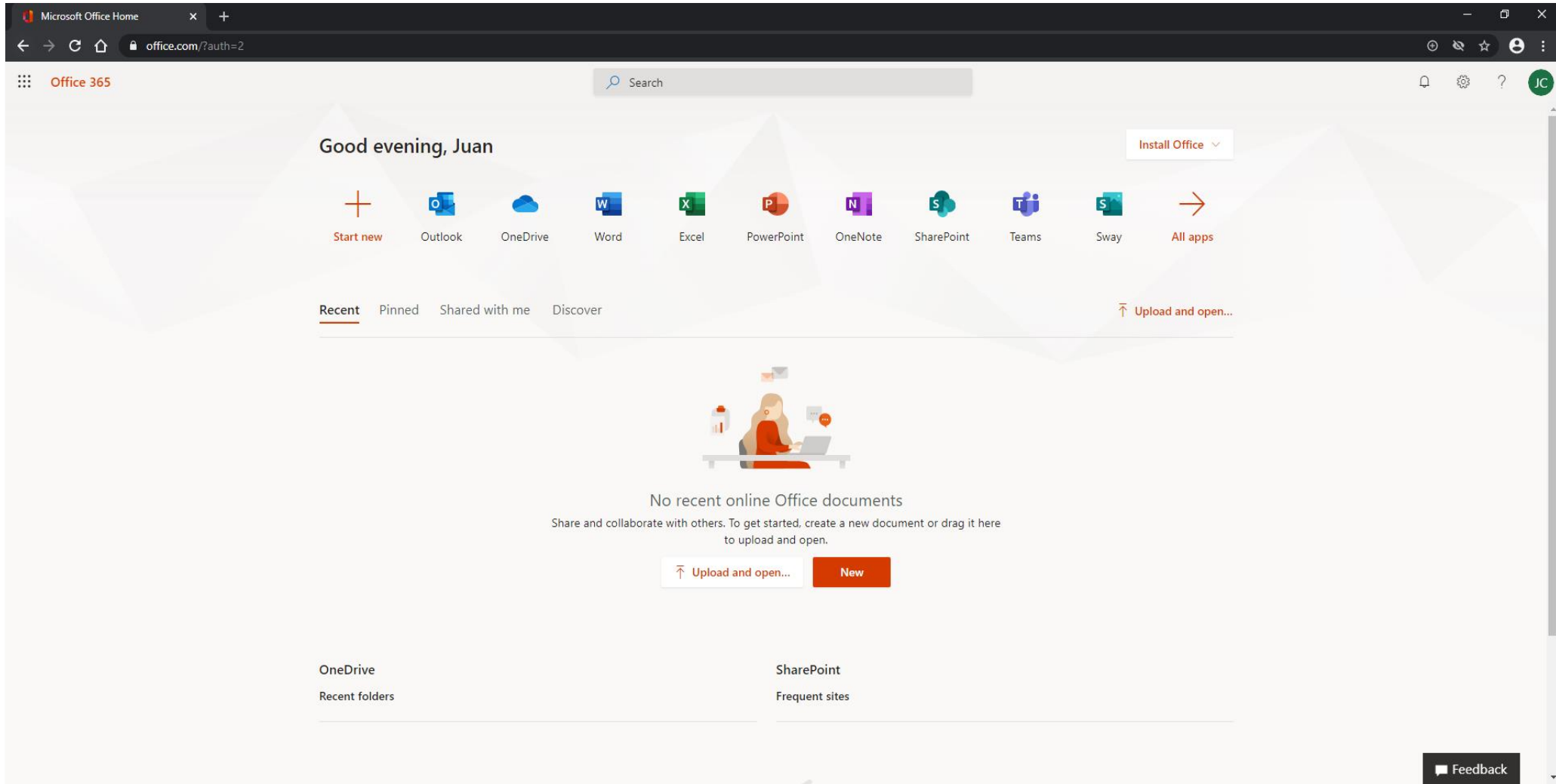
One-time password code
552 822

Set up phone sign-in
Sign in without a password

Remove account



APPLYING DUE DILIGENCE: USER ACCOUNT / EMAIL MAINTENANCE & SECURITY



APPLYING DUE DILIGENCE: OVERALL ORGANIZATIONAL SECURITY POSTURE

Microsoft Compliance Score (preview)

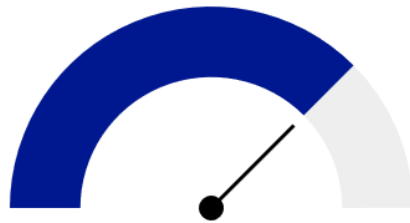
[Overview](#) [Improvement actions](#) [Solutions](#) [Assessments](#)

Microsoft Compliance Score measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

 Filter

Overall compliance score

Your compliance score: 75%



12159/16101 points achieved

Your points achieved ⓘ

66/₄₀₀₈

Microsoft-managed points achieved ⓘ

12093/₁₂₀₉₃

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how Compliance Score is calculated](#)

Key improvement actions

Not completed **276** Completed **4** Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Protect Authenticator Content	+27 points	• None	Default Group	Operational
Limit Consecutive Logon Failures	+27 points	• None	Default Group	Operational
Implement Account Lockout	+27 points	• None	Default Group	Operational
Protect Authenticators Commensurate with ...	+27 points	• None	Default Group	Operational
Refresh Authenticators	+27 points	• None	Default Group	Operational
Protect Wireless Access	+27 points	• None	Default Group	Operational
Protect Passwords with Encryption	+27 points	• None	Default Group	Operational
Manage Authenticator Lifetime and Reuse	+27 points	• None	Default Group	Operational
Restrict Access to Private Keys	+27 points	• None	Default Group	Operational

[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/70 points	12
Azure Active Directo...	9/416 points	25
Azure Information P	0/27 points	1

[View all solutions](#)



APPLYING DUE DILIGENCE: OVERALL ORGANIZATIONAL SECURITY POSTURE

Compliance Manager

[Compliance Manager settings](#)

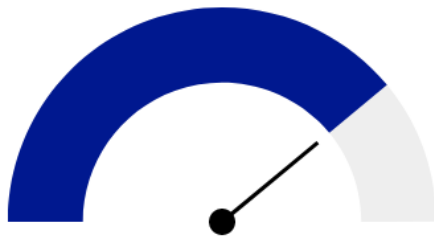
[Overview](#) [Improvement actions](#) [Solutions](#) [Assessments](#) [Assessment templates](#)

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

[Filter](#)

Overall compliance score

Your compliance score: 78%



12276/15645 points achieved

Your points achieved ⓘ

117/ 3486

Microsoft managed points achieved ⓘ

12159/ 12159

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Key improvement actions

Not completed **275** | Completed **5** | Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Protect Authenticator Content	+27 points	• None	Default Group	Operational
Limit Consecutive Logon Failures	+27 points	• None	Default Group	Operational
Implement account lockout	+27 points	• None	Default Group	Technical
Retain training records	+27 points	• None	Default Group	Technical
Use system clocks for audit records	+27 points	• None	Default Group	Operational
Use role-based privileged account manage...	+27 points	• None	Default Group	Technical
Revoke emergency/temporary access	+27 points	• None	Default Group	Technical
Protect data at rest with encryption keys	+27 points	• None	Default Group	Technical
Enforce authenticators strength	+27 points	• None	Default Group	Technical

[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/41 points	9
Azure Active Direct...	0/342 points	20
Azure Information P...	0/54 points	2
Cloud App Security	0/32 points	12
Communication co...	0/31 points	3
Compliance Manager	9/1228 points	149
Data loss prevention	0/82 points	4
Exchange	27/27 points	0
Exchange Online Pr...	54/301 points	11

[View all solutions](#)



INFORMATION TECHNOLOGY AND SECURITY FOR EDUCATION



INFORMATION TECHNOLOGY AND SECURITY FOR EDUCATION



INFORMATION TECHNOLOGY AND SECURITY FOR EDUCATION



TAKEAWAYS / LESSONS LEARNED

- Always **understand** the business & its processes to **make relevant changes**
- **Adoption of New Technologies** is **inevitable** – **do it NOW**
- We all use the **very same technology** from **different perspectives**
- **Information Technology** issues should **never** be a **HINDRANCE** to **PRODUCTIVITY**
- **Due diligence** will always start with **People**
- One aspect of **due diligence** in **IT** is by integrating **security** in the **design**
- Another aspect of **due diligence** is **KNOWING YOUR ASSETS**
- **Recognize your limitations & work within your means** – **but most importantly, START NOW**
- **Admit mistakes & act on it** – **It's ok to not know everything, you can ask questions & learn**
- Don't let your perceived limitations **LIMIT** you – let it be a **CHALLENGE**



TAKEAWAYS / LESSONS LEARNED

- It is better to do things **RIGHT** from the **START** – resolve problems not related to a **LACK OF SECURITY**
- Issues that arise from a **LACK OF SECURITY** are **HARD** to resolve – it can be done, it's not impossible, but it is **HARD** and definitely **TIME CONSUMING**
- **DON'T BE SHORT-SIGHTED:** Consider the **LONG-TERM EFFECTS** – always put **SECURITY & SAFETY** into consideration
- **EVERYONE** needs to **COOPERATE** to make things **WORK – PEOPLE, PROCESS & TECHNOLOGY (Most importantly: PEOPLE)**
- The current setup of our school will **NOT** be **SUCCESSFUL** without the cooperation of **PARENTS, STUDENTS** & most of all, the **TEACHERS (Who used to be parents of former & current students)**
- **Sometimes, we do not realize what is important to us until they are almost gone**



TAKEAWAYS / LESSONS LEARNED



SHAMELESS PLUG

Twitter:

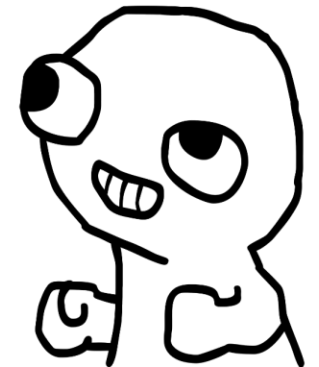
https://twitter.com/_hackstreetboys
<https://twitter.com/themanyhatsclub>

Facebook:

<https://www.facebook.com/hackstreetboys>
<https://www.facebook.com/groups/pitsf>

Website:

<https://hackstreetboys.ph/>
<https://ctf.themanyhats.club/>



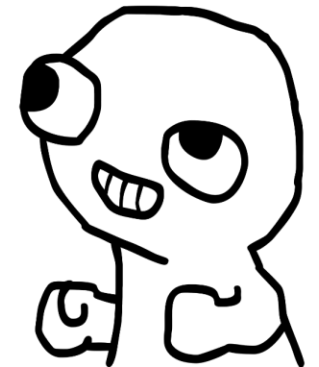
SHAMELESS PLUG

Facebook:

<https://www.facebook.com/COGIA2005/>

Website:

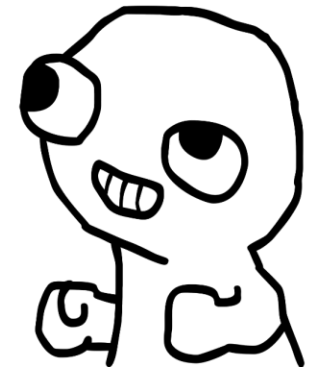
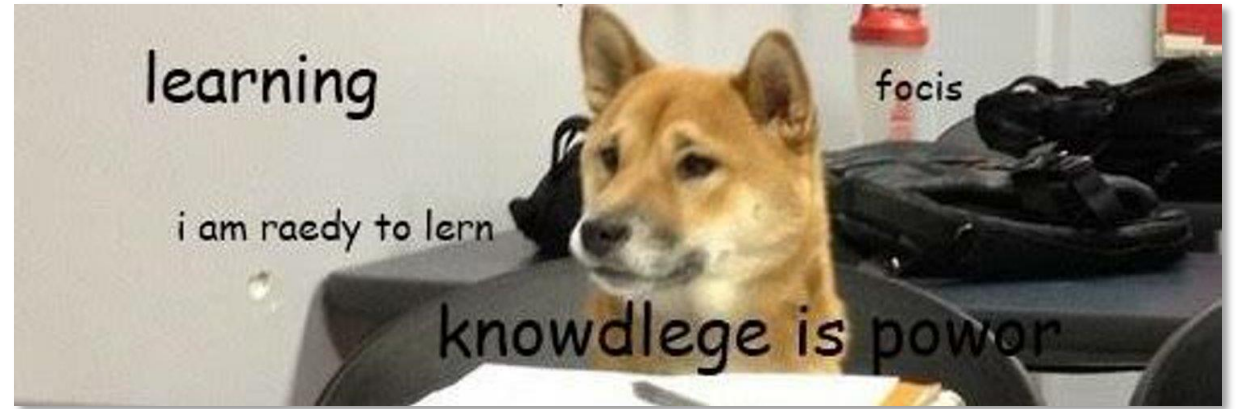
<https://cogia.edu.ph/>



SHAMELESS PLUG

Twitter:

<https://twitter.com/spieeler>
<https://twitter.com/ijpuzon>



Is TRUTH

Objective or Subjective

Absolute or Relative



Another thought provoking question

What standard do you follow
to say something is:

Right or Wrong

Good or Evil





**Thank you
and
God bless!**