



(Cybersecurity image; 2020)

Presented by:

The Alpha Omicron Nu chapter of
Phi Theta Kappa

ΦΘΚ

(PTK image, 2020)

At Eastern Gateway Community College



(Gator image, 2020)

Social Engineering

- Deceives people into believing it's legitimate by obtaining trust
- Tricks you into providing information or supplying access to accounts and/or resources
- Will use emotional triggers, such as curiosity, urgency, intimidation, and embarrassment
- Before clicking any links in emails, did you verify the sender? If it shows from your contacts, does the emails match the sender? Reach out and verify they send it to you if you can't otherwise tell.

Here is an email that was received stating that my Cash App account was locked, telling me to click on the link and verify my identity. As you can see, it shows the sender as Cash App, but the return email address goes somewhere different. No legitimate source will contact you like this and have the emails returned to a different site.

Account Verification Needed. [ref:_MNKDBSWC:ref]



Cash App Yesterday
to me ^



From Cash App • sorakim@bighitcorp.com

To me @outlook.com

Date Oct 8, 2020, 3:11 PM



Account Locked

Your Cash Account has been locked due to fraudulent activity occurred. to restore your payment history, personal information, and previous Cash Balance, you need to verify your identity by clicking the link below.

[Verify Identity](#)



Malware

- **Malicious Software** includes viruses, ransomware, and spyware
- Capable of installing malicious code on computers, causing damage to data & operating systems or gaining unauthorized access
- Word documents, PDF files, images, and other non-executable files can spread malware
- 1 in 14 web requests lead to malware

Ransomware

- Its purpose is to encrypt ALL your data and hold it for ransom
- You must pay and hope to get the correct key to regain your information
- A real threat that is happening to large & small organizations



Botnet

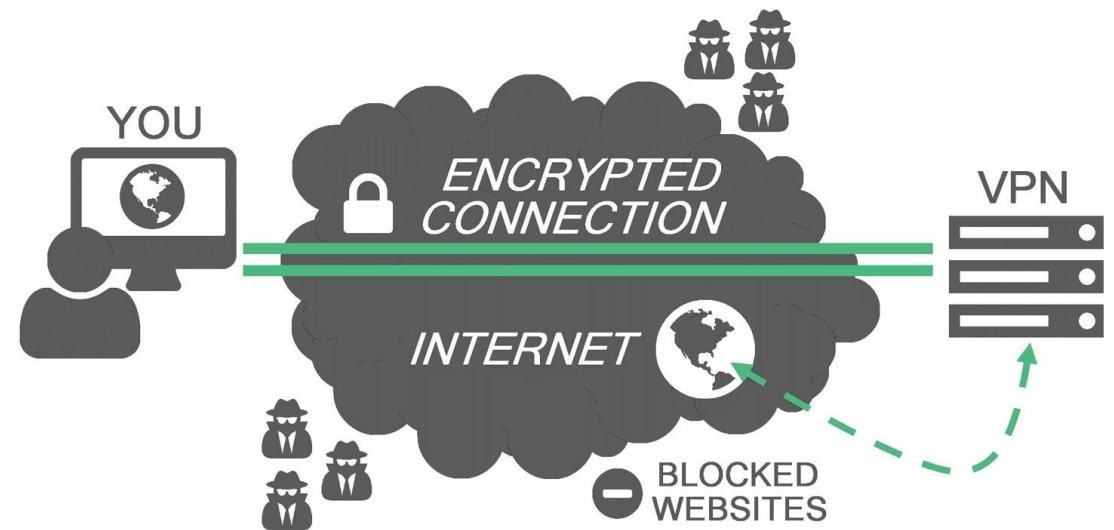
- A network of private computers infected with malicious software and controlled as a group without the owners' knowledge
- Often designed to carry out distributed attacks (DDoS – Distributed Denial of Service)
- Can use your computer to send emails, watch add-ons!



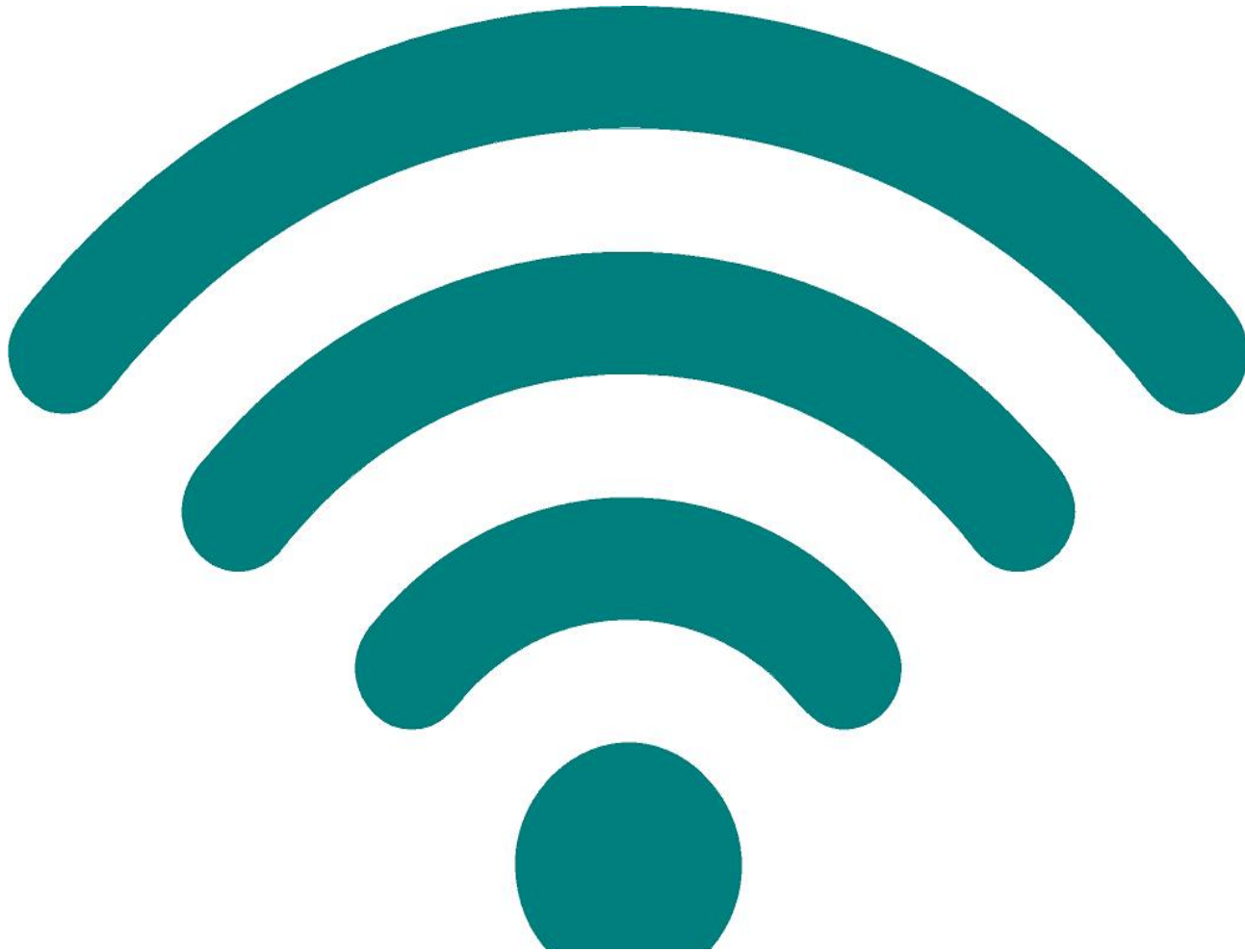
(botnet image; 2018)

VPN (Virtual Private Network)

- VPNs create a private network from a public internet connection
- VPNs masks your internet protocol (IP) address, so your online actions are virtually untraceable
- VPN service provide greater privacy than even a secured Wi-Fi hotspot



Wi-Fi



- WLANs (**W**ireless **L**ocal **A**rea **N**etworks) are often more vulnerable than cable connected LANs because radio signals are easy to capture
- Enabled by APS (Wireless Access Points) that create named “channels” or SSIDs (Service Set Identifier) that manage access
- WP2 and WP3 are examples of wireless security protocols

Public Wi-Fi



- Try not to use public, unsecured Wi-Fi as there is no way of knowing if it's secure
- Use mobile data, whenever possible
- If you need Wi-Fi for a computer or tablet, use your phone as a mobile hotspot
- If you must use public Wi-Fi, never access anything valuable like banking information and resist websites or accounts that require a login

Cryptomining



- Usually associated with bitcoin or other forms of digital currency.
- Cryptomining is the act of verifying cyberrcurrency transactions by solving math problems within the computer system.
- Cybercriminals use cryptomining malware to hack into a computers and use its processing power without anyone knowing. When cyberattackers are using the processing power WITHOUT the owner's knowledge, it becomes very illegal.



Cryptomining ... continued

- Cryptomining malware can slow down the computer because of the power the miner is stealing.
- Cryptomining malware may be attached to a scam email, hiding on websites, in weird social media messages, or can even pretend to be an app.
- You can prevent cryptomining malware by using anti-virus software, blocking add-ons and pop-ups, using strong passwords, checking an email's real source, and keeping your software updated.

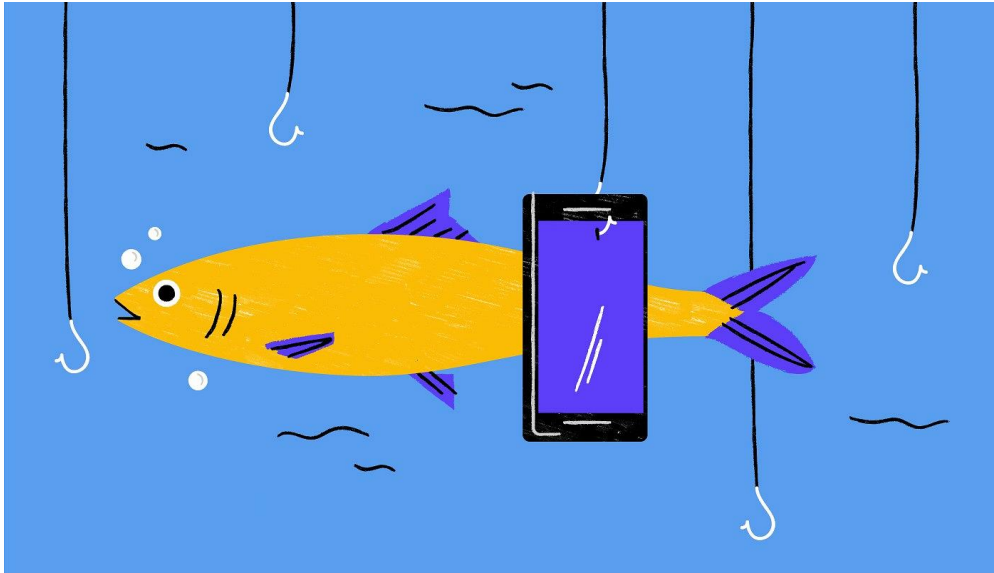
Juice Jacking

- Can occur when using a compromised public charging station installs malware when a portable device plugs in from public areas, such as an airport, train station, or a conference area
- Can pull data from your device and install malware



(juice jacking image, 2019)

Phishing



- One way that cyber criminals phish is by sending an email with a false link, or an attachment that has a software installer on it. When you click it, it installs itself.
- This software attempts to obtain sensitive information of data, as in username, passwords, credit card details, and PII (Personally Identifiable Information)

Phishing Types

- Spear Phishing: Directed at specific individuals or companies, such as executives that work in financial departments that have access to financial data
- Whaling: Directed specifically at senior executives and other high-profile targets. Content could look like a subpoena or VIP / customer complaint
- Voice Phishing: Phone messages claiming to be from a bank asking users to call a number regarding problems with their account
- SMS Phishing: Text messages with a link or phone numbers asking you to provide private data.

****Mobile devices make it difficult to verify web page links****

PII – Personally Identifiable Information

Credentials are the #1 target capture!

- Full name
- Birthday
- Phone numbers
- Home address
- Email address
- Biometrics (fingerprints used for some phones and computers)
- Passport & other ID information
- Credit card information



(credit card image, 2018)



60% of US citizens say they or their close family members have fallen victim to data-related fraud

Receipt Order HCCKQV3PZS ☆

 **Verification Inc** Oct 2
to me ▾ ⏪ ⋮




no name



Hello ,
We could not authorize your payment for the next order, so we suspended your account.

What's going on?
Some information on your account appears to be missing or incorrect .


Please update your account information by clicking the bouton below :  spelling

Login To Get Started

Regards,
Amazon Team

Copyright © 2020 Amazon, Inc. All rights reserved. Amazon is located at
2211 N. First St., San Jose, CA 95131

Receipt Order HCCKQV3PZS ☆

 **Verification Inc** Oct 2
to me ^ ⏪ ⋮

From Verification Inc • support@melhorescola.com.br

To me @outlook.com

Date Oct 2, 2020, 4:55 PM

that's NOT Amazon!



- **71% of all data breaches are financially motivated**
- **Hackers attack every 39 seconds; on average 2,244 times a day**
- **Data breaches exposed 4.1 BILLION records in the first half of 2019**
- **The average time to identify a breach in 2019 was 7 MONTHS**



Legitimate companies:

- Won't request your private information in emails
 - Should call you by your correct name
 - Have domain emails – MyName@amazon.com
 - Know how to spell and use acceptable grammar
 - Will not force you to their website
- **Be aware that a simple click in the background could take you to a bad place!****
- Don't send unsolicited attachments

Did you know?

Research shows that 91% of cyber incidents that occur inside an organization are caused by some form of human error, such as accidentally clicking a phishing email!




Stay aware!

- Be suspicious of emails, texts, or voice messages that request sensitive information or financial transactions. Hover over all hyperlinks before clicking to see what they're connected to.
- Use MFA (Multi-Factor Authentication) i.e., have a security code sent to your phone
- Keep browsers, mobile devices, and computers updated
- Where possible, don't reuse passwords for multiple accounts/devices
- Lock your screen when stepping away from your computer
- Follow company policies & if you don't know what they are, ASK!

Passwords should:

- Have a combination of random uppercase & lowercase letters
- Include numbers & special characters
 - *Hackers have ***dictionaries*** of passwords. They know you'll use @ for a, 1 for l, \$ for s, etc.*
- Not consist of only your pet's name
- Not use your address, birthday, or family members' birthdays
- Always be changed from the default
- Consist of a ***passphrase*** rather than a single word
 - Ex: MyC@tGe0rge or il0vedr@g0ns



Treat your
password like a
toothbrush;
don't share it &
change it often!

www.grc.com/haystack is a website that
can tell you how long it can take to crack
a password!

Ex: lovemycat would take 56.47 seconds
to crack but...

 ilovemycatgeorge<3 would take 4.06
trillion centuries!



Passwords to NEVER use!



123456789

12345678

1234567

123456

12345

123123

111111

666666

654321

Qwerty

qwerty1

Abc123

Abc123456

!@#\$%^&*

Passw0rd

password1

admin

charlie

Donald

football

Iloveyou

Monkey

Password

Princess

sunshine

welcome

zzxxccvvbb

Social Media Security

- Don't log into other apps via Facebook...**yes, including games!**
- Don't follow accounts with minimal followers and weird names and / or profile pictures
- Use unique passwords for each social account
Ex: FBmYc@tGe0rge; Myc@tGe0rgelG; etc.
- Keep your information as private as possible. Think before you share!
- Set your phone to automatically lock after a few minutes of inactivity
- Report spam and posts/people that don't follow acceptable standards (e.g., Facebook "Report" link)
- Wait a while to post vacation pictures, at least until you're back home. Don't advertise that your gone, for how long, etc.

Craigslist / FB Marketplace & Dating Sites



- Whether buying or selling, DO NOT give the other party your personal information such as address or phone #. Use the platforms message system
- NEVER meet with people alone, always take a friend with you
- DO NOT meet at your house or theirs! Meet in public places such as a library parking lot or a local fire or police station parking lot
- If you are meeting someone from a dating site, the same applies. Do not meet at homes. Go to restaurant, sporting event, somewhere there are lots of other people. Do not leave food or drink unattended.
- Always make sure someone knows where you are, who you are with, approximate time you'll be back and check in periodically.
- Trafficking generates billions of dollars a year.

Stay Safe Tips

- Remove all information on devices prior to selling or discarding them
- Disable features that are not currently in use, such as Bluetooth or Wi-Fi
- While traveling, power down your devices completely before storing them
- Be aware of shoulder surfing, which is looking for confidential information or watching you enter passwords
- Never share devices with access to sensitive information or assets (networks/servers) with an unauthorized person, which includes you family members, especially via your user profile.
- If you work from home & have kids or others using your computer, make separate user profiles for each user

Links

- <https://www.facebook.com/safety>
- <https://zoom.us/docs/en-us/privacy-and-security.html>
- <https://about.instagram.com/en-us/community/safety>
- https://about.twitter.com/en_us/safety.html
- <https://support.snapchat.com/en-US/article/safety-tips-resources>
- <https://www.youtube.com/howyoutube/works/policies/community-guidelines/>



(logos image, 2018)

Physical Security Tips

- Keep your desk free of confidential information, i.e. don't put information on a sticky note and put it on your desk or computer screen
- Private information should be locked in a desk drawer when you are away for an extended period and at the end of every day
- Treat all devices, such as your computer, USB drives, and laptops as sensitive if they contain proprietary and sensitive data
- When possible, use a security badge to enter your building, and do not allow anyone to follow you in through a non-public entrance
- Check for ID and ask unknown individuals what the reason is for their visit to your workplace... "Can I help you?", "Who are you here to see?"

Want to learn more?

- <https://training.Fortinet.com>

is a great place to learn more about cyber security



- Cybersecurity & Infrastructure Security Agency,
<https://us-cert.cisa.gov/ncas/tips/ST04-001>



References:

- www.fortunly.com/statistics/data-breach-statistics#greaf
- www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/
- www.varonis.com/blog/cybersecurity-statistics/
- TAUW Cyber Security Webinar provided by NTECH Collaborative
- cyber.gov.au/acsc/view-all-content/threats/cryptomining

Image references (pg. 1)

- *Cybersecurity image* [graphic] mytechdecisions.com. <https://mytechdecisions.com/compliance/covid-19-cybersecurity-workforce/>
- *PTK image* [graphic] ptk.org. <https://www.ptk.org/media/graphic-standards/>
- *Gator image* [graphic] egcc.edu. https://egcc.edu/athletics-2/gatorlogo_4color/
- *Malware image* [graphic] paranet.com. <https://www.paranet.com/2018/06/26/10-tips-on-how-to-prevent-malware-infections/>
- *Ransomware image* [graphic] brightlineit.com. <https://brightlineit.com/detect-prevent-ransomware-attacks/>
- *Botnet image* [graphic] xenonstack.com. <https://www.xenonstack.com/insights/what-are-botnets/>
- *VPN image* [graphic] 9to5mac.com. <https://9to5mac.com/guides/vpn/>
- *Wi-fi signal logo* [graphic] tech-wonders.com. <https://www.tech-wonders.com/2019/08/how-to-improve-your-wifi-signal.html>
- *Security breach image* [graphic] forbes.com. <https://www.forbes.com/sites/louiscolumnbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/?sh=5ecb6ace3ce4>
- *Cryptomining image* [graphic] coinnoounce.com. <https://coinnoounce.com/cryptocurrency-mining-explained/>

Image references (pg. 2)

- *Cryptomining image* [graphic] coinounce.com. <https://coinounce.com/cryptocurrency-mining-explained/>
- *Juice jacking image* [graphic] techcrunch.com. https://techcrunch.com/2019/11/15/los-angeles-juice-jacking-usb/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xLmNvbS8&guce_referrer_sig=AQAAAI8za_UBhll6X69H8HasklluU6keRfEjp-F19PE0C9ZVsd3dc2yUBErF7xpqiSVCVqVPI_p994SnPynZNfhh6VW0ds8HsCrD3e4HzPEHC1w-sI5fnXm3CQS0xLjTyry22dyQL9nX1kr9AlhvVaR7DWZoXTs1Cf66U-MEudROF9G
- *Phishing image* [graphic] medium.com. <https://medium.com/jigsaw/how-to-spot-phishing-the-most-common-cyberattack-fed1360aacc2>
- *Credit card image* [graphic] zeolearn.com. <https://medium.com/jigsaw/how-to-spot-phishing-the-most-common-cyberattack-fed1360aacc2>
- *Security image* [graphic] medium.com. <https://medium.com/swlh/tech-debate-1-online-cloud-security-and-internet-security-with-machine-learning-and-a-i-d548ca06c0f4>
- *CL image* [graphic] shsthepapercut.com. <https://shsthepapercut.com/34726/entertainment/the-dangers-of-craigslist/>
- *Logos image* [graphic] overnightlabels.com. <https://www.overnightlabels.com/social-media-influences-packaging-design/>