

Decades Later: **Mobile Communication Attacks** **That Still Work Today**



Henry N. Caga (@hncaga)

whoami



Henry N. Caga

Lead Penetration Tester (2024)

CEH, ECSA, LPT (Master), eCPTXv2

**Independent Security Researcher /
Bug Bounty Hunter**

Acknowledged / Rewarded by:

Google

Twitter

Cloudflare

Unionbank

eBay / PayPal

Yahoo!

Globe / GCash

etc..

15 years in a Law Enforcement Agency

INTERPOL IT Crime Investigation working party (2007)

First appearance (2004)

About this talk



How Mobile Devices Communicate with Cell Towers

IMSI Catchers

Existing Mobile Attacks that Still Work

SMS Blasting

SMS Phishing / Smishing

Spoofing alphanumeric sender

Emergency Alerts

SMS Interception

Call Interception

Countering IMSI Catchers and Similar Devices

Disclaimer



The presentation on mobile hacking, mobile interception, and mobile attacks is solely intended for educational and informational purposes. The demonstrations and examples provided will be executed on controlled test devices with the explicit consent of the presenter. During the presentation, there is a possibility that certain techniques, such as sending SMS and intercepting calls and SMS, may be showcased.

It is important to acknowledge that due to the nature of the demonstrations, nearby devices within the conference environment might be affected inadvertently. Any potential impact on other devices is unintentional and limited to the context of the controlled demonstration.

Participants are advised to exercise caution and discretion when attending the presentation. The presenter and organizers do not take responsibility for any unintended consequences that may arise from the demonstration. Attendees should be aware that replicating the techniques shown on devices without proper authorization may breach legal and ethical standards and may lead to adverse consequences.



What happens when you turn on your phone?

(In Layman's Term)

Searching for Signal:

When you turn on your phone, it starts looking for signals from nearby cell towers. It's like your phone is trying to find the best radio station to tune into.

Checking the Connection:

Once your phone detects some signals, it sends out a signal of its own to see if there's a tower nearby that it can connect to. It's like your phone saying, "Hey, is there a strong Wi-Fi around here?"

Getting Tower Info:

If a tower responds, your phone gets information from it, like the tower's name and location. It's like your phone making friends with a new Wi-Fi router and learning its name.

Knowing Other Towers:

From the tower's signal, your phone also learns about other towers nearby. It's like your phone finding out about other Wi-Fi routers in the area.

Mobile attacks take advantage of this particular process!

IMSI Catcher / Fake Cell Towers (2G)



- **Signal Emission and Device Connection**
 - Similar to Real Cell Towers, so mobile devices can be attracted easily
- **Authentication**
 - All mobile phones can access the fake cell tower or BTS without requiring authentication! (e.g. Checking of IMSI, etc.)
- **Encryption (A5/0)**
 - Set the encryption to A5/0.
 - A5/0 is the weakest A5 encryption as it does not offer any encryption at all.
 - Lack of encryption means that it's possible to listen to calls and read SMS messages in plaintext.

Disable Additional Security features:

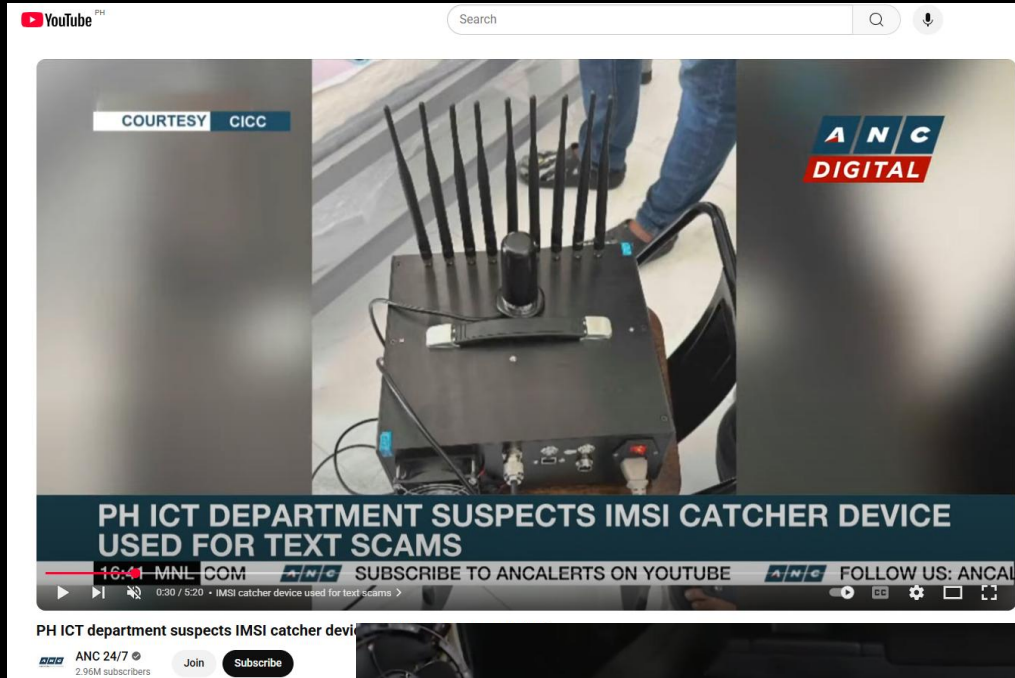
- Unregistered SIM cards remain usable
- Sending of links or URL is not filtered
- Unlimited calls and SMS sending with no subscription required

IMSI Catchers (“Known” Functions)



- **IMSI catchers can simulate legitimate cell towers to attract nearby mobile devices.**
- **They operate by intercepting the unique IMSI number linked to a SIM card.**
- **IMSI catchers can transmit SMS messages that impersonate legitimate senders, making fraudulent messages appear authentic.**

Recent Incidents in the Philippines



**Are those devices
actually used for
spying?**

No!

SMS Blasters are not spy tools, but they can still be dangerous.



- Devices are advertised for sending mass SMS messages (“bulk blast”) without needing a SIM card or a user database.**
- It was being sold in the Philippines via Social Media advertisements (Facebook, YouTube, etc.)**

How an IMSI Catcher Can Deliver a Fake SMS

A quick look at how a mobile phone can be temporarily connected to a fake BTS, receive a message, and go back to the legitimate network — all without the user's knowledge.



Fast and silent

the user may not notice the brief network change.

**But can IMSI catchers be
used to spy on people?**

Yes!

IMSI Catchers (Underlying Threat)



- **IMSI catchers can simulate legitimate cell towers to attract nearby mobile devices.**
- **They operate by intercepting the unique IMSI number linked to a SIM card.**
- **IMSI catchers can transmit SMS messages that impersonate legitimate senders.**
- **IMSI catchers holds the connection of the mobile phone for further attacks.**

IMSI Catcher Attack Flow

A mobile phone can be silently connected to a fake BTS, allowing an attacker to deliver messages, intercept data, and perform other attacks — all without the user's knowledge.



1

Connected to Legitimate Tower

The mobile phone is normally connected to a legitimate cell tower.



2

Attacker Runs IMSI Catcher

The attacker activates the IMSI Catcher / Fake BTS nearby.



3

Phone Connects to Fake BTS

The mobile phone connects to the IMSI Catcher / Fake BTS instead of the legitimate tower.



4

Connection is Held

The IMSI Catcher holds the connection of the mobile phone and does not kick it back to the legitimate tower.



5

Attacker Can Perform Various Attacks

While the phone is connected, the attacker can perform multiple attacks, including:



Send SMS / Blast SMS



SMS Phishing



Spoof alphanumeric sender



Emergency Alert



SMS Interception



Call Interception

6

Attacker Decides to Disconnect

It depends on the attacker to manually kick or disconnect the mobile phone back to the legitimate tower or not.



Happens without the user's knowledge.

From the mobile phone's perspective, it is still online and connected to the cellular network.
From the network or telco's perspective, the mobile phone is currently offline or appears to be turned off.



Can happen very fast.

The connection and attacks can be performed in a short period of time.

DEMO

Running a fake cell tower

Spoofing Mobile Number

Caller ID spoofing is when someone changes the number that appears on your phone to make it look like they're calling or texting from a different number

Spoofing Using Alphanumeric Sender

Manipulating the sender information to display an alphanumeric name or label instead of a phone number.

This technique is often used for branding or to make messages appear more legitimate.

DEMO

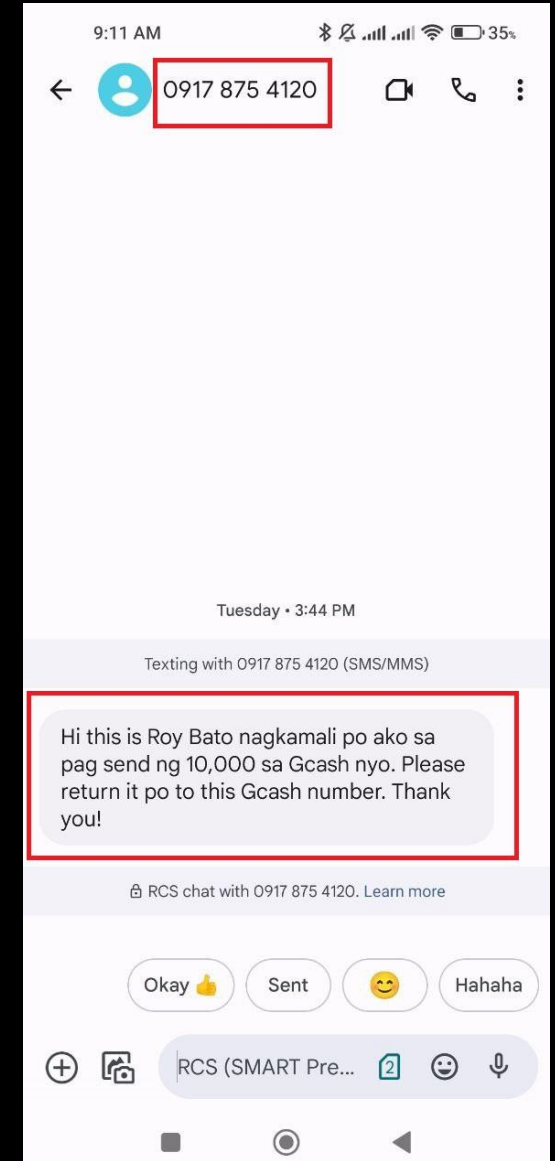
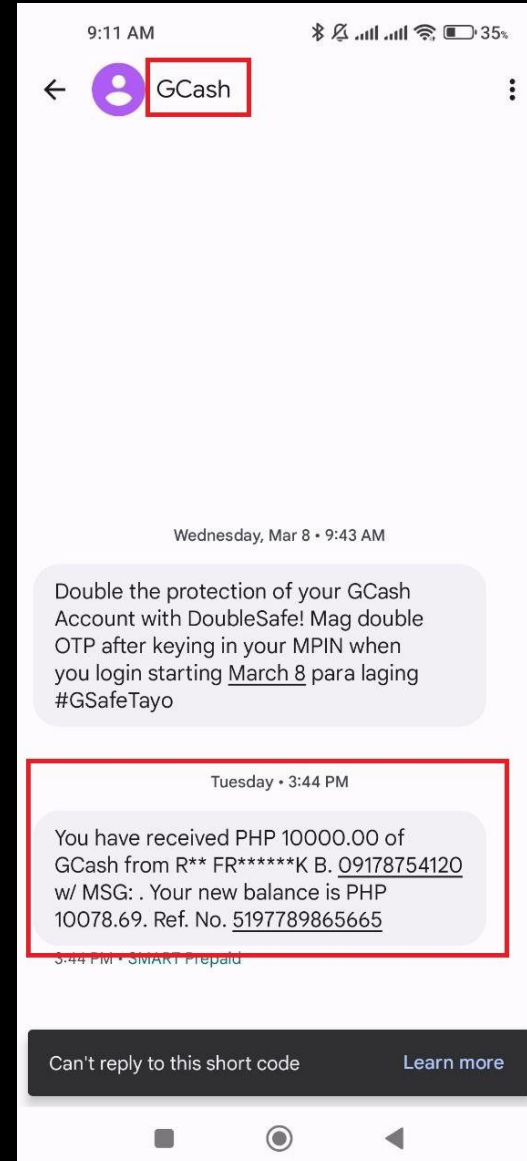
Mobile Number / Name Spoofing

Scammers Using Spoofing



Scammers use alphanumeric senders to make their messages seem official or trustworthy.

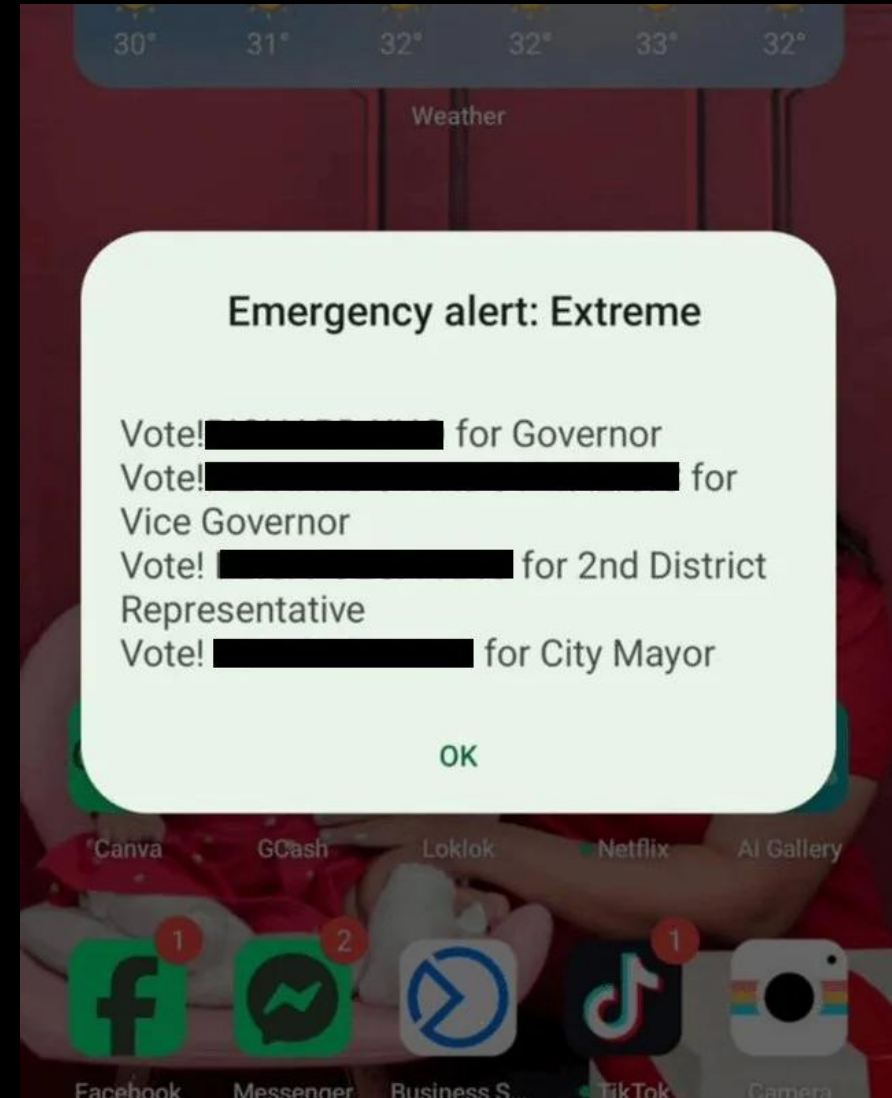
For example, they may send a text message with the sender labeled as “YourBank” or “GCASH” to create a sense of urgency and authority.



Cell Broadcast

Attackers send false messages (e.g., “evacuate now”) to cause panic or social engineering opportunities.

Used to send misleading news, propaganda, or fake political updates during elections or crises.





DEMO

SMS Interception / Calls Hi-Jacking

Other Mobile Attacks



Man in the Middle (MITM)

- Allow the victims to access to the internet
- Allow sending of links
- Sniff traffic
- Scan for open ports
- Scan for vulnerabilities to access files or data

Why 2G?



- **Weak Encryption**
- **Lack of Mutual Authentication**
- **No Integrity Protection**
- **Known Vulnerabilities**
- **Aging Technology**

Attacks are only available on 2G?

**I'm using 4G/LTE and 5G! Am I still
Vulnerable?**

Attacking 4G/LTE, 5G



Generating Noise

- Jamming frequencies other than 2G
- Mobile devices will use 2G when other options are unavailable
- Mobile devices are designed for Network Fallback (2G as a fallback to maintain communication)

Downgrade Attack

- IMSI Catcher for Higher Generations (Another equipment for 4G/LTE, 5G)
- Send deceptive signals to mobile devices, making them believe that higher-generation networks (3G, 4G/LTE, 5G) are not available in the area. This encourages the mobile devices to "fall back" to a lower-generation network, such as 2G, which may be less secure.
- Mobile devices are designed to follow network instructions and prioritize the best available network based on signal strength and other factors

How can we protect ourselves?



Do not click on suspicious or unverified links:

Avoid clicking on links or downloading files from sources that you do not trust or that seem suspicious.

Set your mobile network settings to use higher-generation networks and disable fallback to 2G (if your device allows it):

This is a good practice if you prioritize network security. However, not all devices or network providers allow users to disable network fallback, and in some cases, falling back to 2G might be necessary for connectivity in remote areas with limited coverage.

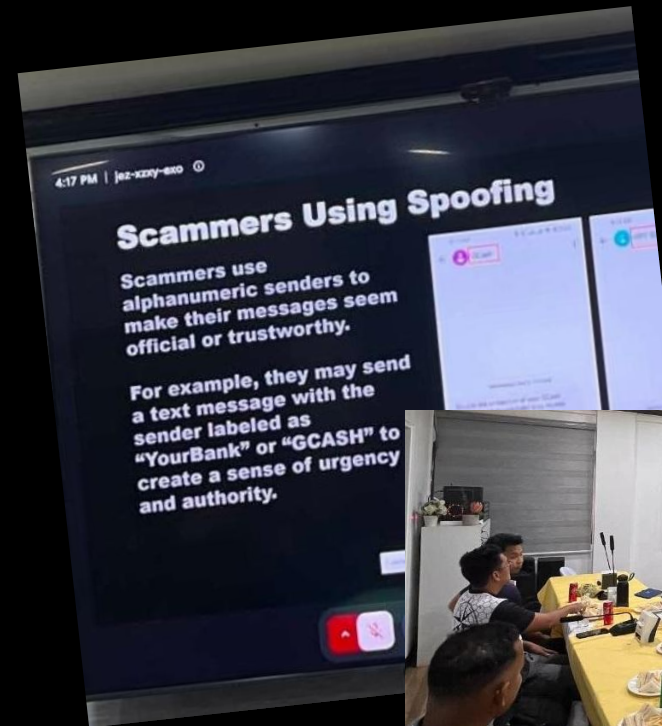
Network providers should implement measures to detect rogue cell towers:

Network providers should employ advanced technologies and monitoring systems to detect and mitigate the presence of rogue cell towers or IMSI catchers.

CAV – Progress and Efforts



Conducted multiple awareness presentations for banks, private organizations, and government agencies.



CAV – Progress and Efforts



Globe Telecom has taken a major step in protecting mobile subscribers from SMS phishing attacks by implementing a monitoring system that detects potentially harmful and suspicious SMS messages. This helps identify possible phishing attempts and other malicious messages.

Activate your Shields!

 **Globe** #AlagangGlobe

Introducing
SMS SCAM SHIELD
on the GlobeOne App



Get notified when you receive SUSPICIOUS LINKS
in texts on your **ANDROID DEVICE**

ACTIVATE NOW

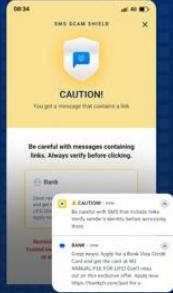
 **Globe** FOR ANDROID USERS ONLY

You can expect three types of notifications from Globe's
SMS SCAM SHIELD

Fake Sender Warning
For "Globe", "GCash",
or private mobile numbers



Link Risk Caution
For Bank & Financial Institution
Related Text Messages



Safety Reminder
For General Broadcast
Related Text Messages



NOTE: GlobeOne app does not read or store any of your messages.

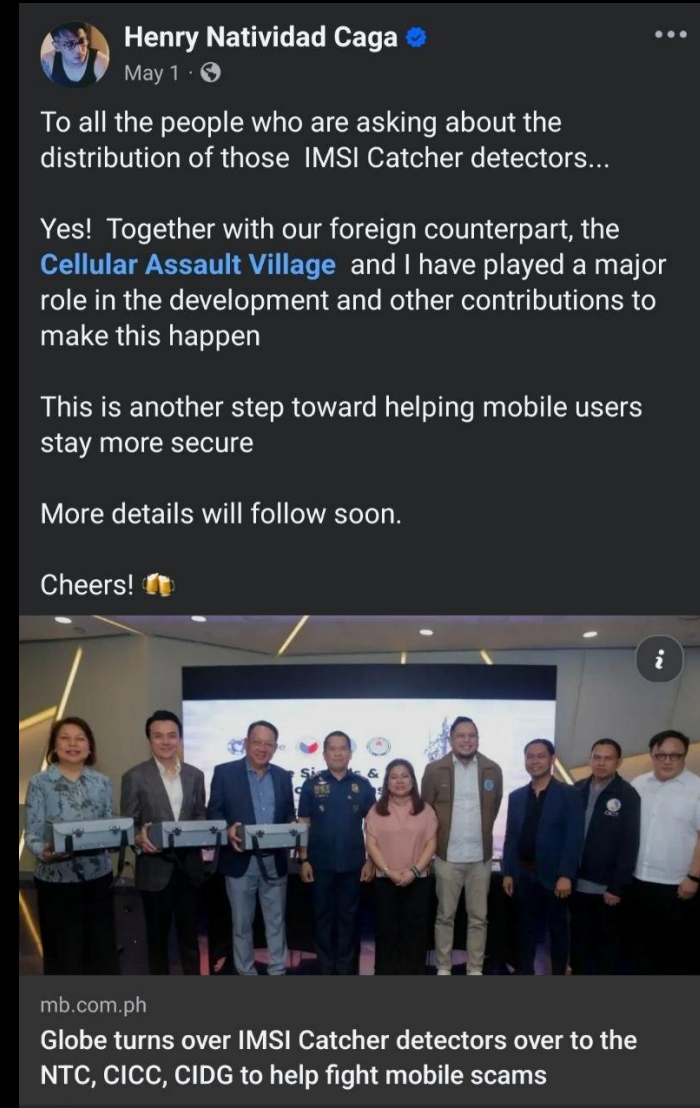
#AlagangGlobe

CAV – Progress and Efforts



Globe Telecom donated IMSI Catcher Detectors to CICC, NTC, and CIDG, with the Cellular Assault Village and our foreign counterparts playing a supporting role in the distribution and implementation.

This is a major step by Globe Telecom in helping law enforcement detect and investigate IMSI Catchers.



CAV – Progress and Efforts



Cellular Assault Village is currently developing our own IMSI Catcher Detectors.

The device can identify legitimate and fake cell towers, and estimate the possible location, distance, and signal strength of an IMSI Catcher or rogue base station.

That's All Folks!

Thank you!

