

Console (In)Security: The Oncoming Storm
Chris Boyd, Senior Threat Researcher

Way back when...



Way back when...



The Digital Divide


- » Current gen built for digital media and online gaming
- » Consoles released that require no physical media
- » The cost of digital downloads continues to rise
- » DRM limits value of purchase
- » Monetary investment in gaming accounts makes them a hot target

September 2008: Gaming Batman

The screenshot shows a Mozilla Firefox browser window displaying the Newsarama.com website. The browser's address bar shows the URL <http://newsarama.com/>. The website header features the Newsarama logo with a 'BETA' tag, a search bar, and navigation links for Home, Comics, Film, TV, Games, Blog, and Video. A banner at the top left reads 'AN IMPORTANT MESSAGE ABOUT THE NEW NEWSARAMA!'. The main content area includes a large image of a man and a woman, and three smaller news snippets: 'EXCLUSIVE Image Preview: Savage Dragon #137', 'CN Announces Clone Wars Premiere Date', and 'Save the House Where Superman was Born'. On the right side, there is a 'FREE ONLINE BATMAN GAME!' advertisement with a background image of Batman in a dark, industrial setting. The ad includes the URL www.BatmanGame.info and 'Ads by Goooooogle'.

September 2008: Gaming Batman

http://www.batmangame.info/ Google





ONLINE BATMAN GAME

- notice -

★ To download and play the Batman Online Game you must download and install Zango as well. It is free, very easy to install and will give you access to the full game. ★

Download The Online Batman Game Now!

FREE DOWNLOAD [CLICK HERE](#)

Batman Online lets you do anything and every little thing you'd like in a Batman game. From leveling up your character to destroying villains, it has it all. **Download and play this amazing game now**, all for free! I'm sure you'll be playing for hours on end, it's that much fun.

- ✓ Level Up Your Character
- ✓ Explore a Huge Vast World
- ✓ Play Online With Your Friends
- ✓ Hundreds of Quests To Finish
- ✓ Perfect Battle System

So start your Batman adventure today! Download the full game below and fight them all!

Download Now!

September 2008: Gaming Batman

http://batmangame.info.powered-by.zango.com/?a670a97af3/ga675aa76f6&s=http%3A//www.b

Get The Online Batman Game for FREE

DOWNLOAD BELOW!

Zango is a free, premium-content access tool, paid for by advertising. Once installed and while online, using keywords sent to Zango from your Internet browsing, Zango software (with Weather) shows ads in a Zango Toolbar; a temporary Slider, on (e.g.) the bottom corner of your screen; and a separate browser window that pops up on your screen. If you search for or view Adult websites, you may receive Adult-oriented ads. Depending on your browser version, Zango may become the default search provider. Additionally, Zango may redirect a search resulting in an error to a list of sites similar to your search terms. Zango's Internet Explorer, Outlook/Outlook Express and Word Toolbars give access to free emoticons (and more) within those applications, when online. Zango runs continuously and upgrades automatically. Uninstallation is easy via Add/Remove Programs.

For more information: [Best Practices](#), [Privacy Policy](#), [FAQ](#)

Zango, Inc.
End User License Agreement
(June 3, 2008)

[View EULA](#) | [Print EULA](#)

By clicking "Start," I represent that I (1) am at least 18, (2) agree to the EULA and Privacy Policy terms and (3) consent to install Zango and access BatmanGame.info.

Cancel Click "Start" to install Zango and access this website for free. Start

zango

September 2008: Gaming Batman

THIS IS A DEMONSTRATION VERSION OF
BATMAN. IT WAS CREATED TO ENABLE YOU TO
VIEW THE GAME BEFORE RELEASE. AS IT WAS
CREATED DURING THE DEVELOPMENT OF BATMAN
IT IS POSSIBLE THAT SOME OF THE FEATURES OF
THE GAME WILL NOT BE PRESENT IN THIS
DEMONSTRATION VERSION. HAVE FUN !

Welcome to the Lab



Methods of Attack

- » Gamers in gaming sessions (can include system tampering)
- » Social engineering / rogue programs online
- » Attacking the console maker (databases, live support)

Under the Hood

Solutions

Top solutions to get the most out of your Xbox experience

Xbox 360



Xbox LIVE



Xbox LIVE Status

Status not available at this time

1 of 5

 Select  Back



Connectivity

Xbox LIVE and networking



ts
avatars, and billing



downloads, and licenses



nds, and parties



Online Safety

Custom

Not Allowed

Video Communication
Video and Music Status
Friends List
Voice Data Collection
Xbox Marketing
Partner Marketing

Change Settings

Risk / Reward – but mostly risk

- » Incentives make you a target
- » When cc details decrease in value, gaming PII can put the price back up
- » Gaming accounts an established commodity on the black market

Tools of the Trade

Tools of the Trade

Thread Tools ▼ Display Modes ▼

06-17-2009, 01:16 PM #1 (permalink)

Senior Member
Respected Member II

come to the dark side (we have cookies)

Tournaments Won: 1

Join Date: Apr 2009

Location: [REDACTED]

Posts: 146

Thanks: 6
Thanked 4 Times in 4 Posts

Awards Showcase

Total Awards: 3

OFF

How to get a free transfer cable for modding

Ok, this works for everybody just as long as you have 1 Xbox 360 Serial Number

Step 1: Call the following number
US: 1-800-4MY-XBOX (1-800-469-9269)
UK: 0-800-587-1102

Step 2: Say: Accessories, Xbox 360, None of Those.


Step 3: Give him your REAL information!

Step 4: When a person gets on the line say you got a 120Gb Hard Drive as a gift and you need an "Xbox 360™ Hard Drive Transfer Cable".

Step 5: Give them all the information they require.

Step 6: They will ship you your Cable within 1-2 weeks for free shipping and all.

The cable will look like this:



To read more about the "Transfer Cable" go here: <http://www.xbox.com/en-US/support/sy...amigration.htm>

THIS WILL **UNLOCK ALL** OF THE ACHIEVEMENTS ON
YOUR XBOX 360. (1000) + THE GAME ADD-ONS

WHY PAY SOMEONE ELSE TO DO IT WHEN YOU CAN DO IT YOUR
SELF AND WHEN YOU HAVE THESE PROGRAMS YOU CAN SELL
400000+GAMERTAGS ON EBAY AND MAKE **££££££££££**.

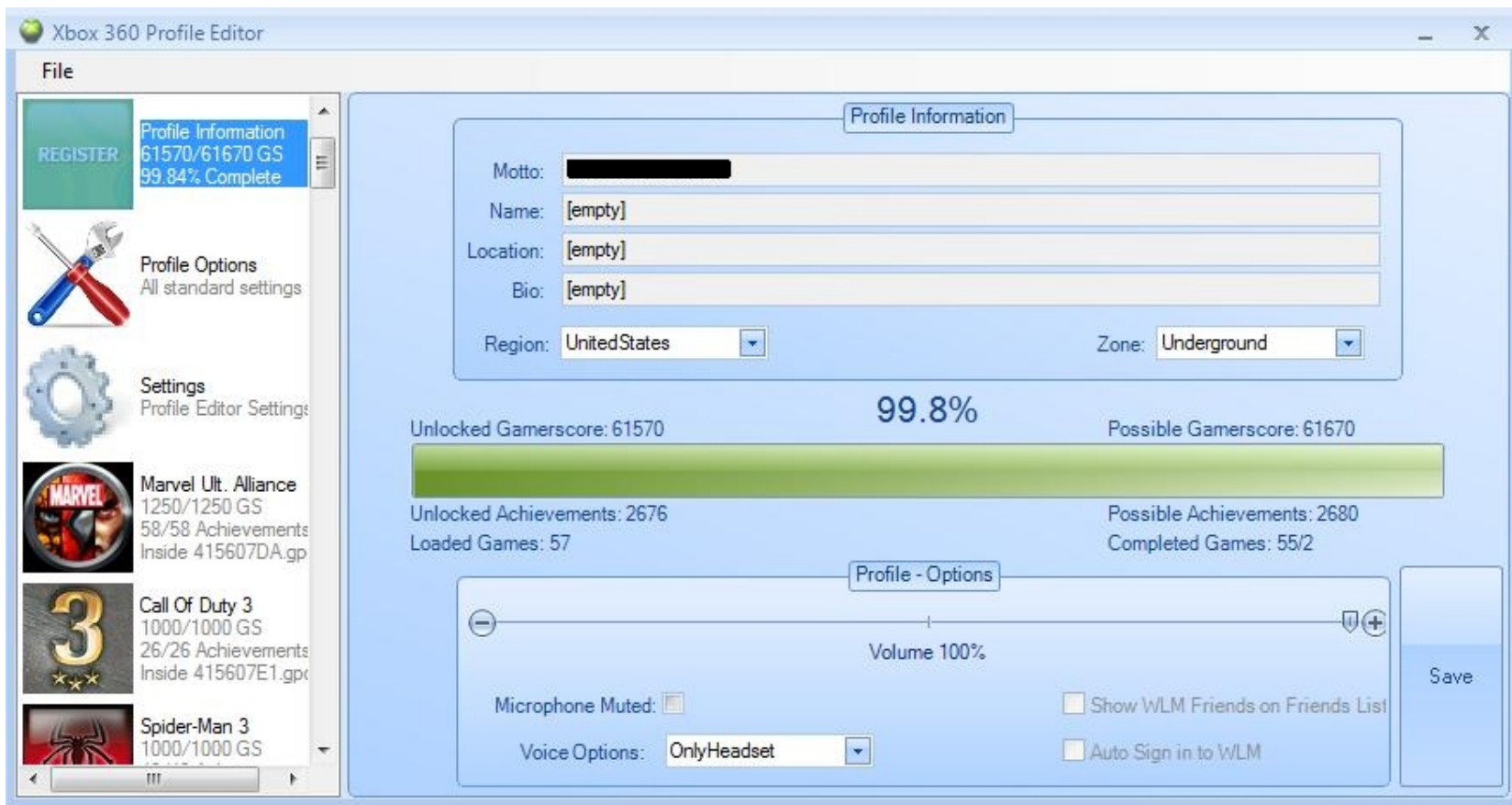


WHY 4 PROGRAMS? - YOU ARE GETTING 4 PROGRAMS BECAUSE THE
DEFUALT ONES NEVER WORK!!!!!!

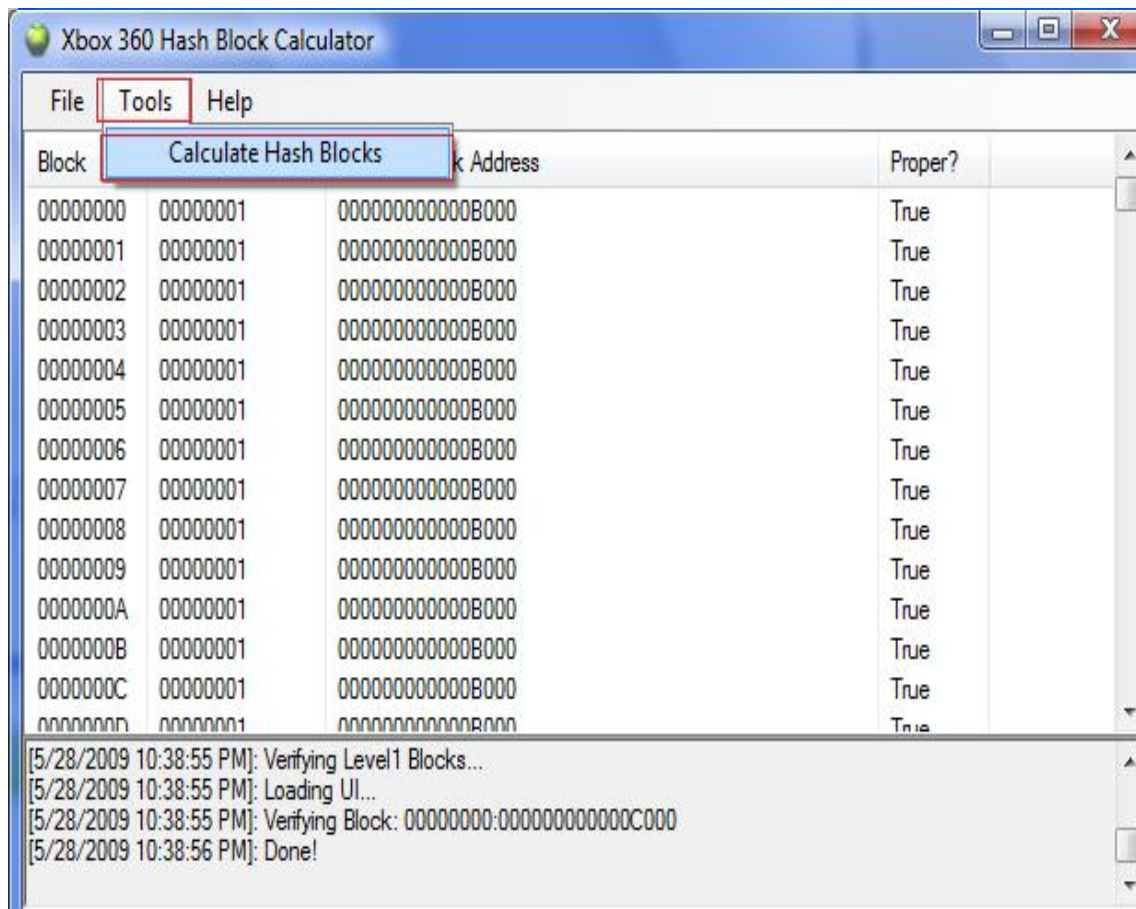


You will need a transfer kit, it is very easy to do, everything you need to know is on the internet, HAPPY BIDDING!!!!!! ANY QUESTIONS
ASK!!!!
ANYONE COPPYING THIS WILL BE REPORTED TO EBAY!!!!

Tools of the Trade



Tools of the Trade





Gamerscore / Trophies

- » Do well in a game, earn Gamerscore / Trophies
- » Gamerscore: accumulated Achievement points
- » The score will only ever go up, giving permanent value to the account



06-19-2009, 8:07 PM

AngrySCORCH62

Rep: ★★★★★

G 21501

Zone: Recreation

Community User Level: 2

I think that party chat is ruining xbox live Reply

A lot of games are so quite and I think that anyone new to xbox live will have t making friends.

Also, people can use it to give their mate and team an unfair advantage, like in SnD.

Also, in objective games, when everyone is in chat it is pretty hard to use tactic stuff.

06-19-2009, 8:10 PM

Smith GTO

Rep: ★★★★★

G 9302

Zone: Pro

Community User Level: 2

Re: I think that party chat is ruining xbox live Reply

I agree, very few talk over game chat now.
Very annoying on L4D when you're trying to communicate with team mates.

06-19-2009, 9:10 PM

Grubish360

Rep: ★★★★★

G 21190

Zone: Recreation

Community User Level: 2

Re: I think that party chat is ruining xbox live Reply

Smith GTO wrote:

I agree, very few talk over game chat now.
Very annoying on L4D when you're trying to communicate with team mate

I quote the truth.
Why make timezones???

Privacy Settings

Use these settings to determine who can communicate with you, view your online status, played games, gamer profile or your user generated content.

Voice and Text

Decide who you communicate with using voice and text on Xbox LIVE.

Voice and text communication is available on Xbox LIVE. You can choose to allow communication from everyone, your friends, or no one. This setting applies to all Xbox LIVE system messages and friend requests.

Everyone Friends No one

Video

Decide who you communicate with using video on Xbox LIVE.

Video communication is available on Xbox LIVE. You can choose to allow communication from everyone, your friends, or no one. This setting applies to all Xbox LIVE system messages and friend requests.

Everyone Friends No one

Gamer Profile

Decide who can see your gamer profile on Xbox LIVE.

Everyone Friends No one

Online Status

Decide whether other users can see your online status on Xbox LIVE.

If you allow others to see your online status, they can see whether you are online, offline, or away, and whether you are available to play a game.

Everyone Friends No one

Member Content

Choose whether you can see member content on Xbox LIVE. This setting does not apply to your own content.

Everyone Friends No one

Played Games

Decide who can see your played games on Xbox LIVE.

Everyone Friends Only Blocked

Friends List

Decide who can see your friends list. If you allow others to see your friends list, they can see who your friends are.

Everyone Friends Only Blocked

It may take up to 4 hours for your changes to appear on your console.

Gamer



Rep ★★★★★

 15777

Zone Recreation

Community User Level: **1**

Everyone Friends Only Blocked

Gamerscore and the Underground Economy

Buying and Selling

Posts: 187
Joined: May 2009
Reputation: 3
h4x\$: 0.00

RE: Xbox Live GamerScore Editor

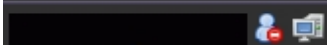
Offline 39 Mins
Last Playing Call of Duty 4

138,350

BUT I AM SELLING THIS TONIGHT SO DONT ADD IT ADD i R [redacted] thats gonna be my new GT and will be modding that when im back at my house in 1 week ;)

How Much For This Account ?

Yesterday, 06:23 PM (This post was last modified: Yesterday 06:28 PM by [redacted])



Privileged



2	z Swordyyy - F94		BUNGIE General, Grade 3		50	
	Kills: 75,779	Total Games: 11,058				
	Deaths: 62,888	Total EXP: 4,679	3	1	15	6
Assists: 28,486	powered by www.bungie.net				10	

2	z Swordyyy - F94	50	
Total Games: 11,058			
Total EXP: 4,679		3	1
BUNGIE bungie.net			

	AYo SwordySword
Member Since: 5/13/2009	
BUNGIE bungie.net	

And it has over 28000 GS With RECON ! Plus a 50 in 7 Playlist and Also 6th In CoD4 and CoD5 2nd. And Rank 4 in GoW2



XBOX LIVE SERVICES ACCOUNT STEALING

ok so for now since i am extremely low on money and offering my xbox live account services.

Now i only take paypal and this process usually takes 1-2 days but here is the info i will give you when i get the account.

First name:

Last name:

Phone #:

CC Type:

Address:

Zipcode:

NEW EMAIL* address:


NEW EMAIL* password:

*You will also get a tut made by me on how to keep the account 95% of the time ;)

System Exploitation in Game Sessions

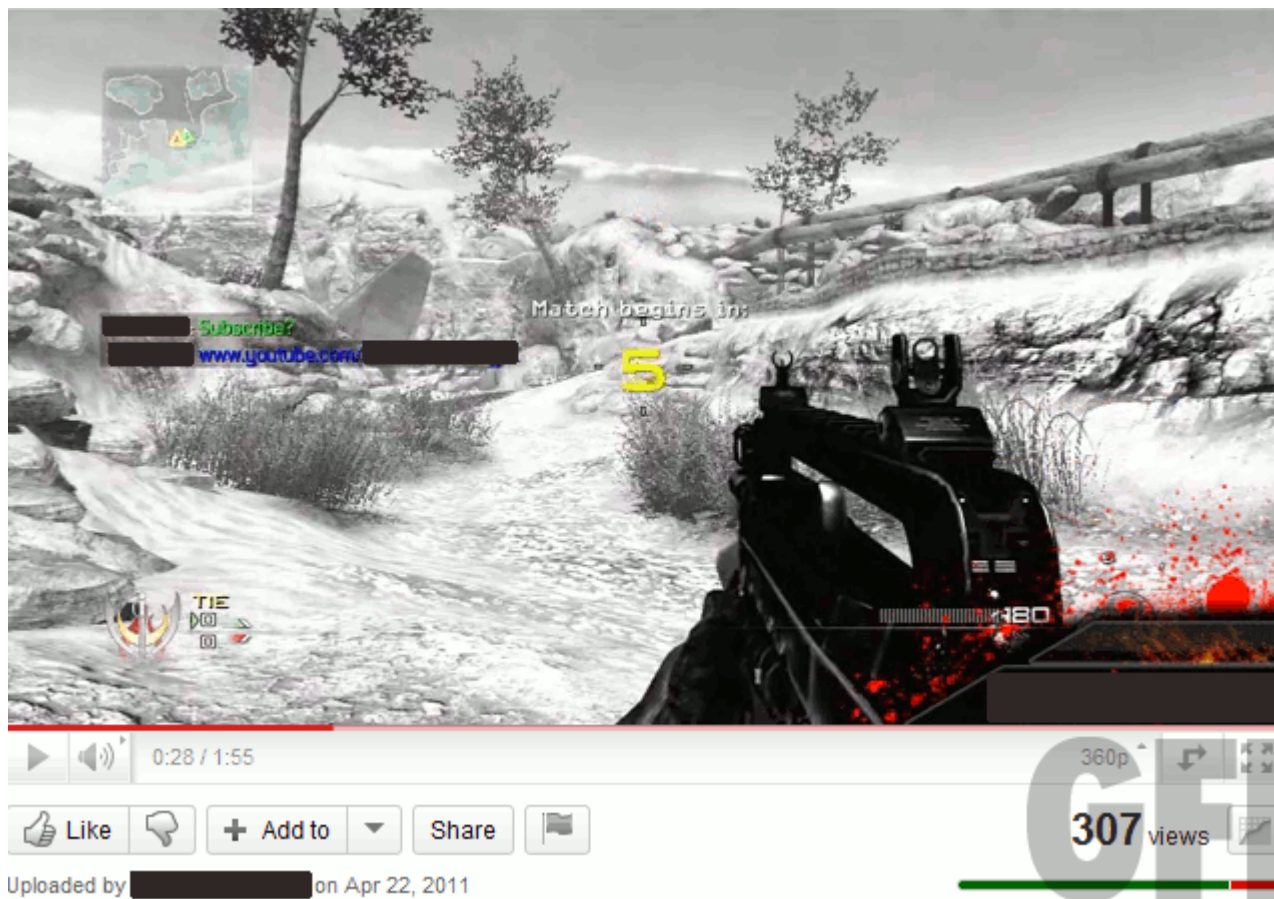
Rank	Picture	GamerTag	Country	Points	Zone
1		Momie		131447	Pro <i>Programmer, Splinter Cell series, Ubisoft</i>
2		Zubbie		105785	Recreation <i>Xbox Live Operations</i>
3		Weapon360		101019	Recreation <i>Technical Standards Analyst, Midway Home Entertainment</i>
4		Waylander73		98005	Underground <i>Producer, Rare Ltd</i>
5		Mad Massey		91623	Pro <i>Level Designer, Certain Affinity</i>
6		GiantBombing		89519	Recreation <i>Co-founder, giantbomb.com</i>
7		BlitzedKraig		87687	Recreation <i>Lead Designer of Blitz: The League, created by Midway</i>
8		irql		86999	Underground <i>Xbox 360 Launch Team</i>
9		MrNintendo1985		86614	Recreation <i>Senior Associate Producer - Pandemic Studios Australia</i>
10		Stepto		86565	Underground <i>Xbox Live Policy Manager</i>
11		Svengali		83502	Recreation <i>Xbox 360 Launch Team</i>
12		HkySk8r187		82190	Pro <i>Designer, Call of Duty Series, Infinity Ward</i>

Players		Score
X	Blue Team	0
H41	F u ck Microsoft M00	0
▼	F u ck Halo M02	0
	F u ck Xbox M03	0
	F u ck Bungie M01	0
1	Red Team	0
	HITIKU J16	0
	CivilDoG C89	0
X	I LunchBox I C89 H41	0
X	Aflac316 J16 A16	0

Hold  to activate.



System Exploitation in Game Sessions



System

--:[Setup/Fee's]:--

Just Bot Setup [Nothing else]

\$5 - Depending on your connection speed!

Bot + Booter Setup

\$10 - Depending on your connection speed!

Configure all my network Internet & Settings
& Firewall Setup To make my booter work

\$5- Depending on your connection speed!

Full Setup Configure Internet/router Settings
& Fully Edit my BOT And fully setup my Botnet
And change my icon of my Bot

\$20 - Depending on your connection speed!

--:[Extras For your Booter]:--

\$2 - [1 Zombie/Bot Added to your booter.]

\$4 - [2 Zombie/Bot Added to your booter.]

Basiclly It's \$2 per bot.

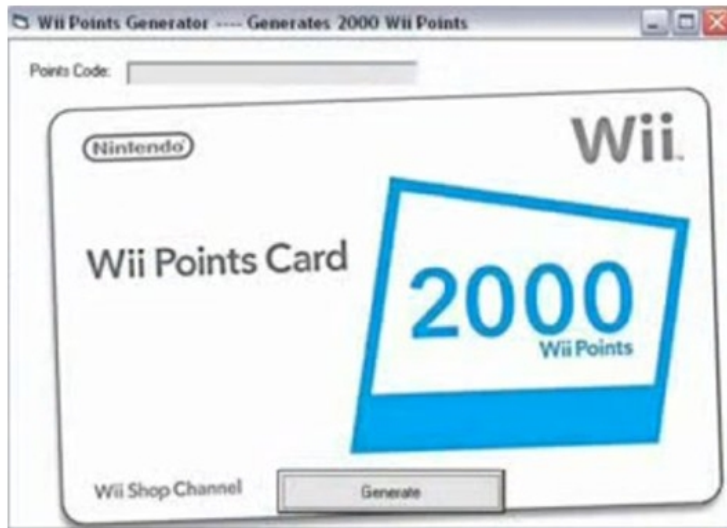
Social Engineering and Miscellaneous Tools

Social Engineering and Miscellaneous Tools

The screenshot displays the Xbox Live Message Center interface. At the top left, it says "Message Center" with an envelope icon. At the top right, there is a "Back to My Xbox" link with a small icon. Below this, on a dark grey bar, is a "Back to My Messages" link with an envelope icon. The main content area is split into three sections:

- Profile Card (Left):** Shows a user's profile with a redacted name, a yellow level bar, a "Rep" of five stars, a "G" rating, and "1750" points. The "Zone" is listed as "Pro". Below the profile are icons for "4" (a green star), "SOF" (a blue eye), "CALL-OUTY" (a red "SOF" logo), and "3" (a gold "3" with a star).
- Message Text (Center):** "If you are wanting points all you have to do is send us your Username,Email,and Password.After that we will log in and give you the points.Thank you"
- Action Buttons (Right):** A vertical stack of four buttons: "Reply", "Delete", "View Profile", and "Block Communication".

At the bottom of the profile card, it says "Sent: 12/20/2008 8:50 PM" and "Expires in 29 days".



Social Engineering and Miscellaneous Tools

Complete the Quick Survey to Continue

ou'll have your download in no time! Just complete any survey below with your valid information and the download will unc

Survey List:

Consumers can receive free, no obligation auto insurance quotes to find the cheapest plan possible.

Want a Starbucks Gift Card? Click to get started!

Do you want free samples? Register for Lifescript Advantage! Free offers for your health!

Play PacMac for FREE!

Who is better, McDonalds or Burger King? Tell us and receive \$100 worth of FREE McDonlad

GFI[®]

Social Engineering and Miscellaneous Tools

The screenshot shows a Windows XP desktop with a system scan progress window open. The window displays the results of a scan for trojans on various drives and folders. A prominent red banner reads "Your Computer is Infected!". Below this, a table lists three detected trojans: Trojan-IM.Win16.PS.fp, Trojan.Win32.SubSys.dr, and Trojan-Clicker.HTML.IFrame.bk, all with a "Critical" risk level and "Waiting removal" state. A progress bar shows 94% completion.

System scan progress

Shared Documents Found 18 trojans

My Documents Found 19 trojans

Hard drives

Local Disk (C:) Found 235 trojans

Local Disk (D:) Found 18 trojans

DVD

DVD-RAM Drive (E:)

94%

Now checking: batcpbxv.cmd

Your Computer is Infected!

fileinfos and actions:

Name	Risk level	Date	Files infected	State
Trojan-IM.Win16.PS.fp	Critical	03/13/2010	15	Waiting removal
Trojan.Win32.SubSys.dr	Critical	05/13/2009	23	Waiting removal
Trojan-Clicker.HTML.IFrame.bk	Critical	04/17/2010	37	Waiting removal

Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords , credit cards and other personal information from your computer.

Social Engineering and Miscellaneous Tools

The screenshot shows a web-based interface for a social engineering tool. On the left side, there is a control panel with a dropdown menu set to "Facebook", an "eMail:" field with a blacked-out input, the Facebook logo, and two buttons: "Freeze" and "Stop Freezing". Below these is a checked checkbox labeled "Let me watch" and a status bar that reads "Freezing Completed".

The main content area on the right is titled "Facebook Login" and contains a red error message box with the text: "You have exceeded the number of invalid login attempts that we allow for your account. If you have forgotten your password, **reset your password here.**"

Community



0

3

Messages (16 New)

12:48

Create New

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend

maximpunish10

Wants to be your friend



maximpunish10
wants to be your friend

Select

Back

Create

The background features a gradient from light blue at the top to white at the bottom, overlaid with several thin, flowing, wavy lines in shades of blue and white that create a sense of motion and depth.

Threats to Business

Threats to Business

- » survey of 200 senior IT decision-makers in public and private sector organizations around the globe
- » 4 in 10: no idea of the threats posed by consoles
- » 8 in 10: no record of who uses the console
- » 49% have a console in the workplace
- » 44% have a net connected console
- » 48% have a Wii, xbox in 2nd place, PS3 in 3rd.

Threats to Business

My Community
Inside Xbox
My Friends
Music Marketplace

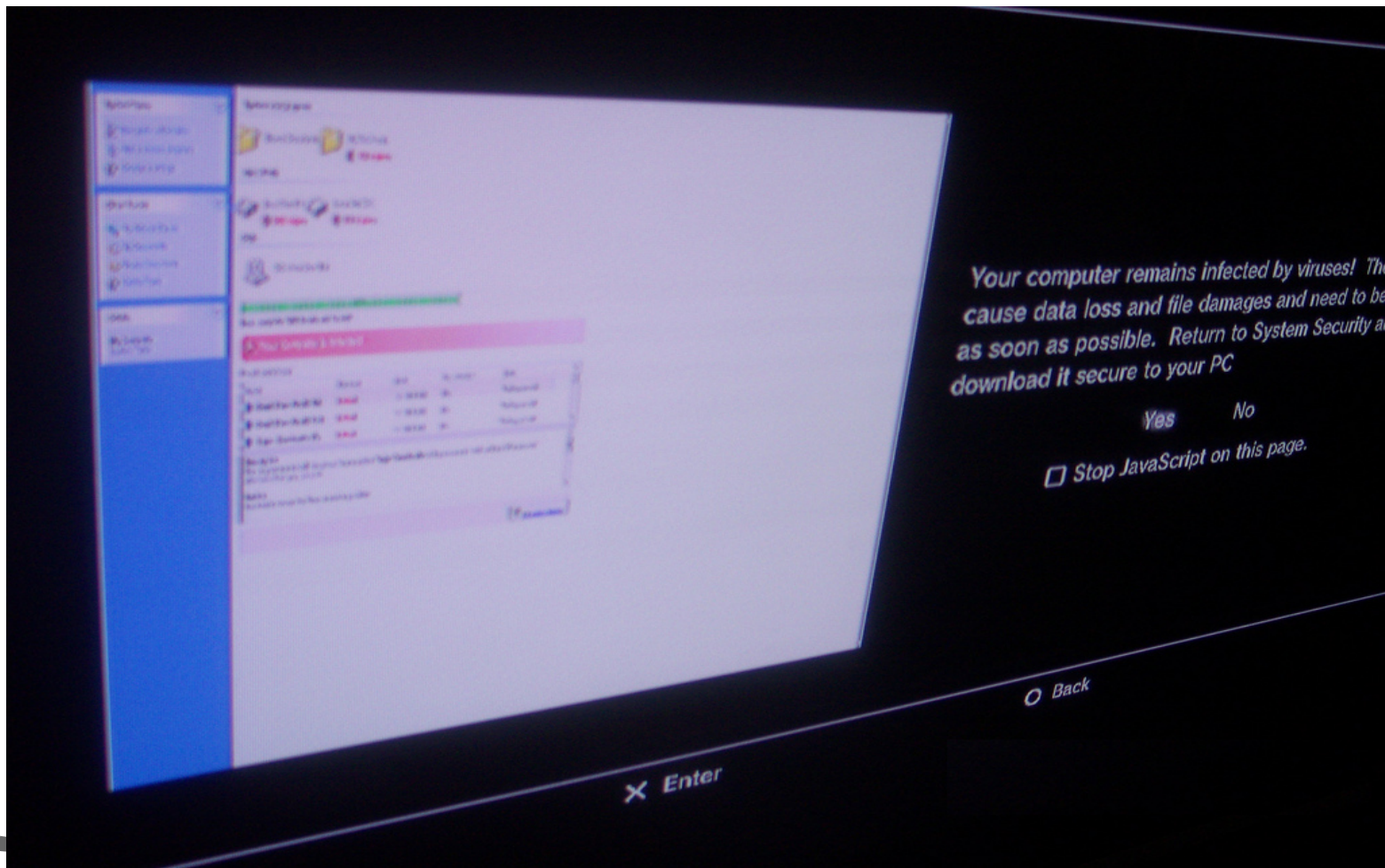
last.fm

Free Personalized Radio
Exclusive for Gold members

Music Games and Stores
Discover the latest tracks

Rocky Horror
Guitar Hero

Threats to Business



Threats to Business - Solutions

- » Put someone in charge of console management
- » Use “Parental Lockout” features to require passwords
- » Keep a logbook to record who uses it and when
- » Don’t use your company name in your gaming account
- » Does the console really need to be online?

The End?

Thank You!

GFI Software

www.gfi.com

GFI Labs Blog:

Sunbeltblog.blogspot.com

Twitter (PH Labs account):

[@gfilabsph](https://twitter.com/gfilabsph)

Twitter (Personal account):

[@paperghost](https://twitter.com/paperghost)

Marketing / PR Only:

(+63) 917 879 0216