



2019 Information Security Nuts & Bolts: Why does it matter to me?

Developed by :

Chris Wisneski

Whittlesey Technology



Whittlesey
Forward Advising™



Today's Presenters



Chris Wisneski

Manager, IT Security and Assurance Services
Whittlesey Technology

cwisneski@WAdvising.com
860.524.4434

- Over 20 years of technology and leadership experience
- Areas of expertise include IT audit, SOC 1 and 2 audits, Cybersecurity, Risk Assessments, IT General Controls, Information Security, Networks, Regulatory Compliance, FDICIA and SMB



Agenda

▶ Massachusetts Data Privacy Act

▶ HIPAA

▶ Social Engineering

- Emerging trends
- How to protect ourselves

▶ Cybersecurity Best Practices

- Password Complexity
- Public WiFi hotspots
- Mobile Device Security



Massachusetts Data Privacy Act



Massachusetts Data Privacy Act

▶ Massachusetts Data Privacy Act (MA - 201 CMR 17.00)

- In effect on March 1, 2010
 - Revised and Effective April 11, 2019
- Who does it apply to?
- Defines Personally Identifiable Information (PII)
 - Social Security Number
 - Driver's License Number
 - State Identification Card Number
 - Financial Account Number, credit or debit card number
- Assesses stiff fines to companies that are breached and subsequently don't comply with the law



Massachusetts Data Privacy Act

▶ Massachusetts Data Privacy Act Requirements

- Written Information Security Program (WISP)
- Designating one or more employees to maintain the program (such as a Privacy Officer)
- Vendor Management Program
- Incident Response Plan
- Security Awareness Program
- Breach reporting within 90-days of finding breach

What Can't You Do?





HIPAA



HIPPA

▶ Health Insurance Portability and Accountability Act (HIPAA)

- Established in 1996
 - Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs
 - Reduces health care fraud and abuse
 - Mandates industry-wide standards for health care information on electronic billing and other processes
 - Requires the protection and confidential handling of protected health information.

The Office of Inspector General recovered over \$3.7 billion in settlements and judgments, \$2.4 billion involved the health care industry, including drug companies, hospitals, pharmacies, laboratories, and physicians.

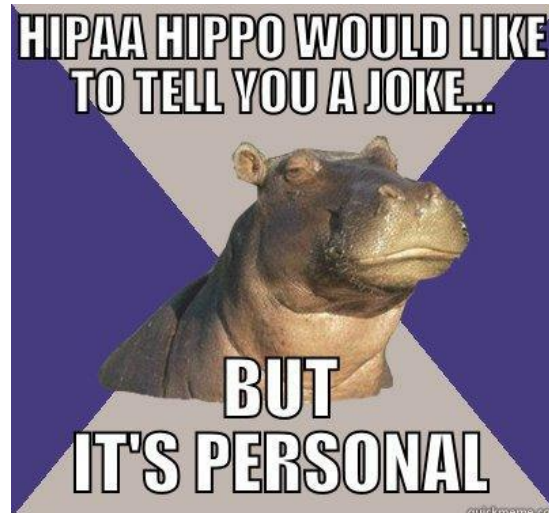
HIPPA

▶ HIPAA Privacy Rule

- The purpose of the Privacy Rule is to establish minimum Federal standards for safeguarding the privacy of individually identifiable health information. Covered entities, which must comply with the Rule, are health plans, health care clearinghouses, and certain health care providers

▶ HIPAA Security Rule

- Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity





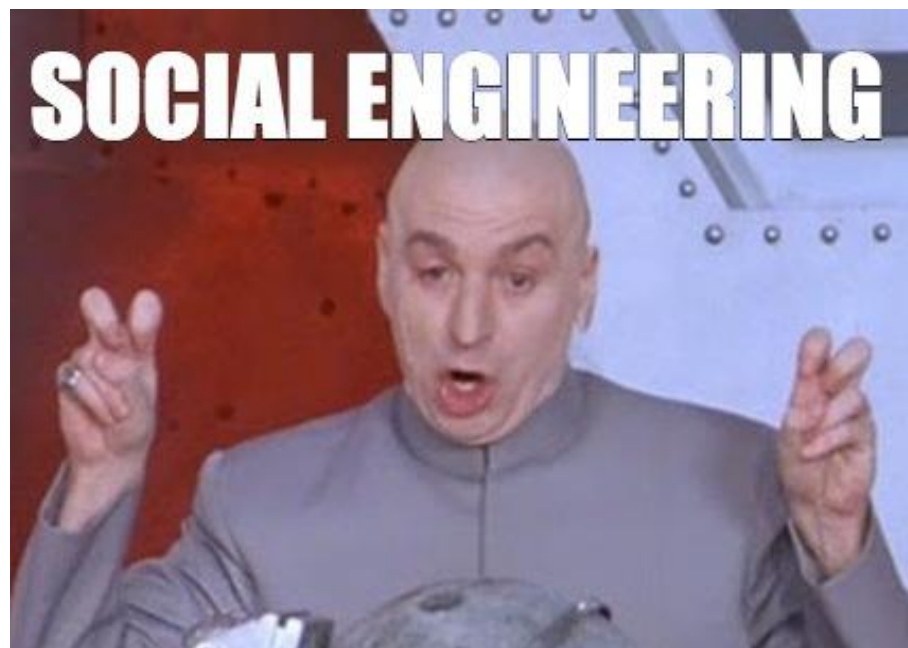
HIPPA Security Rule

▶ HIPAA Security Rule Requirements

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce
- Entities must perform risk analysis as part of their security management processes
- Workstation and Device Security
- Facility Access and Control

In 2018, the Annual Cost of a Data Breach Study by the Ponemon Institute/IBM Security revealed that the average cost of of a HIPAA-related data breach costs over \$3.86 million – an annual increase of 6.4%

Social Engineering





What are Social Engineering Attacks?

▶ Remote

- **Phishing Emails** - email that attempts to trick you into clicking on a link, opening an attachment, or giving up your credentials
- **Vishing Phone Calls** - phone call that from someone impersonating a client or vendor to obtain confidential information

▶ On-site

- **Baiting** – enticing users to plug in infected media like USB drives, CD-ROMs, etc
- **Social Engineering for physical access** – gaining physical access to restricted areas by taking advantage of trusting employees
 - Tailgating
 - Impersonation

Detecting and Avoiding Phishing Attacks

- ▶ Check the sender address for misspellings
- ▶ Take notice of inconsistent language or strange formatting
- ▶ Manually review email header information for clues
- ▶ Call to confirm






Misspelled Sender Addresses

From: security@microsoft.com

Reply-to: security@microsoft.com

 [Send me a test email](#)

Subject: De-activation of [REDACTED] in Process

Microsoft Office 365 Email

Hello [REDACTED]

Confirm Your Email



Your incoming messages are queued and pending delivery on your account [REDACTED]
We require you to confirm your account with a security challenge to protect your account.

[Confirm account](#)

Thanks,
The Microsoft Office 365 account team

This email is for [REDACTED]
Powered by Microsoft Office 365



Strange Formatting or Inconsistent Language

From: [REDACTED]
Sent: Friday, December 07, 2018 2:38 PM
To: [REDACTED]
Subject: Please pull invoice 503745

Good Day all,

Please see attached invoices per your request.

Thank you and have a wonderful day!

[REDACTED]
1800-659-7393 (ext.0453)
[REDACTED]

[REDACTED]
Administrative Coordinator
[REDACTED]
[REDACTED]



Detecting and Avoiding Vishing Attacks

- ▶ Check the originating phone number
- ▶ Be wary of automated calls
- ▶ Call back confirmation
- ▶ NEVER give out confidential information unless you're absolutely sure of who you are talking to

Spam calls rose over 22% in the last 12 months

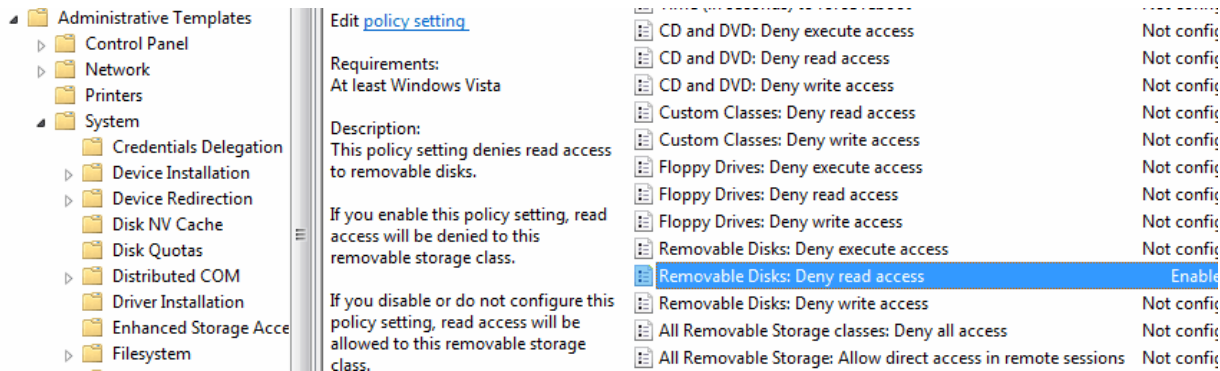
On average, Americans reported receiving 23 spam calls (mobile and/or landline) in the last 12 months

1 in every 10 American adults (10%) lost money from a phone scam in the past 12 months with nearly half (46%) of those who have ever been scammed reporting they've been a victim more than once

With an average loss of \$357 per victim, the result of these scams is projected to have cost 24.9 million Americans approximately \$8.9 billion in total losses.*

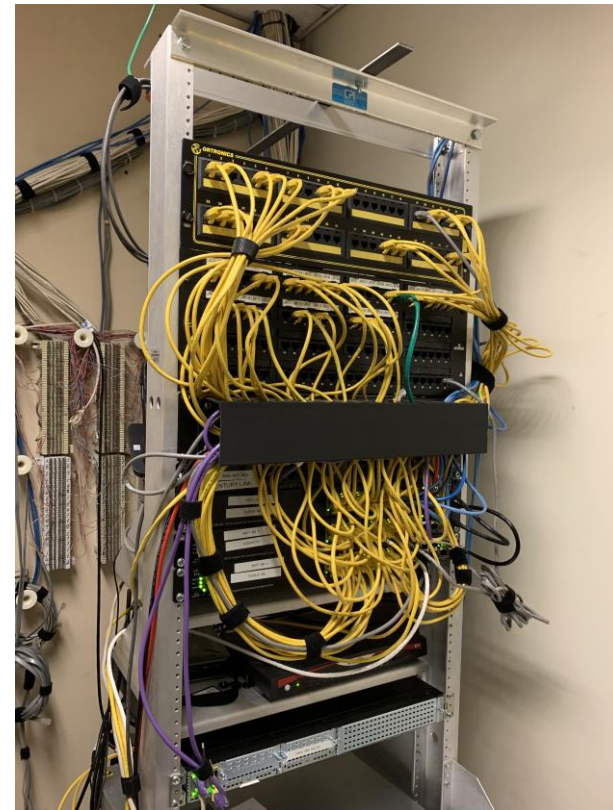
Detecting and Avoiding Baiting Attacks

- ▶ Never plug in unknown devices into your network
 - Create written policy within WISP
- ▶ Ensure antivirus is up-to-date to prevent malware from executing
- ▶ Use software to restrict reading of portable drives by workstations on the corporate network
 - Through third party security software
 - Through Group Policy



Detecting and Avoiding Physical Social Engineering Attacks

- ▶ Have a sign-in process
- ▶ Use guest badges
- ▶ Check credentials of people you don't know
- ▶ Escort visitors





Cybersecurity Best Practices

Public WiFi

▶ Am I Safe?

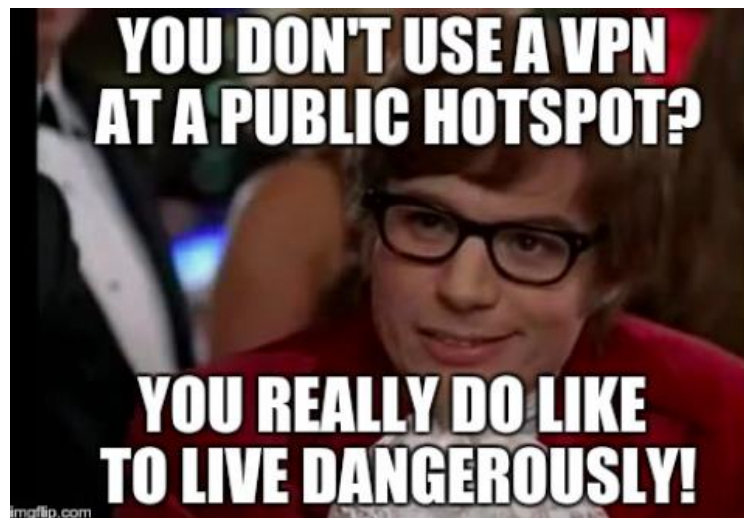
- Phony rogue networks set up specifically by cyber criminals
- Man-in-the-middle attacks where hackers commandeer a public WiFi network and redirect users, often to a phony login site where their credentials are stolen
- Wireless sniffer tools that locate unsecured public WiFi networks, analyze their packets, and steal data, monitor network activity, or gather intel for use in a future attack against the enterprise's network
- Having your device infected by a worm on another user's device that travels through the public WiFi network



Public WiFi

▶ How Can I Protect Myself?

- Use a Virtual Private Network (VPN)
 - Hotspot Shield or NordVPN
- Use Secure Connections
 - Configure browser to 'always uses HTTPS' connections
- Don't Access Anything Sensitive
- Turn Off Automatic Connectivity
- Turn Off Bluetooth
- Turn off airdrop and file sharing




Mobile Device Security

Why Do I Care?

- Android platform has over 300,000 vulnerabilities
- iOS (Apple) has approximately 1651
- Trend Micro reported that it had over 235,000 detections for ransomware targeted at Android platforms in April of 2017


About 251,000,000 results (0.78 seconds)

Videos




Hacking a mobile phone

SPH Razor
YouTube - Jul 26, 2013



How To Hack a Mobile Phone 2019 (100% Working) #HowToHack

HowToHack
YouTube - Dec 10, 2016



How To Hack Someone's Mobile Phone/sms/phone calls/whatsaap all ...

Paul Hacker
YouTube - Oct 31, 2015

[How to hack a cell phone - Phone Hacker App Real-Time - TheTruthSpy](#)

thetruthspy.com/hack-cell-phone/

★★★★★ Rating: 4.6 - 133 votes

May 24, 2018 - How to hack a cell phone - Phone Hacker App Real-Time. With the right spy tool you can hack a phone, and you can monitor your spouse or ...

[How to hack a Android Phones](#) [Instagram hack](#) [SMS Hack](#) [iPhone Hack](#)

[Cell Phone Hacking | Mobile Device Hacking | Phone Hackers](#)

<https://cryptohackers.com/hackers-for-hire/cell-phone-hacking/>

Cell Phone Hacking and phone hacking is one of the services provided by Cryptohackers we specialize in hacking iPhones, Androids and many mobile devices.

[Hire An Hacker - #1 Best place to Hire Hackers](#)

<https://hireanhacker.com/>

Smart Phone Hacking. Full device access. Now a days mobiles have became part of our bodies, It does have all the sensitive information, We will inject a ...

[Android Hacking Apps - Become a True Hacker - cell phone tracking app](#)

<https://celltrackingapps.com> [Question and answers](#)

Aug 6, 2018 - Android hacking apps - What mobile spyware for? How to install/ use android hacking

Mobile Device Security

▶ How Can I Protect Myself?

- Regularly Update the Operating System and Apps
- Use Relevant Built-in Security Features
 - Find My iPhone or Find My Device (Android or Google)
 - Built in Encryption
- Use Strong Passwords or Biometrics
- Install an Antivirus Application
- Avoid Turning On AutoFill on your device
- Utilize a Mobile Device Management (MDM) solution



New NIST Password Standards

► What is NIST?

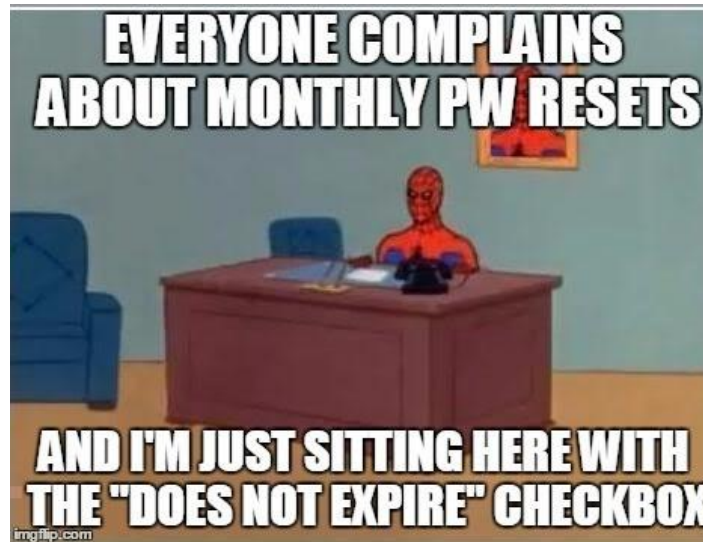
- National Institute of Standards and Technology
- Cybersecurity Framework Version 1.1 (April 16, 2018)
- Framework for security standards for large and small companies and organizations across all industry sectors, as well as by federal, state and local governments



New NIST Password Standards

► Wait for it...wait for it...

- 12 character minimum length
- Passphrases are encouraged
 - For example, 'elatedraccoon' or 'dogsandcatsplay'
- Allow complexity, but not required*
- Abolishing password expirations altogether?



Password Strength Statistics

HOW LONG SHOULD YOUR PASSWORD BE?

Amount of Time to Crack Passwords

"abcdefg" 7 characters  .29 milliseconds

"abcdefgh" 8 characters  5 hours

"abcdefghi" 9 characters  5 days

"abcdefghij" 10 characters  4 months

"abcdefghijk" 11 characters  1 decade

"abcdefghijkl" 12 characters  2 centuries

 Better Buys



Wrap Up

*Remember to treat your password like a toothbrush –
choose a good one and don't share it with anyone else!*

Questions?



ASSURANCE | ADVISORY | TAX | TECHNOLOGY

Headquarters

280 Trumbull Street, 24th Floor
Hartford, CT 06103
860.522.3111

One Hamden Center
2319 Whitney Avenue, Suite 2A
Hamden, CT 06518
203.397.2525

14 Bobala Road, 3rd floor
Holyoke, MA 01040
413.536.3970

WAdvising.com