HOW TO PROTECT YOURSELF FROM CYBER ATTACKS

CYBERSECURITY

CYBERSECURITY

NO ONE (INDIVIDUALS, BUSINESSES OR COUNTRIES) IS IMMUNE FROM CYBER ATTACKS.

- U.S. election process (under investigation)
- Internal Revenue Service
- FDIC
- Google
- JP Morgan Chase
- Wendy’s
- LinkedIn

SOME NOTABLE HACKS, CYBERATTACKS, AND DATA BREACHES OF 2018

- Saks, Lord & Taylor (5 million)
- PumpUp (6 million)
- The Sacramento Bee (19.5 million)
- Ticketfly (27 million)
- Panera (37 million)
- Facebook (87 million
- MyHeritage (92 million)
- Under Armour (150 million)

WHAT IS CYBERSECURITY?

- Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

-Merriam-Webster

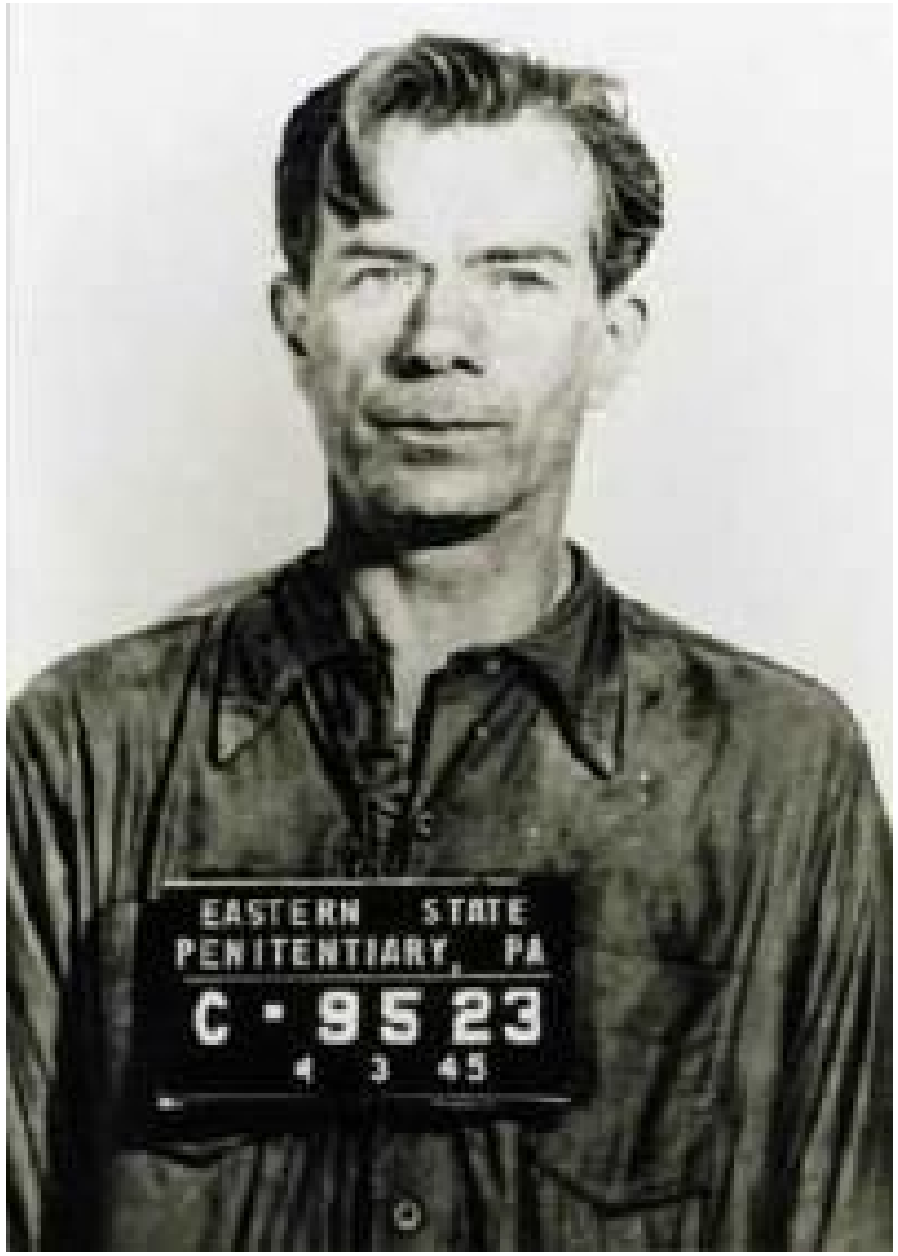
CYBERSECURITY DENIAL

"Hackers aren't going to waste their time with me. I don't have the kind of funds that these large corporations have."

"This will not happen to me."

It's not a matter of if you will be a victim of cybercrime. It's more a matter of when.

"…Law firms and their trove of sensitive data are prime [emphasis added] targets for hackers…"
How to be Sure You're Cybersecure, Finkel; *Illinois Bar Journal*, Vol. 106, February 2018


EASTERN STATE
PENITENTIARY, PA
C-9523
4 3 45

A **cyber attack** is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

WHAT IS A CYBER ATTACK?

TYPES OF FRAUD AND CYBER THREATS

- Wire Fraud
- Check Fraud
- E-mail Compromise
- Malware/Virus
- Spoofing
- Social Engineering & Phishing
- Ransomware & Scareware
- Identity Theft
- Denial of Service Attack

WIRE FRAUD

THE BAD GUYS WILL FOLLOW THE MONEY

- ALTA, May 9, 2017: *Title Companies Report 480% Increase in Wire Fraud Attacks*.
- Monitor transactions from beginning to end.
- Cash transactions
- Transactions below “thresholds.”

CHECK FRAUD

- Check fraud can be committed by your employees, as well as by individuals outside your office.
- Social Media sites have helped facilitate this form of fraud.
  - Craigslist
  - Facebook
  - Twitter
  - Job Websites

MALWARE

- Viruses
- Spyware
- Ransomware

E-MAIL COMPROMISE

BUSINESS E-MAIL COMPROMISE (BEC): A sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

E-MAIL ACCOUNT COMPROMISE (EAC) component of BEC targets individuals who perform wire transfer payments.

- This scam continues to grow, evolve, and target small, medium, and large businesses.
- E-filing & e-mail service increase the importance of e-mail security.

THEFT

The bad guys are primarily after money, but they will gladly steal:

- Personal information (yours and your client's)
- Employee personal information
- Trade secrets or other proprietary information
- Client lists

E-MAIL SPOOFING

- Senders misrepresent themselves by pretending to be the “intended” or “familiar party” to obtain unauthorized access to a targeted system.
- E-mail spoofing is extremely common and simple to complete.
  - randomperson@gmail.com
  - randomparson@gmail.com

SOCIAL ENGINEERING & PHISHING

- Phishing sender attempts to trick individuals (typically employees) into handing over sensitive information.
- The fraudster often acts under the guise of an actual business, client, or vendor.

William W. Austin

From: American Express <AmericanExpress@ampress.com>
Sent: Friday, April 27, 2018 10:17 AM
To: americanexpress@ampress.com
Subject: Important Notice: Card Information Message.
Attachments: AXPNSUYS00180426200.htm

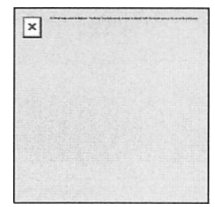
Primary Cardmember Message

For your security:

We are writing to let you know that there is a recent security report cardmember: for your American Express(R) Account(s). At time of report diligency, 'yanpmcioughim@abbey.bac.edu We ran into problem validating your profile.

In view of this, Your profile needs to be to undergo an accuracy check and your mandatory effort is required.

YOU ARE TO



A safe attached tillable Web form is sent with this message.

• See Attached Information Form, Download and Open to Continue.

• Get started by filling all steps required onthe form.

Thank you for your continued Cardmembership.

American Express Customer Service

RANSOMWARE

The holding hostage of computers or data in exchange for money. Cybercriminals take control of network data, which is then encrypted and held for ransom.

Ransomware is projected to be the biggest cyber threat in the near future.

- Wannacry
- NotPetya
- SamSam
- TeslaCrypt
- SimpleLocker
- Ryuk

BEWARE OF SCAREWARE

An increase in Scareware is predicted.

Difference between Ransomware & Scareware?

Ransomware is the holding hostage of computers or data in exchange for money.

Scareware creates the perception of a threat, to induce the user into paying for and/or downloading unnecessary, unwanted, or infected software.

DENIAL OF SERVICE

This attack essentially shuts down the network connectivity, as well as additional services or functions that may be provided.

HOW TO PROTECT AGAINST WIRE & CHECK FRAUD?

- Staff training
- Background checks
- Minimize acceptance & retention of trust funds
- Reconcile bank accounts
- Obtain cybercrime insurance coverage
- Protect wiring instructions
  - Inform clients of risks
  - Confirm wiring instructions.
  - Use a private domain (jsmith@smithlaw.com, not jsmith@gmail.com)
  - Encrypt e-mail communications

HOW TO PROTECT AGAINST E-MAIL COMPROMISE?

- Identify valuable data.
- Use a private domain (jsmith@smithlaw.com, not jsmith@gmail.com)
- Change passwords

PASSWORD POLICY BEST PRACTICES

KEEP YOUR PASSWORDS STRONG

- Use a minimum of 10 symbols, including numbers, both uppercase and lowercase letters, and special symbols.
- Even better, use passphrases consisting of a minimum of 15 symbols using letters and numbers.

PASSWORD POLICY BEST PRACTICES (CONT.)

AVOID COMMON PASSWORD WEAKNESSES

- Easy-to-guess passwords, especially "password"
- Your name, the name of your spouse or partner name, or other names
- A string of numbers or letters like “1234” or “abcd”, or simple patterns of letters on the keyboard, like “asdfg”
- Your phone number or your license plate number, anybody’s birth date, or other information easily obtained about you (*e.g.*, your address, town or alma mater)
- Passwords of all the same letter
- Words that can be found in the dictionary
- Default passwords, even if they seem strong
- Any of the above followed or preceded by a single digit

PASSWORD POLICY BEST PRACTICES (CONT.)

PROTECT YOUR PASSWORD

- It is vital to remember your password without writing it down somewhere, so choose a strong password or passphrase that you will easily remember. If you have a lot of passwords, you can use password management tools, but you must choose a strong master key and remember it.
- Be aware of how passwords are sent securely across the Internet. URLs (web addresses) that begin with “https://” rather than “http://” are more likely to be secure for use of your password.
- If you suspect that someone else may know your current password, change it immediately.
- Change your password periodically (every 90 days for a strong password, every 180 days for a passphrase), even if it hasn't been compromised.
- Don't type your password while anyone is watching.
- Avoid using the same password for multiple websites containing sensitive information.

PASSWORD POLICY BEST PRACTICES (CONT.)

PASSWORD POLICY BEST PRACTICES FOR SYSTEM ADMINISTRATORS

- Configure a minimum password length of at least 10 characters for passwords or 15 for passphrases.
- Enforce password history, with at least 10 previous passwords remembered.
- Set a minimum password age of 3 days.
- Set a maximum password age of 90 days for passwords and 180 days for passphrases.
- Enable the setting that requires passwords to meet complexity requirements. This setting can be disabled for passphrases but it is not recommended.

PASSWORD POLICY BEST PRACTICES (CONT.)

PASSWORD POLICY BEST PRACTICES FOR SYSTEM ADMINISTRATORS (cont.)

- Reset local admin passwords every 180 days.
- Reset service accounts passwords once a year during maintenance.
- For domain admin accounts, use strong passphrases with a minimum of 15 characters.
- Track all password changes by enabling password audit policies.
- Create email notifications for password expiration.

COMPUTER & NETWORK SAFEGUARDS

ANTIVIRUS RESOURCES:

- McAfee Antivirus Plus
- Symantec Norton Antivirus Basic
- Bitdefender Antivirus Plus
- Webroot SecureAnywhere Antivirus
- Kaspersky Antivirus*

COMPUTER & NETWORK SAFEGUARDS (cont.)

Anti-Malware:

- Bitdefender Total Security
- McAfee Total Protection
- Symantec Norton 360 with LifeLock Select
- Malwarebytes Free
- Microsoft Windows Defender

Firewalls

Use current editions!

Run updates!

WHAT TO DO IF YOU ARE A VICTIM?

- Don’t panic
- Identify the infected computer and take it offline.
- Notify your client(s), and other affected parties, if any (*e.g.*, bank)
- Notify law enforcement
- Report to the Internet Crime Complaint Center (IC3) (www.ic3.gov)
- Change passwords & settings
- Consult with your IT service provider

KNOW THE RISK RAISE YOUR SHIELD*

TRAVELING OVERSEAS WITH MOBILE PHONES, LAPTOPS, PDA'S & OTHER ELECTRONIC DEVICES

- Strengthen your passwords.
- Lock down your social media accounts.
- Delete suspicious emails
- Don't expect privacy when you travel
- Know who you're talking to

If you can do without the device, don't take it.

*The National Counterintelligence & Security Center (NCSC) Awareness Campaign

SOME ETHICAL ISSUES

- RULE 1.1: COMPETENCE
- RULE 1.3: DILIGENCE
- RULE 1.6: CONFIDENTIALITY OF INFORMATION
- RULE 5.1: RESPONSIBILITIES OF PARTNERS, MANAGERS, AND SUPERVISORY LAWYERS
- RULE 5.3: RESPONSIBILITIES REGARDING NONLAWYER ASSISTANT

WONDERING IF YOU'VE BEEN IMPACTED?

- Take a look at some of the biggest recent data dumps.
- Pay a regular visit to the *Have I Been Pwned?** https://haveibeenpwned.com/website to make sure:
  - that an attack on a website that you frequent; or
  - a website that you once frequented;

  hasn't occurred.

*Check to see if you have an account that has been compromised in a data breach.

ADDITIONAL WEBSITES & OTHER RESOURCES

- www.identitytheft.gov
- www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield
- www.ftc.gov/news-events/audio-video/video/data-breach-response
- www.dhs.gov/topic/cybersecurity
- How to be Sure You're Cybersecure, Finkel; *Illinois Bar Journal*, Vol. 106, February 2018
- The High Price of Free Email, Draper; *Illinois Bar Journal*, Vol. 106, April 2018
- www.isba.org/practicehq/protect
- How Secure Are You? Cybersecurity for the Illinois Practitioner; ISBA LawEd