PERSONAL CYBERSECURITY 2020

MARV WASCHKE

CHRIS WASCHKE

2/1/20

INTRODUCTION TO MARV AND CHRIS

- Marv Waschke
  - Wrote my first computer program in 1967
  - Developed enterprise network and service management software
  - Divisional VP for Software Development and Senior Principal Software Architect for Fortune 500 software development house
  - Three books on cloud computing and security
- Chris Waschke
  - Digital Native
  - Studying for Linux System Administration Certificate

STATE OF CYBERSECURITY 2020

THE GOOD

- The computing industry is taking security seriously
  - Computing IS more secure
  - Best reports: vulnerability discovery rate flattening
  - Bug bounty programs thriving
  - Chip makers are designing in security at lowest level

THE BAD

- Hacking culture is vigorous
- More sophisticated “master hackers”
- Hacking kits for “script kiddies” readily available
- Hacking services and utilities readily available on “dark net”
- The “Dark Net” offers ready markets for stolen data

INTERNATIONAL

- Border security does not stop hacking
  - Business likes connectivity
  - The Internet was designed to cross borders
  - Examples where network traffic in Germany was routed through China for a few hours
- Offshore hacking
  - Little advance in anti-hacking treaties
  - Extradition is stagnating – no new extradition treaties

THE INTERNET OF THINGS - IOT

- Network connected devices – Industrial, Home
- Becoming more uniform = easier to hack
  - Hackable PCs on chips replace more secure custom controllers
  - Standard network connection
- Hard to keep updated – Disconnected white box third parties
- Hard to avoid -- find a new car that's disconnected…

THE WORST - INDUSTRIAL HACKING ON THE RISE

- Hacks that blow up oil refineries
- Power grids disrupted in Ukraine
- Insecure Supervisory Control and Data Acquisition (SCADA)
- Many industries lack cybersecurity– just lock control room
- Penetrable "air gapped" systems

GOVERNMENT - CYBERWAR IS REAL

- North Korea funds missile program by hacking inter-bank transfers and crypto-currencies -- $2B estimated
- US and Israel hacked Iranian nuclear centrifuges a decade ago
- Russia interfered in the US presidential election
- China exfiltrates intellectual property
- Cyber retaliation is most likely response from Iran

PROTECT YOURSELF

BASIC COMPUTER HYGIENE

- Beware of “phishing” and social engineering
- Use strong passwords
- Run anti-malware scans frequently
- Keep your operating system and apps up-to-date
- Download and install with caution
- Avoid dodgy sites

WHY AREN'T BACKUPS ON THIS LIST?

- Backups save your bacon after you are hacked, but they don't decrease the likelihood that you will be hacked
- I've given up on telling people to backup. I can't scold you into it
- By all means, backup your computer
- Regular backup are easy with cloud and modern operating systems
  - Backup to a cloud and to a local device (external drive, big thumb drive, etc.)
  - Create a system recovery disk

Beware of “phishing” and social engineering

TRICKERY!

SOCIAL ENGINEERING

- Most hacks begin with “social engineering”
  - Never blindly assume a pop-up, email, or phone call from Microsoft, the IRS, law enforcement, your bank, or your boss is legit
  - Your first reaction may be fear. Take a deep breath. Don’t be intimidated. Most likely, you have nothing to fear
  - Legitimate sources are glad to be contacted through publicly known channels

PHISHING SELF-PROTECTION

- Legitimate businesses, including Microsoft, will not contact you about a support problem. You must initiate the conversation
- Legitimate vendors will not ask for passwords or to install remote access software
- Ignore unsolicited calls, emails or other contacts even if they have detailed information about your system and issues
- If you have reason to deal with Microsoft, be sure it is Microsoft

STRONG PASSWORDS

- You will be hit by a password list heist sooner or later
  - Mozilla will help you find out
- Password cracking systems test the 10,000 most common passwords in seconds. Choose a password that is not in the "rainbow table."

PASSWORD RULES

- *NEVER* use duplicate passwords. The worst breaches grew from duplicate passwords.
  - Do not use duplicate passwords on trivial accounts
  - Trivial accounts can validate significant transactions
- National Institute of Standards (NIST) no longer recommends scheduled forced password changes. Change when you're warned of a breach.

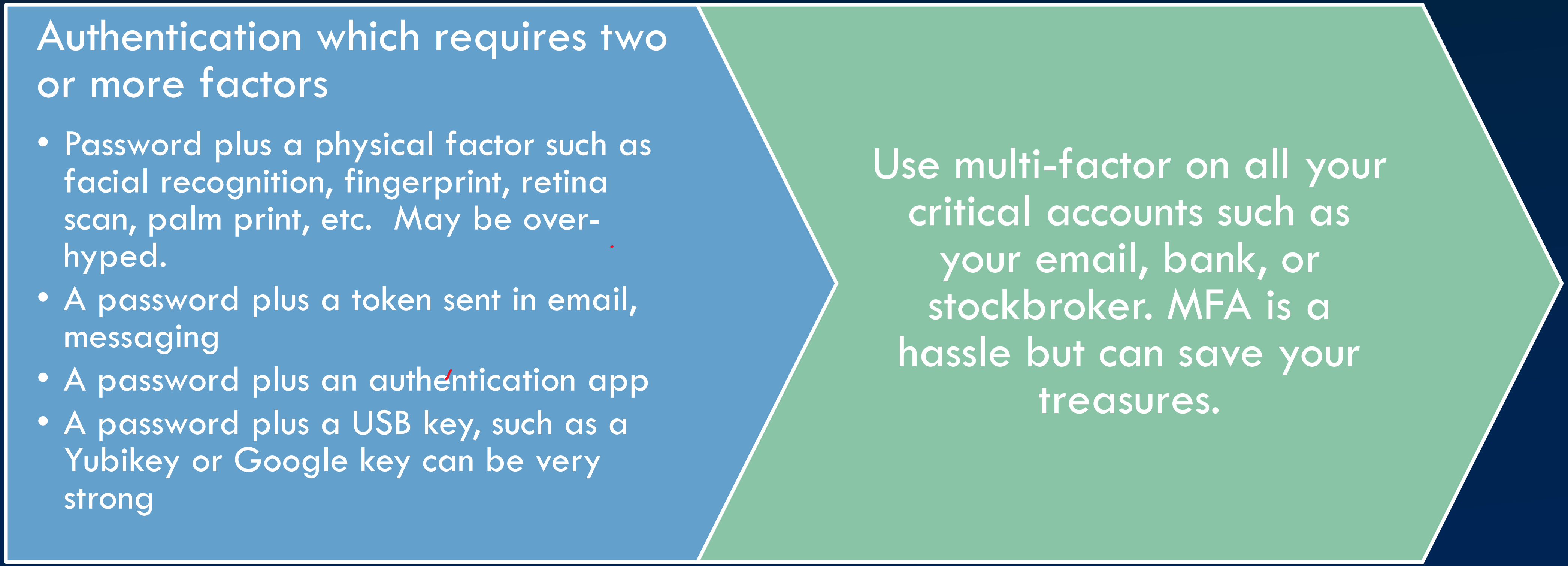
CHOOSE A STRONG PASSWORD

- Long random sequences best
- Not on the rainbow list. (What's common? Any word in any dictionary. Any common phrase. Google it.)
- Long. (Over 16 characters is almost impossible to crack)
- Large character set (letters, numbers, symbols)
- Don't use a short password substituting symbols (pA55w0rd). Used to be good, but fast cracking machines crush them

PASSWORD MANAGERS

- Generated long random passwords are the hardest cracks
- Managers make avoiding password reuse easy
- Manager's database likely is safer than home storage
- A paper system is still safer-- *IF* you can maintain it

MULTI-FACTOR AUTHENTICATION IS YOUR FRIEND



Authentication which requires two or more factors

- Password plus a physical factor such as facial recognition, fingerprint, retina scan, palm print, etc. May be over-hyped.
- A password plus a token sent in email, messaging
- A password plus an authentication app
- A password plus a USB key, such as a Yubikey or Google key can be very strong

Use multi-factor on all your critical accounts such as your email, bank, or stockbroker. MFA is a hassle but can save your treasures.

MULTIFACTOR CONSIDERATIONS

- Mobile phone messaging (SMS) is weak form– cellphone stores are a weak link
- Email is stronger, if you keep your email secure
- Multifactor systems (like Google's) that raise an announcement on your phone are safer than SMS or email
- Multifactor apps are stronger yet
- Multifactor physical keys are currently the strongest. Consider putting a spare key in a safe deposit box

Run anti-malware scans frequently

ANTI-MALWARE – ANTI-VIRUS

- Not all nasty stuff is a virus
- New vulnerabilities appear daily. Keep up to date
- Run scans regularly (once a day, minimum)
- Apple is not inherently safe
- Regular scans and updates are more important than brand

HOW TO CHOOSE AN ANTI-MALWARE TOOL

- An anti-malware tool that you don’t use is worthless— Convenience matters
- The market is hyper-competitive— the products are revised continually
- On Windows, Microsoft’s anti-malware tool is convenient and adequate
- Unix based systems (Apple, Linux) are architecturally safer, but they are hackable
- Apple, hacked much more frequently now, recommend using anti-malware
- Linux, still under the personal hacking radar
- Malware Bytes is a useful tool for cleaning infected machines
- Anti-malware tools have been accused of selling your privacy (Avast)

Keep your operating systems and apps updated

USE AUTOMATIC UPDATE

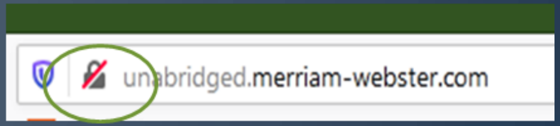
- New vulnerabilities are discovered every day. OS and app vendors continually patch the cracks, but they have to be able to update.
- A patched system is much stronger defense than a scan that finds a hack and removes it– you may have already been compromised when the scan runs.
- Running non-supported OS s and apps invites attack. Outdated systems are low-hanging hacker fruit. If you can’t afford to keep your system updated, switch to Linux. It’s free.

DOWNLOADING AND INSTALLING

- Never install anything from an insecure site
- Get your drivers from OS and hardware vendors, not 3rd party sites
- The Microsoft, Apple, and Google stores vet their content. Use them, but realize they are not perfect
- Beware of ***free*** USB sticks

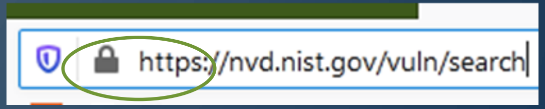
IDENTIFY SECURE WEBSITES

Insecure



unabridged.merriam-webster.com

Secure

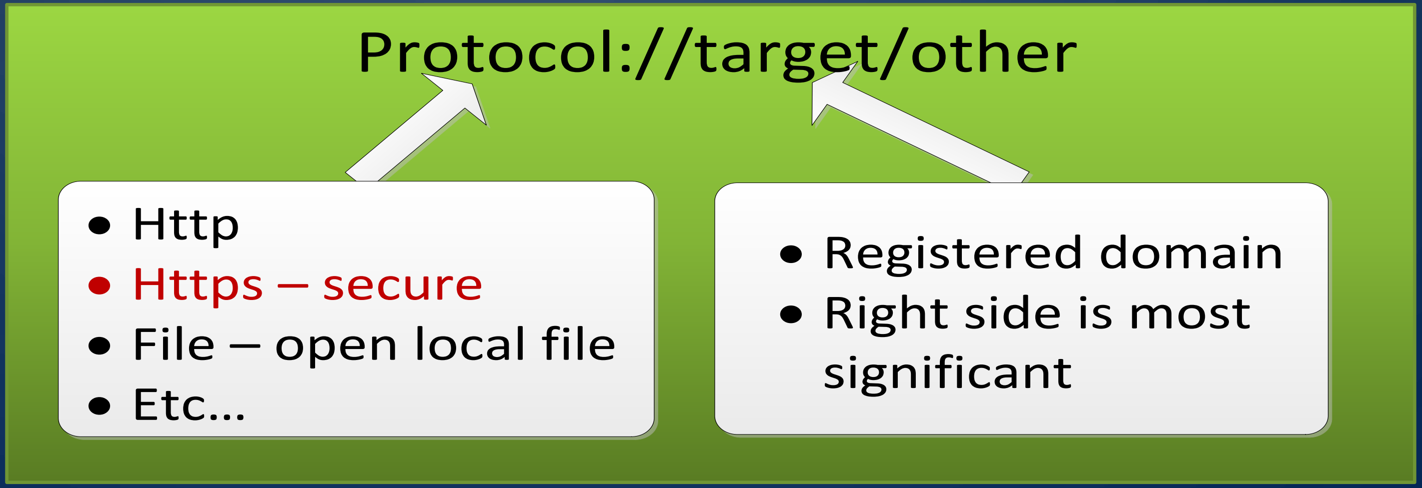


https://nvd.nist.gov/vuln/search

- HTTP v. HTTPS
- Secure
  - Assurance that the site you connect to is the site you intended
  - Your data on the network is encrypted
- If you get a “certificates” message when you connect to a site, be cautious
- Most sites are now secure (Google started avoiding insecure sites)
- Put a password on your home wireless (also on your router)

URL MINI-TUTORIAL

- URLs are the addresses that connect the Internet
- URLs are case insensitive
- The registered domain between "//" and "/" is the site address
- Domains names are in hierarchies from right to left
  - http://www.Microsoft.com addresses Microsoft in the .com (commercial) family and Microsoft's area "www" (World Wide Web)
- The text after the "/" addresses specific pages and search patterns



Protocol://target/other

- Http
- Https – secure
- File – open local file
- Etc…

- Registered domain
- Right side is most significant

URLS

- "Microsoft.com" directs messages to Microsoft
- "Microsoft.com.thugs.lv" directs message to thugs.lv in Latvia, ***not*** Microsoft
- .com, .net, .edu, .gov addresses are a little harder for criminals to get, beware unexpected extensions like .bid
- Criminal sites use domain names like xxrqzz.bid

Avoid dodgy sites

STAY OUT OF DARK ALLEYS
IN BAD NEIGHBORHOODS

IOT SAFETY

- Research before you buy
- Does the device support automatic update?
- Can you set the password for administering the device?
  - ALWAYS change the default password
- IoT devices increase importance of securing your home Wi-Fi
  - Both the network and router

IF YOU ARE HACKED…

- If you think a hacker is in your computer
  - Power down
  - Disconnect your Wi-Fi router
- Get help from an expert
  - Restart with caution, run malware scan before reconnecting to network, then again after update
- Check your credit card bill and call your bank– you are not liable for false charges if you inform your bank soon enough.
  - Credit cards are a little safer than debit cards
- Freeze your credit with the credit bureaus (Equifax, Experian, TransUnion, Innovis)
- Change your passwords

FOR FURTHER INFORMATION

Chris and Marv are at the Ferndale Public Library from 3-4p, first and third Wednesdays, September through May

Visit https://MarvinWaschke.com for periodic blog posts on security and privacy

My book, Personal Cybersecurity, is available through WCLS and for purchase on Amazon

RESOURCES

- Phishing
  - Details on Microsoft December 2019 data breach https://www.computerweekly.com/news/252477154/Internal-error-left-Microsoft-customer-service-data-exposed
  - Microsoft Support Suppliers https://www.microsoft.com/en-us/professionalservices/suppliers
- Password theft
  - https://monitor.firefox.com/breaches/
  - https://haveibeenpwned.com/
- Common password list
  - https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords
- Password managers
  - https://www.tomsguide.com/us/best-password-managers,review-3785.html
  - https://www.cnet.com/news/best-password-managers-for-2020

RESOURCES - 2

- Multi-factor
  - Multifactor apps https://www.pcworld.com/article/3225913/what-is-two-factor-authentication-and-which-2fa-apps-are-best.html
  - YubiKey https://www.yubico.com/
  - Google Titan Security Key https://store.google.com/us/product/titan_security_key_kit
- Anti malware
  - Windows: https://www.pcmag.com/picks/the-best-malware-removal-and-protection-software
  - Apple: https://www.techradar.com/best/best-mac-antivirus-software
  - Linux: https://www.tecmint.com/best-antivirus-programs-for-linux
- Vulnerabilities
  - Search NIST/DHS National Vulnerability Database: https://nvd.nist.gov/vuln/search

QUESTIONS?

SUPPLEMENTARY SLIDES

THE UNDER ARMOUR PASSWORD HEIST

- May, 2018, Under Armour Inc. announced that 150 million accounts from a subsidiary were exfiltrated in February, warning users to change their passwords
- Usernames, email addresses, and hashed passwords were taken
- The thieves decrypted the passwords at their leisure
- The decrypted passwords used to break into other accounts

MICROSOFT DATA BREACH

- Microsoft database servers containing customer support conversations were mistakenly exposed for about 3 weeks in December 2019
- When the exposure was discovered, Microsoft quickly fixed it
- Whether the data was exfiltrated (stollen) is unknown
- Phishing attempts may have detailed information on problems discussed with Microsoft between 2005 and 2019

PHISHING — DECEPTIVE EMAILS

(C) MARVIN WASCHKE 2020

- *Spam:* Email you didn't ask for
- *Plain phishing*: Simple spam to trick you
- *Spear phishing*: Use personal information such as your contact list, friends on Facebook, …
- *Whale phishing*: uses VIPs (whales), like your boss or an official
- Becoming more automated

VIRTUAL PRIVATE NETWORKS (VPN)

- Technology for making public networks private
- Critical for business, not so much for individuals
- May be useful if you spend a lot of time connected to public Wi-Fi
- Good ones cost—bad ones are downright dangerous
- If you stick with secure websites, you are safe without a VPN
- VPNs may help with privacy