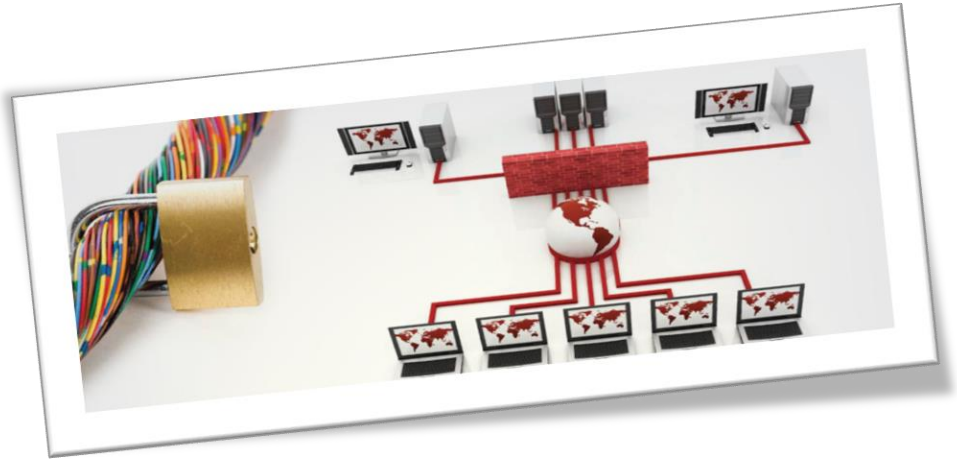


CyberSecurity Practices

A Guide to County Citizens on CyberSecurity

Agenda

- What are the threats?
- How to protect ourselves?
- Government Cybersecurity programs
- Online Security Best Practice Sources and Information

Popular Threats

Malware

- Malicious software that is designed to gain silent access or damage a computer system.
- Risks: Private data, financial data, extortion, attacks to other sites
- Includes:Spyware, Keyloggers, Ransomware, Rootkits

Suspicious Emails and Links: Spam, Phishing, Spear Phishing Attacks

- Spam - Electronic unsolicited, bulk, unwanted Junk email or from Social networks
- Phishing – use of email or malicious websites to collect personal/financial information. It may infect computer systems with Malware and viruses
- Spear Phishing – specialized attacks against a specific target or small group of targets to collect information or gain access to systems.

Ransomware

- Malicious software that hackers use to encrypt an infected computer system or critical files. To unlock them, you have to pay ransom.

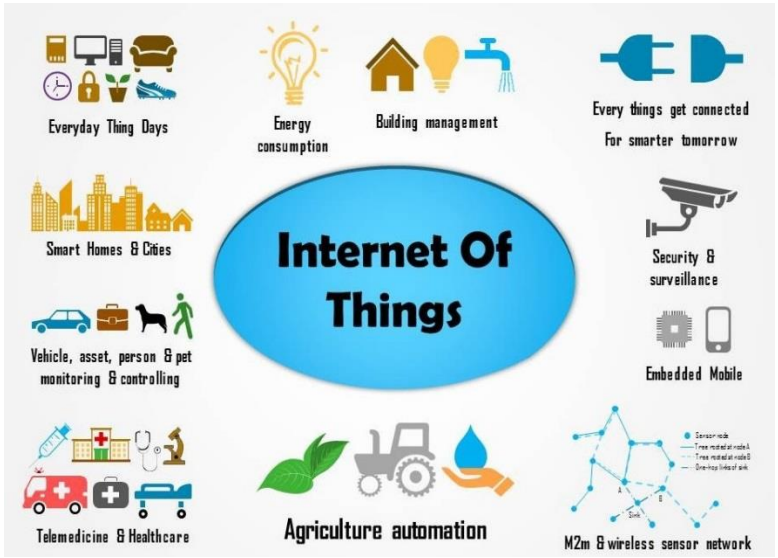
Connected Home, Internet of Things (IoT) attacks

- Network connected devices is growing at a fast rate. We need to take a step back so that security keeps up with IoT innovations.

How to protect ourselves?

Technology Personal Computing

1. Software Updates
2. Email Protection from Spam, Phishing
3. Password Management (strong passwords, change passwords often, use of two-factor authentication)
4. Endpoint Protection (Malware detection, Viruses, Firewall)
5. Browser Security Settings
6. Use of free Third-Party DNS (Web content filtering, Parental controls, Phishing protection, Geoblocking)

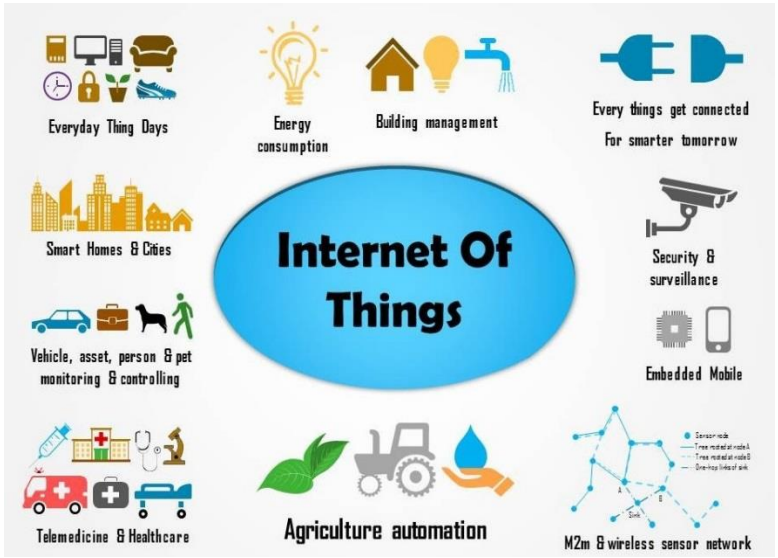


Fairfax Internal Use only

How to protect ourselves?

Technology: Mobile Phones

1. Use latest version of Phone OS and apps
2. Complex Password, Encryption, change default security settings
3. Download apps with caution (iTunes store relatively safe, Android Market not so much)
4. Consider Security Software
5. Avoid conducting transactions on Unsecured Wireless networks

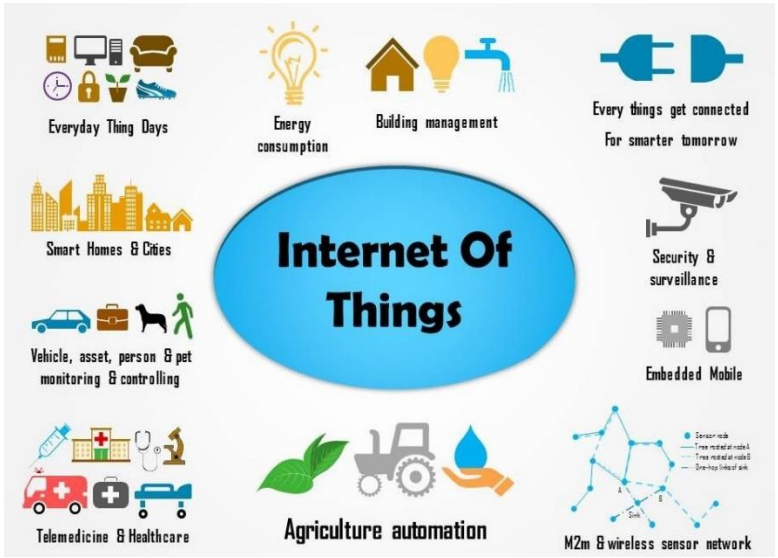


Fairfax Internal Use only

How to protect ourselves?

User Awareness

1. Make sure system is updated and secure
2. Be very skeptical clicking on pop-up windows, error messages, attachments. (Think before you click!!)
3. Report anything malicious (Spam, malicious emails from friends, content from social networks, etc.).
4. Use Caution when installing new Software and Apps. Consult with a tech savvy person
5. Behave Online as you would in Real Life. If you feel it's unsafe, trust your gut.
6. Keep up-to-date on best Security practices

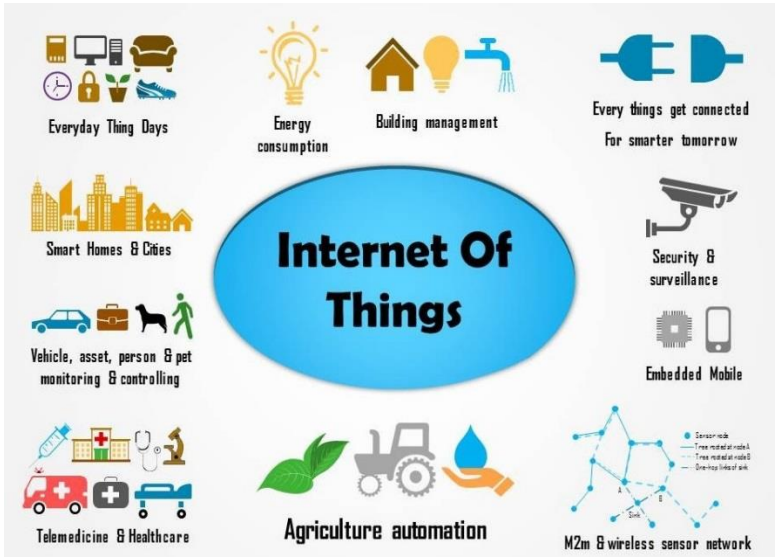


Fairfax Internal Use only

How to protect ourselves?

Connected Home & IoT

1. Software updates
2. Change default security settings of devices (passwords, users, network setup, etc.)
3. Extensive research before purchasing a product. Make sure the manufacturer invests on continuous product development and extended support.
4. Networking: Best practice on network segmentation, Network Security, Wireless security, Wireless signal strength and surveys
5. Access Control and management
6. Mobile Device Integration and Security



Fairfax Internal Use only

Government Cybersecurity Programs

Security Awareness Training

Incorporate Cybersecurity in the Public School System

- Teach Cybersecurity in our schools

Use of Social and Broadcast Media

- Reach out to employees and citizens using social media (Twitter, Facebook, YouTube Video Vlogs), broadcast technology (tv, radio programming), Posts Public and Private blogs about Security practices, announcements and threats using County Website resources

Community Outreach

- Talking to Citizens about the importance of Security (Senior, kids, employees)
- Participate in Industry Security Panels, meetings, Conferences

Fairfax Internal Use only

Online Best Security Practices Sources and Information

https://cyberva.virginia.gov/
https://www.usa.gov/online-safety
https://www.dhs.gov/topic/cybersecurity
https://www.dhs.gov/stopthinkconnect
https://www.consumer.ftc.gov/features/feature-0038-onguardonline
https://www.fbi.gov/investigate/cyber
https://www.iad.gov/iad/library/ia-guidance/security-tips/best-practices-for-keeping-your-home-network-secure-updated.cfm (one of the NSA sites)
https://kids.usa.gov/online-safety/index.shtml
https://digitalliteracy.gov/taxonomy/term/93
https://stopthinkconnect.org/

http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
http://security.fnal.gov/UserGuide/password.htm
http://www.pcmag.com/article2/0,2817,2407168,00.asp
https://www.grc.com/passwords.htm

IoT
https://cta.tech/cta/media/Membership/PDFs/Recommended-Best-Practices-for-Securing-Home-Systems-v16.pdf
https://www.dhs.gov/securingtheIoT
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program