

Government Data and Social Engineering in the Work Place

CORPORATE TRAINING

BY BE SURE CONSULTING INC.

2021/2022

Cyber-Safe At Work

BY

DETECTIVE RICH WISTOCKI (RET.) NAPERVILLE POLICE
DEPARTMENT HIGH TECHNOLOGY CRIMES UNIT

2021 COPYRIGHT BE SURE CONSULTING

Biography

- Detective 30 Years of Service (RET.)
- Naperville IL Police Department
- High Technology Crimes Unit
- SWAT Sniper 22 Years
- Internet Crimes Against Children Task Force (ICAC)
- United States Secret Service Chicago Electronic Crimes Task Force
- Authored The Illinois Sexting, Cyber-Bullying, and Swatting Laws



CYBER-SAFETY THREATS

What are some of the threats you may encounter every day?

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

Spyware

Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.

Objectives

- How does a Corporation get compromised?
- What types of security should we be concerned about?
- Understand the principles of social engineering
- Define the goals of social engineering
- Recognize the signs of social engineering
- Identify ways to protect yourself from social engineering

What Is Your Responsibility?

- Security is Everyone's Responsibility
- If You See Something, Say Something!
- If You Think You Opened Something Or Gave Out Sensitive Data, Contact Your IT Immediately!

Data Security Touches 3 Levels

- Physical Security
- Technological Security
 - Application Security
 - Operating System Security
 - Network Security
- Policies & Procedures

Physical Security

- Limiting access to physical space to prevent asset theft and unauthorized entry
- Protecting against information leakage and document theft
- Dumpster Diving - gathering sensitive information by sifting through the company's garbage
- SHRED BINS



Technological Security (Application Security)

- No flaws in identity verification process
 - Who is using the system
 - Are Passwords Secure and Changed Routinely
- Configure server correctly
 - local files
 - database content
- Interpret data with sincerity and concern
 - If there is a reported breach, who interprets the data?
 - Is there a Emergency Response Protocol?



PROTECT PASSWORDS

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.
- Change your passwords periodically.
- **Put into Effect 2 Step Authentication**
- When choosing a password:
 - Mix upper and lower case letters
 - Use a minimum of 8 characters

Technological Security User Operating System

- Some Application are likely contains vulnerabilities
 - Regularly download patches to eliminate (e.g. Windows Update for critical patches)
 - Some hackers expose these vulnerabilities and hold the company for ransom or else they will release the vulnerability.
 - This allows the corporation to be hacked.
- Network Security: mitigate malicious traffic
- Tools: Firewalls & Intrusion Detection Systems



INSTALL OS/SOFTWARE UPDATES

➤ Keep Your Operating System Up To Date

Install Windows Updates Weekly

REBOOT LAPTOP DAILY!

- 1) Make sure you complete a "SOFT" shutdown of your computer regularly.
- 2) Windows button and then Shut Down or ReStart
- 3) This allows any MSN updates or patches that needs to be installed taken care of ASAP

If You Have A MAC Update:

- 1) Choose Apple menu > System Preferences, then click App Store.
- 2) Select "Automatically check for updates." To have your Mac download updates without asking, select "Download newly available updates in the background."



ANTI-VIRUS SOFTWARE

- Find out what software your city/government uses.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.



AVOID SPYWARE/ADWARE

 Malwarebytes™

- Spyware and adware take up memory and can slow down your computer or cause other problems. Software such as Malware Bytes Does A GREAT job protecting your systems.
- Watch for allusions to spyware and adware in user agreements before installing free software programs. Usually you should watch for the checked boxes on any internet download.
- Be wary of invitations to download software from unknown internet sources.



BACK UP ALL FILES

➤ Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.

➤ INSERT NETWORK FOLDER & MICROSOFT ONEDRIVE Icons



Top things you can do to protect your information



1. Check Anti-virus Software



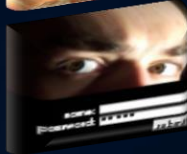
2. Avoid Spyware/Adware



3. Protect Passwords



4. Back up Important Files



5. Install OS/Software Updates

Policies & Procedures

➤ Social Engineering

- Taking advantage of unsuspecting employees and manipulates the employee

➤ Guard sensitive corporate information

- Training the employee about malicious attachments and links
- Testing the employee to ascertain if they will open the malicious link
- Remedial Training for that employee

➤ Employees need to be aware

➤ Does the corporation have an acceptable use policy?

What is “Social Engineering?”

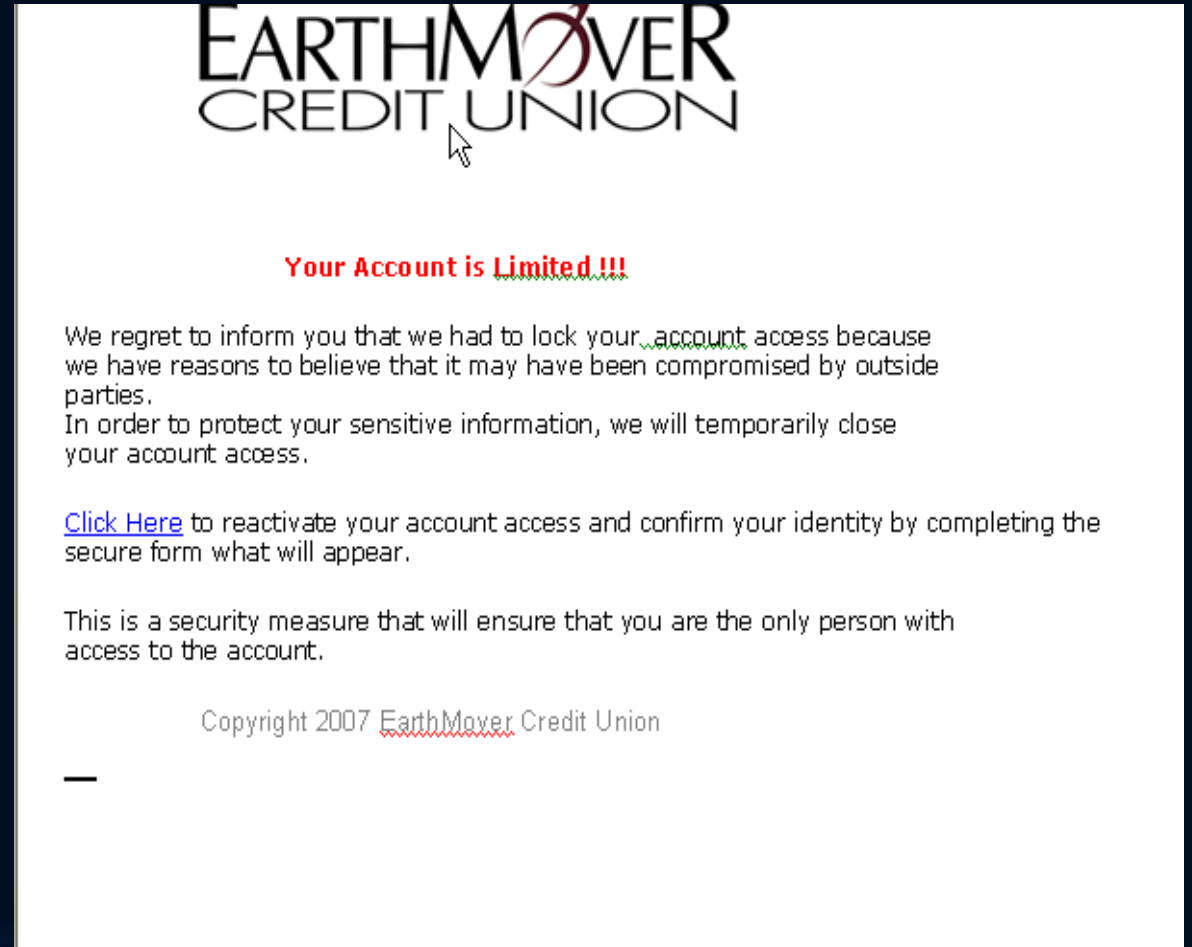
- Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. [Wikipedia](#)

“Phishing”

- This the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do. For example: sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Example of Phishing

- Financial institutions you belong to will NEVER solicit you via email, unless you request it.
- Right click on the link
- Go to properties or open link.
- Look at the website and you will see who actually set up the scam.



What are they looking for?

- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
- **Have you seen on FB to post childhood memories?**
 - What's the name of your first pet?
 - What is your maiden name?
 - When was your mother/father born?
 - Where were you born?

Tactics

- Pretexting – Creating a fake scenario
- Phishing – Send out bait to fool victims into giving away their information
- Fake Websites – Molded to look like the real thing. Log in with real credentials that are now compromised
 - iTunes
 - Amazon
 - Comcast
- Fake Pop-up – Pops up in front of real web site to obtain user credentials

How does it work exactly?





PREVENT IDENTITY THEFT

- Don't give out financial account numbers, Federal Tax ID, Banking Information, Social Security numbers and drivers license numbers . Call the recipient at a number you know to be connecting to them. NOT what they are telling you.
- **CONFIRM IN REAL LIFE!**
- Make sure you shred financial information and personal information when throwing it away
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information.

Who You Going To Call?

- These Threats Usually Occur In Other Countries. Middle of the night for us.
- No One is at the servers monitoring 24/7
- You must have an agreement with Emergency Response Specialists



Cyber-Safe At Home

BY

DETECTIVE RICH WISTOCKI (RET.) NAPERVILLE POLICE
DEPARTMENT HIGH TECHNOLOGY CRIMES UNIT

20 21COPYRIGHT BE SURE CONSULTING

How is a 13 year old affected by Social Media?

How many 4/5 grade students have Snap Chat, Instagram, Twitter?

- How old are they at this age? 9 to 11 Right?
- Did you know that you have to be 13 years old to have a Social Network?

Are You Lying About Your Age?

Kids Usually Round Up to Born in 2000

Now how old are they and who are they talking to?

PSA National Center from Missing and Exploited Children



How Do I Report Cyber-Crime to make it stop?

DOES IT FIT A CRIME?

- False Personation
- Harassing and Obscene Communications
- Cyber-Stalking
- Computer Tampering
- Wire Fraud
- Theft
- Embezzlement
- Copyright Infringement

What Evidence Do I Need To Give To IT TEAM?

What do I need to collect as evidence?

- Take a Screen Capture
- Get the User ID
- Get all pertinent dates and times
- Do not report it to the Social Network
- Make a detailed typed statement
- Print out and save items as a file
- Place ALL of these items in a flash drive

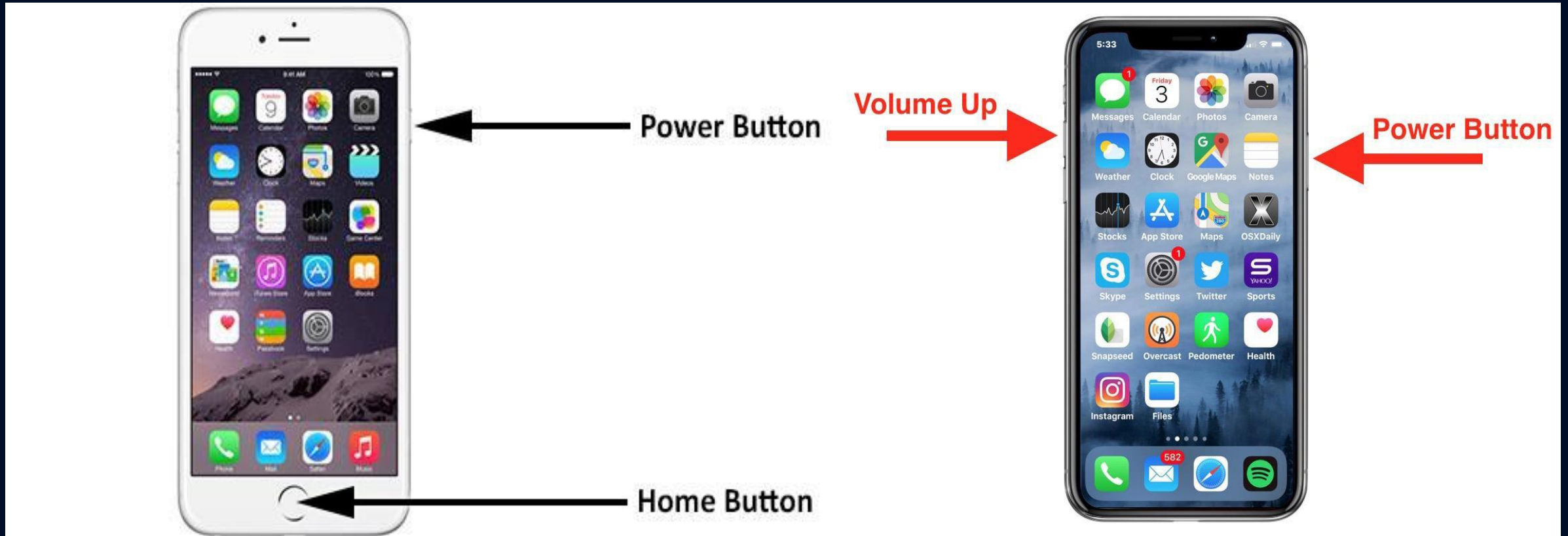
Screen Shots on a Windows Machine



Screen Shots on an Apple / Mac



How to take a screen shot on an iPhone



Regular iPhone

iPhone X

Take a screen shot! -Android



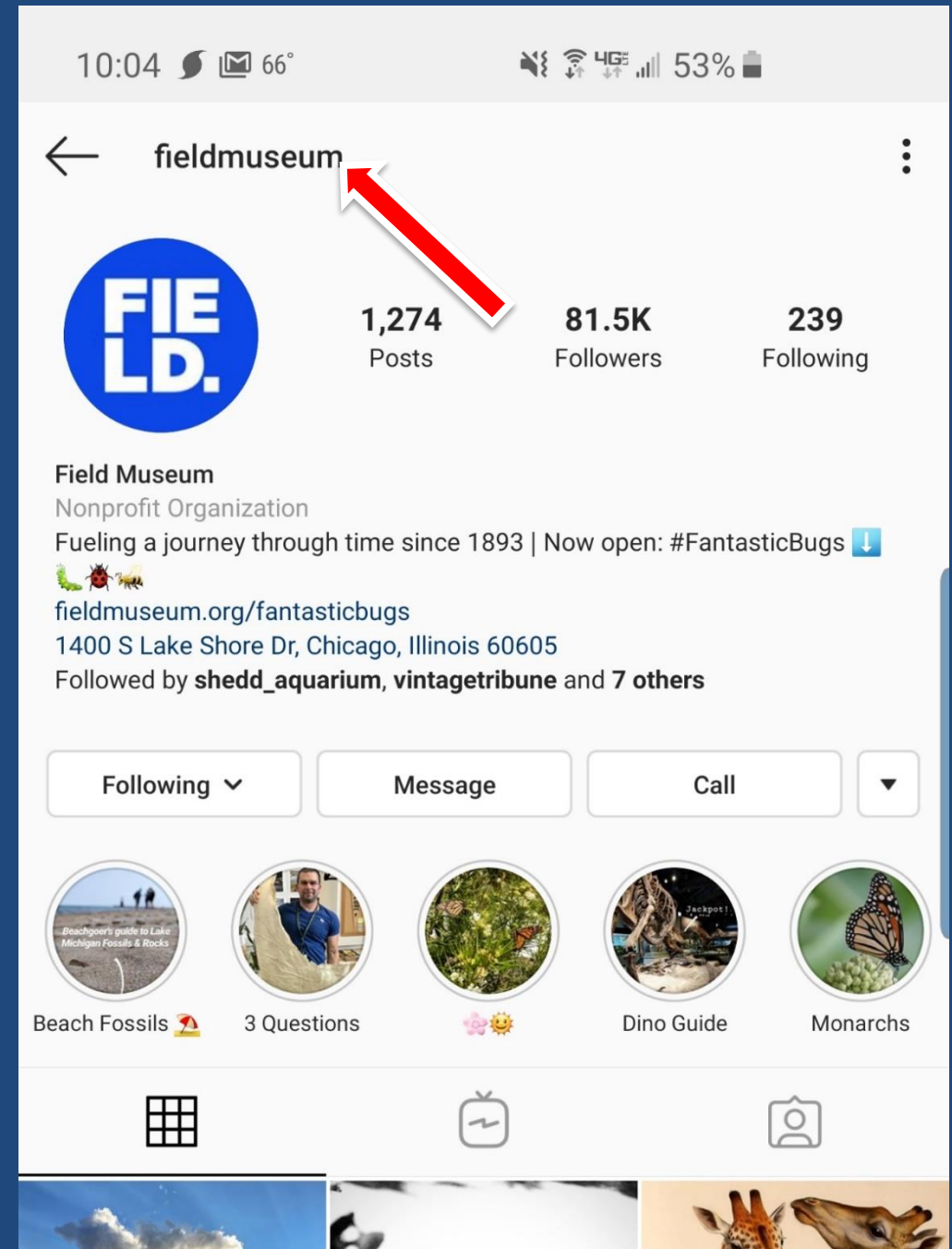
Power Button



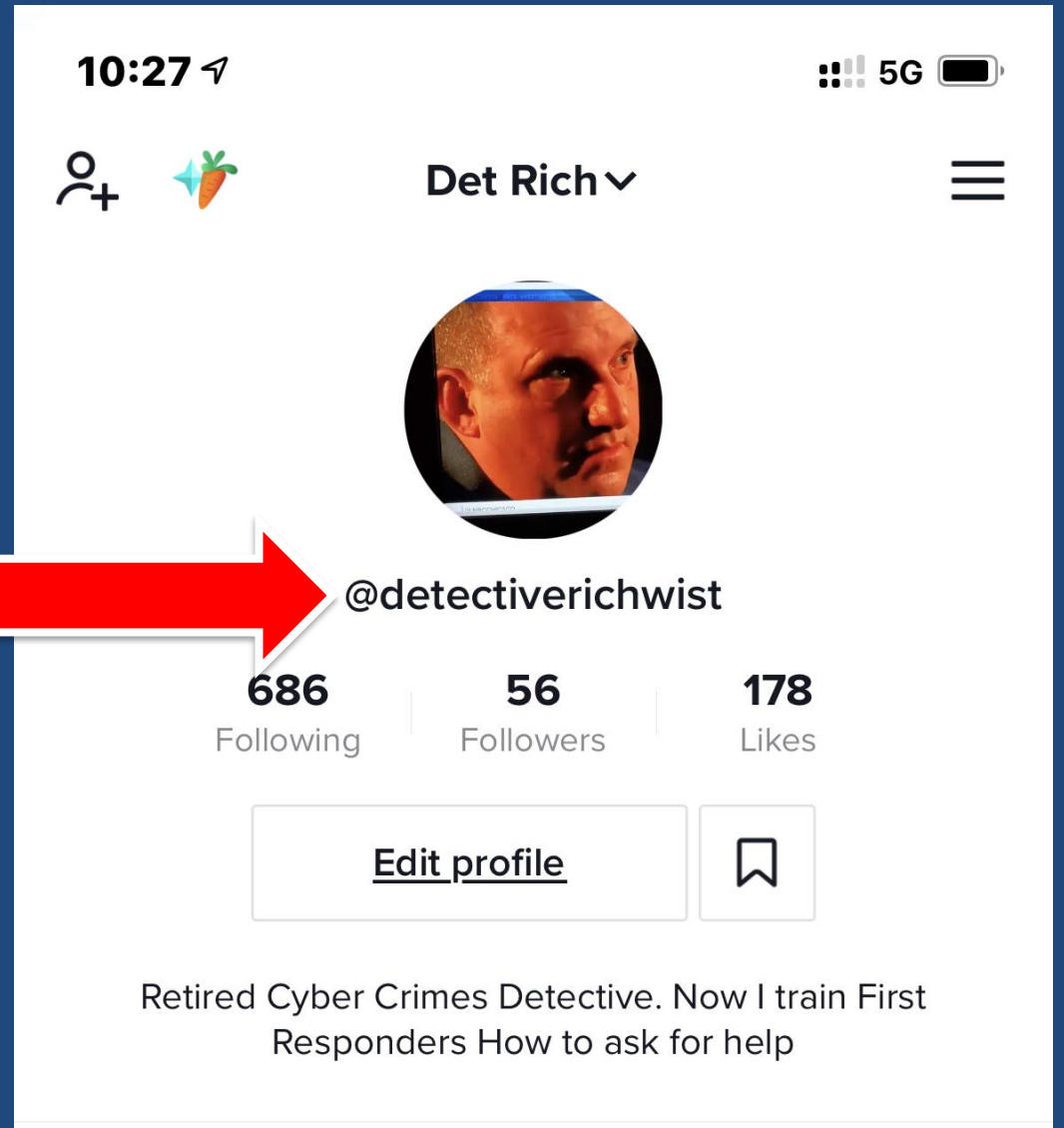
Home Button



Where are the Instagram User ID's?




TIKTOC User ID



10:27 5G

Det Rich



@detectiverichwist

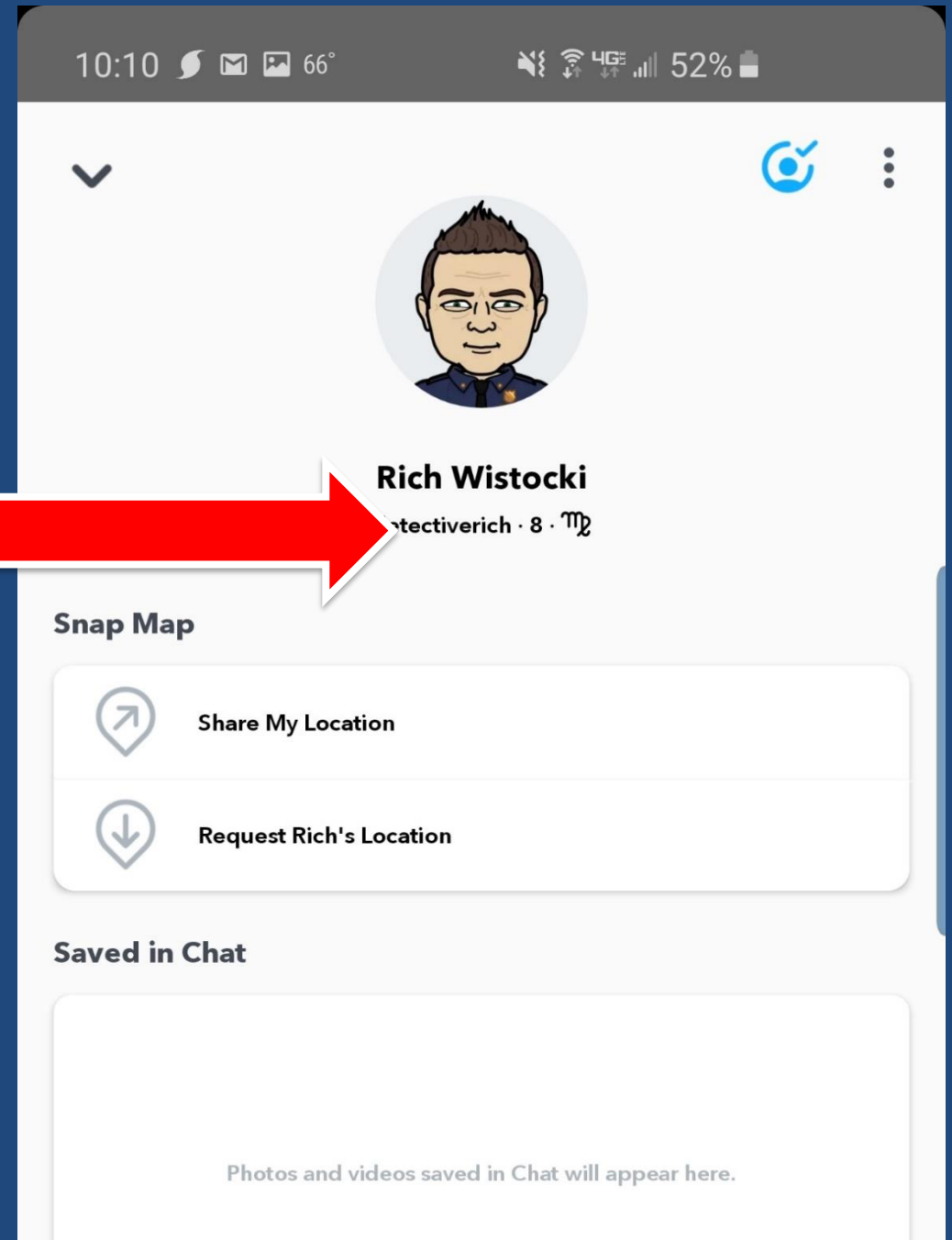
686 Following | 56 Followers | 178 Likes

[Edit profile](#)

Retired Cyber Crimes Detective. Now I train First Responders How to ask for help

A red arrow points from the left towards the username @detectiverichwist.

SNAPCHAT User ID



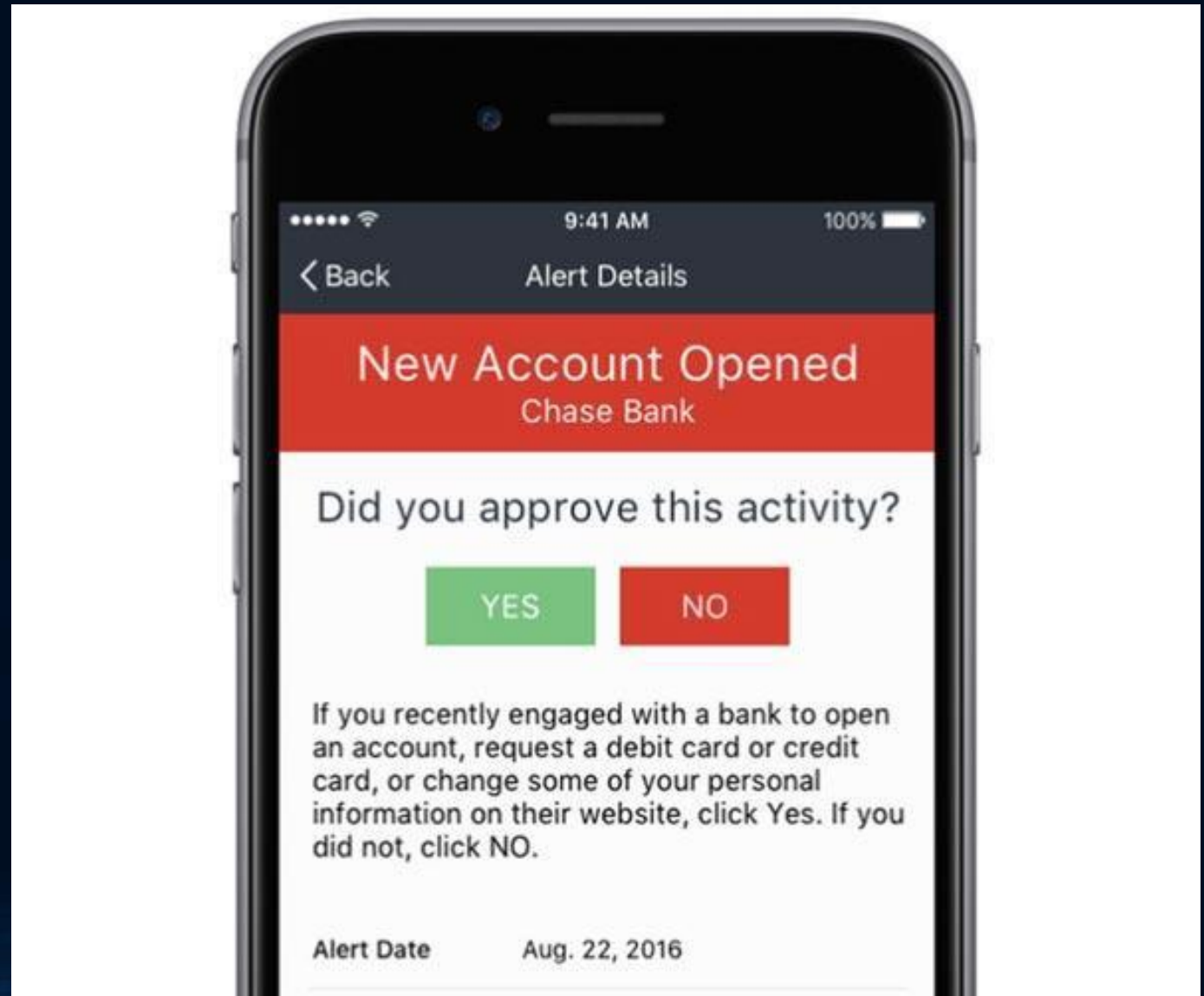
Does Life Lock Really Work?

- What is Doxing?
- Family members opening up accounts using your information?
- Someone stealing your garbage to get your billing information?



An alert from Norton / Life Lock

- Anytime anyone opens an account using your information.
- Anytime anyone does an inquiry on your information.
- Obtaining your credit score
- Dark Web transferring of files
- Any new credit cards in your name
- Any irregular activity on your investments



How Do I Monitor My Child's Cell Phone and Social Networks?



How Do I Monitor My Child's School Devices?



GoGuardian[®]



Lightspeed Systems[®]

My Contact Information

Detective Rich Wistocki (Ret.)

RichWistocki@besureconsulting.com

Phone: (630) 461-0044

www.BeSureConsulting.com

