Personal and Family Cybersecurity

RISKS AND BEST PRACTICES – 2018
JAMES M HEWITT, CISSP, MA

Involved with Information Technology for over 35 years.

Archaeologist (MA-Arizona), Computer Programmer, Entrepreneur (Top Giver Software), and I.T. consultant to non-profits, government, and small businesses.

Graduated from SecureSet Academy in Denver in Cybersecurity Core program, 2017.

Passed certification exam for CISSP (Computer Information Systems Security Professional) in 2017

Currently employed at Dish Network as a cybersecurity analyst.

Also plays the fiddle and other stringed instruments, maintains an awesome recording studio (a.k.a. “the money pit”) in Littleton, CO.
Today we will be focusing on cybersecurity for yourself and your family.

- Risks, counter-measures, and best practices for avoiding:
  - Ransomware
  - Phishing
  - Identity Theft
  - Internet of Things
- Controlling the content your kids access
- What we won’t be covering today:
  - Cyber Stalking
  - Cyber Bullying
  - Spam
  - Chat room “friends”

Google “cyber safety for kids”, “kid friendly browser”, “cyber security risks for families” etc. for more information and products for protecting families.
WWW – a.k.a. “the wild, wild web”

Who are the “bad actors”? 
- State-sponsored hackers
- Criminal hackers
- Malicious hackers
- “Script Kiddies”
- You, I, and your kids when we don’t follow best practices!
How pervasive is the problem?

- 2017 Top 10 Sources of Attacks
  - China 41%
  - U.S. 10%
  - Turkey 4.7%
  - Russia 4.3%
  - Taiwan 3.7%
  - Brazil 3.3%
  - Romania 2.8%
  - India 2.3%
  - Italy 1.6%
  - Hungary 1.4%

All are both targets and sources of attacks.
Real Time

- Checkpoint World Wide Threat Map
- Looking Glass Threat Map

- It’s OK to be a little paranoid when it comes to the Internet and cybersecurity risks.
Security by anonymity?

“I think there’s more to cyber security than hiding your laptop under the bed.”
RISKS - open doors for the bad guys

- Unsecured Wi-Fi router/modem
- Use of default router passwords
- Email Phishing / Social Engineering
- Weak passwords (dictionary words), sharing passwords
- Operating System patches not current
- No Anti-Virus or Anti-Malware installed
- Risky downloads, popups, media plugins, etc.
- Using Admin account for routine work
- Unsecured IoT (Internet of Things)
The old favorites….and the new!

- Malvertising (popup ads)
- Spyware, Key loggers
- Viruses
  - Trojans (disguised)
  - Remote Access Trojans (RATS) (backdoors)
  - Worms (Propagate themselves)

Trending now….
- Parasitic Crypto-miners

Remember, the same security problems that affect adults can affect children and teens, who are among the most active Internet users.
Risks you did not expect?

“Air-Cracking” drive-by hacking

- Perpetrator parks in front of your home and uses software to hack into your Wi-Fi network via your unsecured router.

Internet of Things (IoT) - unsecured

- Over 46 million home routers are vulnerable to remote attacks using same ports that your ISP uses for updates. Check with your ISP for router patches.
- Smart door locks, networked printers, smart TV’s and appliances, even children’s toys with Internet connections can be hacked.
- Smart surveillance cameras and baby cams are among the least secure, if they still have their factory default passwords.
- Once cracked, attacker has full access to your network to install trojans and key loggers to get at your passwords and personal info, and will be able to visit illegal sites using your IP address, possibly implicating you in felonious activities.
Ransomware

- As of the end of March 2016, 93% of all phishing emails contained encryption ransomware.
- Mostly companies, but you too!
- Encrypts all of your files with a secret key
- The clock is ticking....
- Bitcoin – pay to get them back!
- OR NOT – 1/3 of time the unlock key won’t be provided even if paid for
- Backups must be current and off the net
- Variant: “ScareWare” – intimidation but no encryption
Social Engineering – the family risk factor

- Email Phishing scams
  - Spear phishing
  - Smishing (SMS, texting URLs)
  - Pharming (spoofed web sites)
  - Vishing (voice phishing, phone calls)
- A Microsoft tech calls you! Really?
- Password guessing (pet names, home town, mascots)
- Shoulder surfing
- Found a flash drive in the parking lot....
- “Fan sites” – free stuff, looks like they are from friends, free music or ring tones, anything tempting to download
Social Media

- Don’t reveal too much personal info on social media sites, can be used for spear phishing, identity theft and cyber stalking
- Limit your posts containing personal information to friends only, never public.
- Check your privacy settings, who can see your posts?
- Never post about medical issues, this is private information that can be used against you by insurance companies and prospective employers.
- Don’t post photos about your vacation until after you return.....
Identity Theft

Your life gets stolen – how?

- Oversharing personal info on social media
- Compromised accounts and passwords
- Malware, hacking, phishing
- Trash (un-shredded documents)
- Breaches of financial and credit systems

Equifax Breach 2017: 148 million records stolen from unpatched servers. Your social security number is out there.

Department of Homeland Security breach 2018: 250,000 government employee records of PII (personal identifying information)
Example of Identity Theft
Spear Phishing = “targeted to you”

- March 2018 – A FedEx “Malspam” email contains your Social Security Number and name.
- Email looks like it’s from Federal Express
- Has a tracking number link
- Has YOUR social security number in the phone number field
- The FROM address comes from invalid domains, e.g. Juggler.net, W3cblog.com, Bordersvinyard.com
- Clicking the tracking link installs a banking trojan, Ursnif. This banking trojan is commonly observed around tax season and steals banking and credit card data using key logging to acquire login credentials.
- See https://www.identitytheft.gov for help on reporting identity theft.

John Q Private
555-444-3333
Best Practices

Accounts and passwords

- Complex but memorable (to you)
- 12+ characters, mix of character types, upper, lower, numbers, special characters like !@#$.
- OR, passphrases if long enough and unique to you.
- Vary your passwords, don’t reuse the same one all the time.
- Limit sharing of passwords

Use a password manager app that syncs to an encrypted cloud account

- LastPass
- Dashlane, etc.

81 percent of hacking-related breaches leverage either stolen, default, or weak passwords.

TIP: Make protected access to your password list or password manager part of your estate plan.
Phishing Emails – How to spot

1. Sender address suspicious
2. To: (recipient is blank)
3. Dear “Customer” instead of your name
4. Grammar simple, or poor
5. No logo, or message signature
6. Wants you to open or download something

From: "FedEx." <xxxxxx@berkeley.edu(link sends e-mail)>
To:
Date: Tue, Jan 3, 2017
FedEx
Dear Customer,

We could not deliver your item.

You can review and print complete details of shipping duty on your order.

Thanks

PDF Attachment: update_Form.pdf

Hover your mouse over log in link, examine the URL in the tool tip popup. This link uses secure-paypal.com.
Validate the link

- Ultratools Domain Lookup
- Secure-paypal.com is registered to CONFLUENCE-NETWORK-INC
- Located in the Virgin Islands....
- Hmmmm, let’s google them.
- They are not associated with PayPal, which is located in San Jose, CA
- If unsure, directly contact the company to verify if the email is valid or not.
- When in doubt, Delete!
Active Protection, Defense in depth

1. Install Anti-Virus and Anti-Malware
   - Keep it updated! Paid versions offer better protection.
   - Don’t install software from unknown or non-reputable sites, be careful with "freeware"

2. A secure login password is good, but...
   - Enable lock screen timeouts on all computers. Manually lock with:
     - Windows: Windows Key + L
     - Mac: Control + Shift + Eject or Control + Shift + Power
   - Don’t share your passwords with friends (but parents should know them)
   - Change your passwords periodically, update your password manager, especially after breaches

3. Smart phones, portable devices, Apple IOS
   - When surfing using public Wi-Fi, install and use a VPN app (Virtual Private Network).
   - Enable Screen Lock with PIN or thumbprint with timeout for your smart phone or tablet.
   - Android is much less secure than Apple IOS, however install A/V and A/M on both for additional protection regardless of platform. Mac’s are vulnerable to malware! It’s a myth that they are not targets.
How to change your default home router password

• Open a browser tab and enter
  • http://10.0.0.1 (Xfinity/Comcast)
  • http://192.168.0.1 (Century Link)
• Enter the username and password provided by your ISP installer
• Change the password to something more secure
• Check the connected devices to make sure you know what they are.
Xfinity Wi-Fi public home hotspot

- If you have Comcast/Xfinity, your Wi-Fi router might already have this feature enabled.
- It’s great for letting your visiting friend or relative log into your home network without exposing your private password, BUT
- It is a potential security risk since ANY Xfinity customer within range of your home network can log in.
- You can disable this easily by logging into our account.
Use Multi-Factor Authentication

- To avoid abuse of your credentials, use MFA (multi-factor authentication) for critical apps like online banking. This is becoming a standard for companies. Use at least two of:
  - Something you know (e.g. password)
  - Something you have (e.g. smart phone)
  - Something you are (e.g. fingerprint, facial)
  - Some place you are (e.g. not Russia)

For example, password + text or voice code sent to your phone (good, two factors)
Password + secret answer, like high school mascot (not so good, only one factor)
Ways to filter and block Internet content

- **Disconnect.me** – blocks adware and popups that appear on web sites, some of which may contain malware, free version

- **Https Everywhere** – free browser extension for Chrome, Firefox, and Opera that forces a secure connection where possible

- **McAfee WebAdvisor** – Free, protects against malicious web links, scans your downloads, checks your security settings

- **OpenDNS** – a free way to block and audit content and web sites, “Family Shield” parental control
And never forget your Backups

- On-site and Off-site (cloud)
- If cloud backup, be sure the service encrypts the backup and uses password
- Keep a flash drive handy for backing up important documents, and lock it up when not using it.
- Backup on a schedule
  - Full (less often)
  - Recovery (with OS image)
  - Incremental (changed files) – Daily or weekly
  - Recovery - Test it once in a while
- Disconnect external drive when backup complete (ransomware can encrypt it if connected)
Patch – Patch – Patch!

- Patch the operating system on your computers and portable devices as soon as updates become available.
  - Most Zero-Day vulnerabilities are fixed within a few weeks
- Unpatched computers are one of the biggest risk factors, re: Equifax breach
- Enable automatic operating system updates
- Patch your browser and other critical applications as well, e.g. Office 360, Adobe Flash.
Caveat – There is no such thing as 100% safe and secure....

The wild, wild web can be a scary place these days. But if you follow these best practices you can avoid the worst of the threats and substantially reduce the risk for you and your family!
Resources

Windows 10 Defender (built-in) - Windows 10 version 1709, also known as the Fall Creators Edition, has ransomware protection but does not work with 3rd party anti-virus.

Also Recommended: MalwareBytes, McAfee Total Protection, Norton Security Premium (paid versions) (Windows or Mac)

Clam A/V (Linux)  https://pcantivirusreviews.com/Comparison/


How to Protect Your Child Online:
https://www.huffingtonpost.com/entry/theresa-payton-keep-kids-safe-online_us_5a944d02e4b02cb368c46c87

Threat Maps:


Verifying domain name owners:

How to recognize fraudulent emails and websites
https://www.virustotal.com/#/home/upload

Ransomware
https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

Identity Theft: https://www.identitytheft.gov