PROTECTING YOUR IDENTITY, DATA, + ASSETS

IT'S NOT A MATTER OF IF, BUT WHEN...

17.6 million
people experienced identity theft in 2014

Source: Bureau of Justice Statistics

63%
of confirmed data breaches involved weak, default, or stolen passwords

Source: Verizon 2016 Data Breach Investigations Report

Identity fraud is a serious issue. Fraudsters have stolen $112 billion in the past six years, equating to

$35,600
stolen per minute

Source: 2016 Javelin Strategy & Research, Survey Report Results

DISCUSSION TOPICS

+ Common cyber threats
+ How cybercriminals use stolen data
+ Protecting your data
+ Other helpful resources

COMMON
CYBER THREATS

COMMON CYBER THREATS

1. Email Account Takeover
2. Malware
3. Phishing
4. Credential Replay
5. Social Engineering
6. Call Forwarding
7. Spoofing

EMAIL ACCOUNT TAKEOVER

WHAT IS IT?

A cybercriminal hacks an email account and reads emails to learn about the victim and their habits so they can pose as the victim to steal money.

WHAT DOES IT LOOK LIKE?

Your email is hacked, and posing as you, the cybercriminal emails your advisor instructions to forward funds to an account.

HOW DOES IT HAPPEN?

Cybercriminals find vulnerabilities within service providers' servers or personal users' IP addresses to gain access to login credentials, or to the email account directly.

WHAT'S THE IMPACT?

Because the cybercriminal has access to your email and can impersonate you, the recipient of the cybercriminal's email believes the correspondence comes from you. The cybercriminal may provide instructions within the email to transfer funds to a fraudulent account. Without proper verification, the money could be transferred and stolen.

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.

MALWARE

HOW DOES IT WORK?

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

WHAT DOES IT LOOK LIKE?

Examples of malware include viruses, worms, trojan horses, ransomware, and spyware.

HOW DOES IT HAPPEN?

Malware may be installed on a computer when a user clicks an unsafe link, opens an infected file, or visits a legitimate website that could contain adware.

WHAT'S THE IMPACT?

Malware can delete files or directory information, or it may allow attackers to covertly gather personal data, including financial information and usernames and passwords.

HOW CAN YOU DEFEND AGAINST IT?

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

PHISHING

WHAT IS IT?
Cybercriminals pretend to be a trustworthy source in order to acquire sensitive personal information such as usernames, passwords, social security numbers, and credit card details.

WHAT DOES IT LOOK LIKE?
An email from a seemingly legitimate email address instructs you to click on a link to take action (e.g., “validate your account,” “confirm your identity,” “access your tax refund”). The link brings you to a website requiring you to enter your personal information.

HOW DOES IT HAPPEN?
Because the cybercriminal masquerades as a legitimate source (e.g., financial institution employee, realtor, banker), you believe the request is from a trusted source and you unwittingly oblige when they ask you for your personal information.

WHAT’S THE IMPACT?
Victims of phishing may have malware installed on their computer systems or have their identity stolen.

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.*

70% of cyberattacks use a combination of phishing and hacking

Source: Verizon 2015 Data Breach Investigations Report

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, and then request fraudulent fund transfers.

WHAT DOES IT LOOK LIKE?

Cybercriminals hope to access a few accounts by using a large cache of stolen login credentials to access a firm's online accounts.

HOW DOES IT HAPPEN?

Cybercriminals can easily purchase large numbers of stolen login credentials from the dark web.

WHAT'S THE IMPACT?

Your account is compromised, and the cybercriminal can quickly re-use your credentials to access other accounts, and steal additional funds and your confidential data before detection.

HOW CAN YOU DEFEND AGAINST IT?

- Use a unique password for each account to prevent a quick and invasive attack on all of your accounts.
- Make each password unique and long and strong. Use 8-12 characters, upper- and lowercase letters, and symbols.

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.

WHAT'S THE IMPACT?

The cybercriminal commits fraud, steals your money, and disappears.

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, keeping your personal information private (e.g., home address, phone number, employer, vacation dates, birthdate).

CALL FORWARDING

WHAT IS IT?

The cybercriminal takes over your cell phone number and impersonates you or reroutes your calls.

WHAT DOES IT LOOK LIKE?

A cybercriminal gets the phone company to forward your cell number to their cell phone so they can impersonate you when your bank calls you back for verification before transferring funds or opening accounts.

HOW DOES IT HAPPEN?

Cybercriminals scam the phone company into forwarding phone calls. They may also use scanners, eavesdrop, clone your phone identity, and sell bogus ringtones or other gadgets to access your phone.

WHAT'S THE IMPACT?

Your phone is compromised, your conversations may be accessed, and your identity may be stolen.

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. This may include phone numbers you don't recognize or calls placed at odd times (e.g., during works hours, while overseas or on vacation).

SPOOFING

WHAT IS IT?

A fake email header that gives the impression the email is from someone or somewhere other than the actual source, with the goal of tricking the recipient into opening and responding to the email. Phone spoofing is a comparable common cyber threat using a similar phone number.

WHAT DOES IT LOOK LIKE?

Your advisor receives an email from a cybercriminal who impersonates you and confirms a fraudulent wire transfer request.

HOW DOES IT HAPPEN?

The cybercriminal creates an email address nearly identical to your email address (i.e., off by a character).

WHAT'S THE IMPACT?

Similar to the other cyberattacks we've discussed, your money is stolen, and you become the victim of fraud and/or identity theft.

HOW CAN YOU DEFEND AGAINST IT?

- Carefully check the incoming emails for the proper email address and the accuracy of the spelling of the sender's name.
- If an email or phone call are questionable, contact the sender directly, using the email address or phone number you have on file for that individual.

HOW CYBERCRIMINALS
USE STOLEN DATA

HOW CYBERCRIMINALS USE STOLEN DATA

Cybercriminals are constantly trying to steal data and 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

IDENTITY THEFT IS EVERYONE'S PROBLEM

Identity theft is the fastest growing crime in America.

Source: Trans Union Website, January 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

HOW YOU CAN PROTECT YOUR DATA

WAYS YOU CAN PROTECT YOUR DATA

BE STRATEGIC WITH USERNAMES/PASSWORDS

DO

- Create passwords that are long and strong, using 8-12 characters, upper and lowercase letters, numbers, and symbols.
- Use a unique password for each account to prevent a quick and invasive attack on all of your accounts, known as credential replay.
- Change your password often. (General rule of thumb: Change passwords every 90 days.)
- Where available, request a security token for two-factor authentication when accessing your accounts.

DON'T

- Use information that can be easily found about you online or otherwise.
- Share passwords with others.
- Store your passwords online.
- Use any part of your Social Security number, birth date, or other personal data when creating passwords.

SURF SAFELY

DO

- Use wireless networks you trust and know are protected.
- Be cautious when using public computers.
- Ensure you are downloading legitimate apps from trusted publishers.
- Be aware that secure websites start with *https,* not *http.*
- Be sure to log out completely (which terminates access) when exiting all websites to prevent cybercriminals from obtaining your personal information.
- Consider purchasing a personal Wi-Fi hot spot.
- Hover over questionable links to reveal the true destination before clicking.

DON'T

- Use public computers to access confidential information or accounts, or to perform financial transactions.
- Click on websites you don't know or on pop-up ads or banners.

PROTECT YOUR MONEY

DO

- Review your credit card, cell phone, and financial statements as soon as they are available.
- Contact your financial institution if you see anything suspicious on your statements.
- Help us protect your information and assets by following our guidelines for identification verification and procedures for transferring funds.

DON'T

- Send your personal identifiable information or account information via unsecure channels like email, chat, or text.
- Respond to requests for personal information from a unsolicited email or from an unsolicited incoming phone call.

LIMIT WHAT YOU SHARE ONLINE

DO

- Be very selective about the information you choose to share on social media and with whom you choose to share it.
- Keep your personal information private (home address, phone number, and birthdate).
- Set privacy and security settings on web services and devices to your comfort level for sharing.
- Configure your online accounts with two-factor authentication where available.

DON'T

- Post personal information about family and friends online.

SAFEGUARD EMAIL ACCOUNTS

DO

- Exercise caution when reviewing unsolicited email.
- Obtain secure storage programs to archive sensitive, private data, and documents instead of storing emails.
- Create separate email accounts specifically for financial transactions.
- Delete all emails that include financial information.
- Cautiously evaluate the risk versus convenience of transferring confidential information by email.

DON'T

- Do not click on the links or pop-up ads in unsolicited emails, as these links may pass on viruses.

KEEP EQUIPMENT UP TO DATE

DO

- Install the most up-to-date antivirus and anti-spyware software on all devices that connect to the Internet (e.g., PCs, laptops, tablets, smartphones)
- Set each device to run regular scans to update software.
- Ensure you've installed the latest versions of your software and your patches are up to date.
- Make sure your networking equipment and computers are all still supported by the manufacturer.
- Recycle, exchange, or dispose of your old mobile device safely by:
    - backing up your data,
    - performing a secure erase (factory reset) or have the device vendor wipe your device,
    - removing SIM and SD cards from your cell phone – transfer to new phone or destroy.

DON'T

- Don't purchase any networking devices secondhand.
- Forget to set up a passcode or PIN and auto-lock on your mobile devices.
- Use free or found USB drives, as they typically are infected with malware.

RESOURCES

RESOURCES

INDUSTRY RESOURCES

- Go to StaySafeOnline.org and review the STOP. THINK. CONNECT.™ cybersecurity educational campaign
- Visit OnGuardOnline.gov, also a part of the STOP.THINK. CONNECT.™ campaign, that focuses on online security for kids and includes a blog on current cyber trends
- Visit https://www.fbi.gov/scams-safety/fraud to learn more about common fraud schemes

TO REPORT A CYBERCRIME

- Forward suspicious emails to: nophishing@cbbb.bbb.org
- Visit www.identitytheft.gov to report identity theft and to get a recovery plan
- Go to FTC.gov for additional consumer resources and to report identity theft
- http://www.ic3.gov/default.aspx is another website where you can file cybercrime complaints