YOUR CYBERSECURITY

Email Account Takeover

What is it?
A cybercriminal hacks an email account and reads emails so they can pose as the victim to steal money.

How can you defend against it?

Follow proper identification processes. Use secret passwords, phone call verifications, and video chats to help verify the identity of people you correspond with.

70% of cyberattacks use a combination of phishing & hacking

Phishing

What is it?
Cybercriminals pretend to be a trustworthy source in order to acquire sensitive information.

How can you defend against it?

- Hover over questionable links to reveal the true destination before clicking.
- Beware that secure websites start with **https**, not http.

Call Forwarding

What is it?
The cybercriminal takes over your cell phone number and impersonates you or reroutes your calls.

How can you defend against it?

- Follow proper identification verification processes. Consider using secret passwords to help verify the identity of people you're corresponding with.
- Check your monthly phone bill for any suspicious activity.

Malware

What is it?
Malicious software is created to damage/disable computers and computer systems, steal data, or gain unauthorized access to networks.

How can you defend against it?

- Install the most up-to-date antivirus and anti-spyware software on all devices and run regular scans.
- Make sure your networking equipment and computers are all still supported by the manufacturer.

Credential Replay

What is it?
Most people re-use passwords and usernames. Cybercriminals obtain these login credentials, test them in large numbers against financial institutions' websites to find matches.

How can you defend against it?

- Use a unique password for each account.
- Make each password unique and long and strong.

Social Engineering

What is it?
This involves manipulating or impersonating others to divulge sensitive, private information, and then demanding financial transactions be executed to avoid consequences.

How can you defend against it?

- Be selective about who you allow to join your social networks.
- Be cautious about the information you choose to share on social media.

Spoofing

What is it?
A fake email header that gives the impression the email is from someone or somewhere other than the actual source.
Phone spoofing is a comparable common cyber threat using a similar phone number.

How can you defend against it?

- Carefully check the incoming emails.
- If an email or phone call are questionable, contact the sender through another trusted means.

REMEMBER TO

Be Strategic with Usernames/Passwords
Surf Safely
Limit What You Share Online
Safeguard Email Accounts
Keep Equipment Up to Date

IT IS EVERYONE'S PROBLEM

- Identity theft is the fastest growing crime in America.
  (Source: Trans Union Website, 01/14/2015)
- Someone's identity is stolen every 2-3 seconds.
  (Source: https://identity.utexas.edu/id-perspectives/top-10-myths-about-identity-theft)
- The average loss per identity theft incident is $4,930.
  (Source: U.S. Department of Justice, Javelin Strategy & Research)
- On average it takes 600 hours to recover from identity theft.
  (Source: The Identity Theft Resource Center website, April 28, 2015)

Cybercriminals are constantly trying to steal data & identities:

Personal Data Stolen

- Social Security numbers
- Usernames
- Date of birth
- Passwords
- Credit card numbers
- Account numbers
- Employment information
- Checks

Resulting Crimes

- Fraudulent Transactions
  - – trading
  - – electronic funds or wire transfers
  - – account opening
- Identity Theft
  - – using stolen Social Security numbers for employment or other gain
  - – filing a false tax return
  - – impersonating another person