Staying Safe & Secure Online
A Quick and Simple Guide to Information Security

Joseph Guarino
Owner/CEO/Sr. Consultant Evolutionary IT
A+, Net+, Security+, CISSP, LPIC, MCSE 2000/2003, PMP
www.evolutionaryit.com

Objectives

- Demystify the subjects of information security in plain English.
- Impart understanding of the security risks, impacts, ramifications.
- Device/technology independent
- Give you practical knowledge to protect yourself, family and community.

Misperception

It can't happen to me

Common Misperceptions

- *"I have anti-virus software..."*
- *"I don't personally have anything of value on my computer..."*
- *"I have a firewall..."*
- *"I don't need to backup..."*
- *"There are no major financial risks...*

Let's Define Some Key Terms & Trends

General Terms

- **Software Bug** – an **error, flaw** or mistake in a computer program.
- **Vulnerability** – is a **weakness** in a system that allows an attacker to exploit or otherwise violate the integrity of your system.
- **Patch** – a **fix** for a software bug or security vulnerability.

Malware Terms

- **Malware** – software designed to **infect and damage** a user's computer system without the owner's consent. This is the general all encompassing term.
- **Virus** – computer program that infects or **copies itself** onto a user's computer system without user's permission/consent. Most often a virus delivers a dangerous payload or action.

Malware Terms

- **Spyware** – software installed surreptitiously on a users computer system to intercept, monitor, market.
- **Adware** – software installed surreptitiously which is designed to deliver ads.
- **Badware** – alternative term used to describe spyware, malware and deceptive adware.
- **Grayware** – term used to describe spyware, adware, dialers, remote access kits that harm systems performance.

Malware Terms

- **Bot** – machines infected with worms, trojans or other malware under a **centralized control structure**.
- **Worms** – network enabled or aware viruses.
- **Rats** – remote access toolkits which allow **remote access** to a users machine.

Malware Terms

- **Dialer** – an unwanted dial application which connects to pay-rate phone numbers.
- **Rootkits** - program that takes fundamental control of your system without your consent.
- **Key Loggers** – hardware or software means of capturing users keystrokes.
- **Phishing** – attempt via email, IM or other malware to redirect user to fraudulent websites.

Malware Terms

- **Spear Phishing** – targeted at specific individuals or group
- **Whale Phishing** – targeted at wealthy powerful targets

Malware Terms

- **Drive by Download** - unintended

  (or misunderstood) download that delivers malware
- **Ransomware** – Holds your data for ransom
- **Mobile Malware** – Malware that focused on mobile devices – smartphones, tablet.

State of Malware

- Increasingly - malware have advanced characteristics: distributed, polymorphic, automatically evading detection, encrypted, self-protecting and self-healing.
- Shows all the hallmarks of professional software developments but with a deeply pernicious/criminal intent.

Changing Face of Malware

- Malware's evolution will NOT stop and it will be a constant battle to defend against an ever changing threat.
- Profit motive of cyber criminals will always bring new threats.
- Consider that the threats will expand to new technologies.

Malware Marketplaces

- There are underground criminal marketplaces
- Sell professionally developed tools that make this easier for other criminals
- Sell any manner of cybercriminal tools and black hat activities

Internet = Ocean

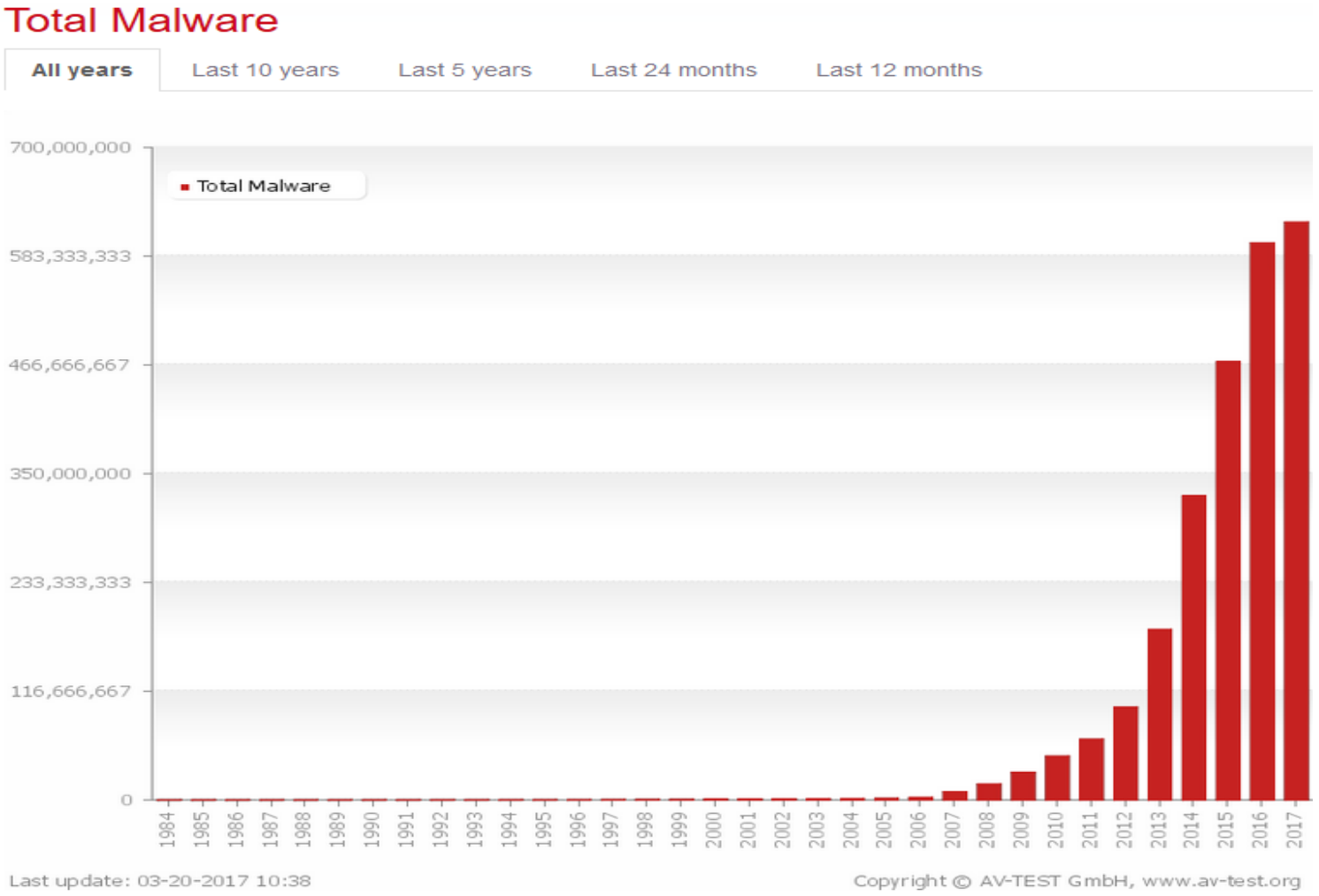
- **Surface Web** - Anything you can find at a typical search engine such as Google, Bing or Yahoo.
- **Deep Web** - Inaccessible via conventional search engines. Examples are private databases of academic information, medical records, government resources, etc.

Internet = Ocean

- **Dark Web** - Part of the deep web marketplaces for illicit activities Accessible by TOR (The Onion Router) or I2P (Invisible Internet Project) network. Example is the former SilkRoad.
- Encryption & anonymity
- Has many legitimate and legal uses

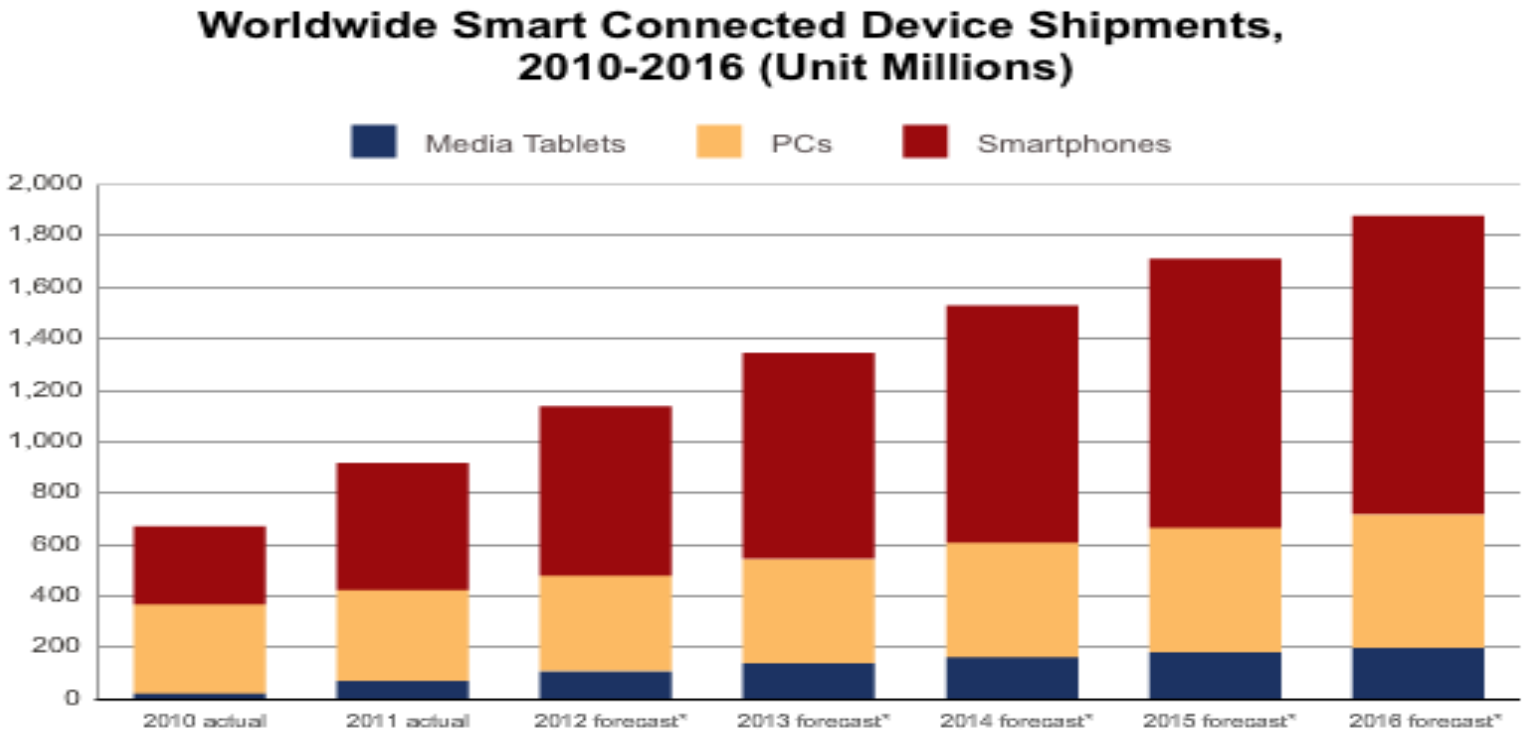
Malware is an EVER growing problem!

Malware Ever Expanding



See: http://www.av-test.org/en/statistics/malware/

So Will Malware Growth Focus



Source:IDC

Mobile Malware

- As the market grows so does threat
- Mobile devices offer opportunity because often have less evolved security mechanisms
- Lax mobile marketplace standards

Stats Financial Consequences

Source: 2016 Norton Cybersecurity Report

Who Creates This Stuff?

Hackers Hats?

- **White hat** = Good. Often called ethical hackers who help society, law enforcement and government.
- **Grey hat** = Middle of the road, sometimes good sometimes bad.
- **Black hat** = Compromised ethics and often criminally minded.

Cybercriminals

- Today it is less of teens just “messing around”
- Real threats are: criminal syndicates, foreign governments, general thugs.
- These organizations are the “well-source” of most of these activities.

Cybercriminals

- Motive (Money), Opportunity (Unpatched, insecure systems/network), Means (Resources).
- Cybercriminals use increasingly sophisticated software to mount attacks.
- Malware consistently evolves around the attempts to defend against it.

Security Isn't All About Technology

Operating Securely

- Computer security is as much about what you do as it is about technology.
- Being aware of how to safely navigate your digital is step one.
- The right technology with proper application of that technology is only part of the equation.

Social Engineering

Social Engineering

- Cyber criminals will attempt to manipulate, finesse, trick the information from you in the most conniving and creative ways.
- Comes in the form of calls, emails, IM's, etc.
- Don't trust them. Don't give them information.
- Always decline and go back to official source

Social Engineering Uses

- Emotions
- Money
- Sex
- Power
- Ego
- Etc.

Social Engineering

- Many forms of malware/attacks have a social engineering aspect
- Ask yourself if you have reason to trust?

Key Internet Technologies

Key Internet Technologies

- Domain name system - It translates the underlying IP or numeric addresses of the internet into humanly readable form.
- Domain name locates an organization online. GTLD (Generic Top Level Domains). Class of organizations. Ex. .com, .net, .gov.
- CcTLD (Country Code Top Level Domain). Country or territory. Ex. .us (USA), .it (Italy)

Anatomy of a Web Address

- URL – Universal Resource Locator or URI Uniform Resource Identifier.
- Web address
- http://en.wikipedia.org
- Protocol – http, https, ftp, etc.
- Hostname – name of machine.
- Domain name - .org - non-profit

SSL/TLS

- Https
- SSL/TLS
- Secure encrypted web connection. Shows up as a lock in the browser.
- Much like a drivers license or other form of ID.
- Issued by Certification Authority such as Verisign, Thawte, GeoTrust, Entrust, Comodo or Godaddy.
- Validates that the website you are connected to.
- Look for the Lock and the color green!

Additional Security Browser Plugins

- No script - Control Javascript, Plugins
- uBlock – Ad blocker
- EFF Privacy Badger- Block Ads & trackers
- HTTPS Everywhere – Forces SSL/TLS

Web Based Threats

Web Based Threats

- Client side malware is often delivered via websites, email, social media, etc. clandestinely without your knowledge or approval.
- This type of attack pinpoints vulnerabilities in the browser software itself and it associated plug-ins(Flash) or technologies(Java/Javascript, cookies).

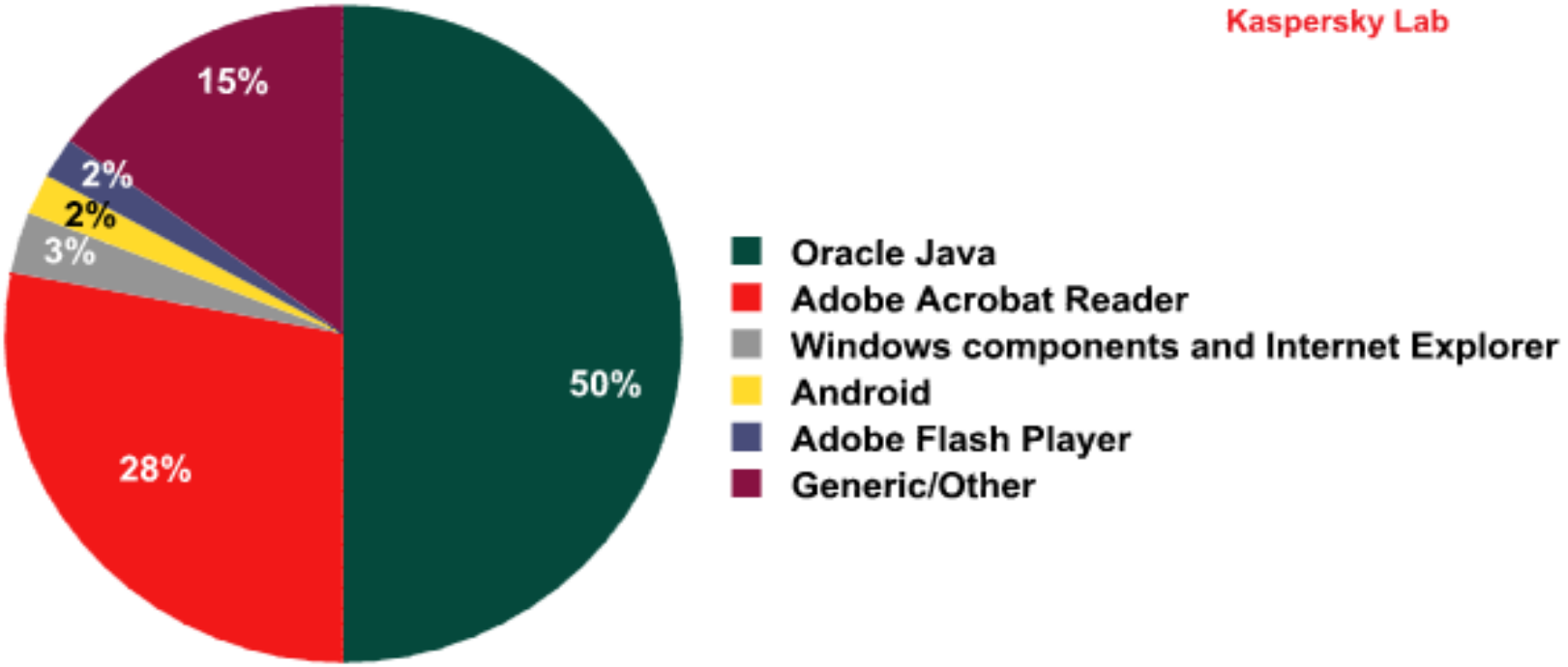
Web Based Remediation

- Only visit sites you can judge to be legitimate.
- Trust not click not.
- Mistyping a URL can lead you to a fake/phishing or even malware site.
- Only go directly to the associated website via typing it in the location or address bar.

Web Attack Focus

- Browsers (All)
- Java
- Adobe Flash
- Adobe Reader

Vulnerable Applications



See http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_%202012_The_overall_statistics_for_2012

Phishing

Phishing

- SPAM, Social Media Site, brings you messages that seem to be from legitimate parties that send you to phony/look-alike website.
- Your (Personally Identifiable Information) and credit card information is collected and sold in the underground.
- Usually an attempt is also made to infect your machine with malware.
- Best to not even open. Delete.

Phishing

- Think before you click! Don't open. Delete it!
- Are you a customer? - If not Mark as SPAM and delete.
- Did you have any recent interaction with the company involved? - Don't open it. Deleted!
- INSTEAD, go to the official website Validate its certificate.
- Then log on to your account.

Phishing Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Account cancel!
- Social Engineering – Attempt to mislead, persuade,confuse, etc.
- Generic or Targeted Greetings – Hello Distinguished Sirs!?
- Urgent Request for PII – We need to validate your account or you will be terminated from the internet!
- Forged Email. - Email is often not valid and or not from the domain in question.
- Incorrect Link – Link is obviously wrong. https://www.payppal.net/~noway

Phishing Advice

- Paypal Anti-Phishing Guide
- Ebay Identifying Phishing/Spoofing
- Phish Tank Website
- Anti-Phishing Working Group

SPAM

Spam Characteristics

- Spam is often a carrier/propagator of malware
- Social Engineering is a common thread in SPAM.
- Spam and Phishing (among other malicious ends) are interrelated activities.

SPAM Remediation

- Don't post your email address online on websites, forums, chatrooms, etc.
- Don't open spam! Use your email software to mark it as spam and delete it.
- Never respond to SPAM.
- Never EVER buy from SPAMMERS.

SPAM Remediation

- Most standalone email clients such as Outlook, Thunderbird and OS X Mail offer built-in SPAM filtering.
- Optimally shut off or limit; Images, Javascript, Java, Flash etc in your email client or web browser if you use web based email.
- Shut off HTML mail and use plain text.
- If you are getting lots of SPAM in your Inbox, switch to another email provider that does a better job filtering.

Social Media

Social Media Threats

- Notion of relationship & trust makes for ripe social engineering
- Cyber criminals use social networking sites as a delivery mechanisms for malware.
- Spammers and Malware purveyors use these sites features (email, chat room) to “promote” less than reputable software and websites.
- Leaving open anonymous access to your account and PII (Personally Identifiable Information)

Social Media Threats

- Third party add-on applications may have security concerns.
- Fake accounts and spam content abound on some of these sites.
- Comment spam is a major problem on some of these sites.

Social Media Study

- Provide Security
- 28 Day Study
- Fake person/profile - Robin Sage
- Connected with over 300 in information security professionals

Robin Sage

facebook Home Profile Friends Inbox Settings Logout

Send Robin a Message
Poke Robin

Information

Relationship Status:
Single

Birthday:
February 2, 1986

Current City:
Virginia Beach, VA

Political Views:
Not Obama

Religious Views:
If I lived in ancient Greece, Dionysus would be my god

Website:
http://www.linkedin.com/in/robinsage
http://twitter.com/robinsage
http://robin-sage.blogspot.com

Robin Sage

Wall Info Photos

Write something...

Attach: Share

Omachonu Ogali I'm sorry, but you're extremely sketchy.

You create LinkedIn, Blogger, and Twitter profiles with a fake name, all on the same day.

Your LinkedIn profile initially said you were a "Cyber Intelligence Operator", which is a position that does not exist. You recently changed it to "Cyber Threat Analyst".

You claim your hometown is Moyock, NC, which is Blackwater's US training HQ.

No one in the 2003 class of St. Paul's has any idea who you are.

Worst of all, you randomly add tons of people in the security industry, but no one can vouch for you.

3 minutes ago · Comment · Like · See Wall-to-Wall

RECENT ACTIVITY

Robin and Omachonu Ogali are now friends. · Comment · Like
Robin and Zach Valko are now friends. · Comment · Like
6 more similar stories
Robin became a fan of Blackwater. · Comment · Like · Become a Fan
Robin changed her Religious Views. · Comment · Like
Robin and Gunter Ollmann are now friends. · Comment · Like
Robin and Murdøc D. Net are now friends. · Comment · Like
3 more similar stories
Robin likes Mike Roadancer's status.
Robin commented on Mike Roadancer's status.
Robin and Robert RSnake are now friends. · Comment · Like
Robin and Jeremiah Grossman are now friends. · Comment · Like

Social Media Remediation

- If you don't know the person and have established a relationship with them then do NOT add them to your network.
- Delete or mark as SPAM, emails, IM's or comments that illegitimately advertise, or otherwise violate the sites terms of service.
- Don't click on content in people profile as it may redirect you to somewhere you don't want to go and or infect your computer with malware.

Spy/Ad/Bad/Greyware

Spy/Ad/Bad/Greyware

- Programs are shareware/freeware or are downloaded, arrive in spam, phishing, social network site, IM, etc.
- Trust not click not!
- Be in the habit of being skeptical!
- Research before you click or install.

Spy/Ad/Bad/Greyware Remediation

- If you really need the program, buy from a respectable vendor.
- If you want a truly free program that has none of these problems - then get Free Software or Open Source Software.
- Read the fine print, EULA (End User License Agreement), Privacy Policy.

If You Want Really Free Programs

Software Licensing

- **Commercial Software** – proprietary software that you commonly use. Has very restrictive rights on use.
- **Shareware/Trialware/Nagware** – a trial version of a commercial program. Can sometimes contain malware.
- **Freeware** – free in terms of price. No cost but can sometimes contain malware.

Software Licensing

- **Open Source** – allows anyone the liberty to use, extend and distribute the software as they see fit. No Nag/Grey/Ad/Badware.
- **Free Software** - allows anyone the liberty to use, extend and distribute the software as they see fit. Focus on freedoms/liberty above all else. No Nag/Grey/Ad/Badware.
- **FOSS** – Free and open source software is a term to specify the range of free and open source software.

Free & Open Source Software

Libre Office - Office suite

Ubuntu Linux - Entirely free operating systems

Mozilla Firefox - Open source browser

Wikipedia list of Open Source Applications

Open Source Alternative

IoT

- Internet of Things
- All connected things need to be secured

General Security Recommendations

General Recommendations

- **Backup** your data to external disk, CD, DVD and or internet backup (encrypted in transit and at rest).
- **Patch** your devices. Ex. Windows (Windows Update), Apple OSX (Systems Update). Set to auto update!
- **Patch third party applications**. Currently there is no common patch framework.
- **Remove Flash, Java, Adobe Reader**.
- **Least privilege**. Run as regular user not Administrator/Root. Windows (Standard User), OSX (Standard User).

General Recommendations

- Buy an **Anti-malware** scanner. Make sure it covers ALL malware threats! Keep it up to date.
- **Don't run EOL** (End of Life) software or hardware. Ex. Windows XP or Apple OS 9.
- **Trust not, click not**. Trust nothing unless you can validate its source.
- Don't read/open/click on spam, phishing emails, IM's, websites, content that you do not know or trust.

General Recommendations

- **Encrypt** always and everywhere
- Especially on any sensitive data
- Especially portable devices
- Full Disk vs. File Encryption

General Recommendations

- Deploy both software/hardware **firewall**. Most anti-malware suites have a software firewall in them.
- Hardware firewalls from Asus, Netgear, Linksys, are inexpensive and generally effective.
- Look for next generation/UTM like features like Anti-malware scanning, URL Filtering, anti-phishing.

General Recommendations

- Don’t use your ISPs modem/router/firewall/wireless router. Get your own!
- Hardware firewalls from Asus, Netgear, Linksys, are inexpensive and generally effective.
- **Update your firmware**. See vendor site for details.
- Secure your wireless with WPA2 and long complex key (same rules as password) >32-64 alphanumeric characters. Also see: https://www.grc.com/passwords.htm

General Recommendations

- Choose strong passwords. >12 alphanumeric, not a word in any language. Use mnemonics or “memory device”. Go for passphrases!
- Strong passwords for you systems, websites, network devices, etc.
- Always use multi factor authentication. Ex Banking, Google, Apple, Paypal
- There are also simple password management applications such as RoboForm, Lastpass or KeePass.
- http://www.us-cert.gov/cas/tips/ST04-002.html

General Recommendations

- Only get software from official sources. Example Adobe Flash = adobe.com
- Official marketplaces. Example Android = Google Play
- If available you can check integrity w/ hashes

General Recommendations

- Choose the vendors you use wisely
- Do they offer the security features you need
- Do they stand by the product
- Vote with your $$$’s

Wireless Recommendations (Coffee Shop and Travel)

- Protect yourself from MiTM Man in the Middle Attacks and many others with encryption
- MiTM interception, eavesdropping, hacking on wireless networks
- Use a VPN (your own) or a VPN service

VPN Services

- F-Secure Freedome VPN
- https://www.f-secure.com/en_US/web/home_us/freedome
- Private Internet Access
- https://www.privateinternetaccess.com/
- Check for Privacy Leaks
- https://ipleak.net/

Use a Password Manager

- RoboForm - Windows, OSX, Mobile
- LastPass – Windows, OSX, Mobile
- KeePassX - Open Source - Windows, OSX, Linux, Mobile, etc.
- KeePass - Open Source - Windows, OSX, Linux, Mobile, etc.

Multi Factor Authentication

- MFA – security method that requires 2 or more authentication factors
- **Something *you know*** (password or secret questions), something you have (ATM card, proximity card), **something *you are*** (fingerprint, face)
- We use it with online banking, email accounts, cloud storage, etc.
- Facebook Login Approvals, Google 2-step verification

Backup

Backup

- Critical
- Microsoft & Apple have built in backup technologies for local backup.
- Always 2 or more backup locations
- Always ENCRYPT all backups

Backup

- Get external USB hard drives for backing up local machine (local backup).
- Online backup
- Do BOTH

Online Backup

- CrashPlan
- Carbonite
- Mozy

Anti-malware

Anti-Malware

- You must have it!
- Not foolproof 100%
- Still useful when coupled with other technologies and behavior changes

Anti-malware Vendors

- Kaspersky
- Trend Micro
- Eset
- McAfee
- Symantec

Data Remanence & Recycling/Disposing of Your Digital Devices

Data Remnance

- When you recycle your old computer or (any other digital device) don't do it without securely erasing the data.
- When you delete data its not gone. It can be easily recovered.
- Same goes for all other digital devices such as cell phones, smart phones, personal assistants, etc. that have personal information on it.
- USB Thumb drive/Key, CD/DVD.

Data Remnance

- Deleting files or even formatting a drive is not enough. Wipe them.
- OSX, Windows, Linux all have free & commercial tools to do this.

Erasure Apps

- Eraser (Windows) Open Source
- ShredIt (Mac) Commercial
- O&O Safe Erase (Win Commercial)
- Active@ KillDisk (Windows/Linux Comm)

Smart Phones

- Remove and destroy the SIM (subscriber identity module) card.
- Remove and erase and micro SD memory (same tools to remove data as normal disk) or hit with hammer and trash it
- Check for delete or reformat instructions at:
  - Smartphone Manual
  - Smartphone Manufacturers Website
  - Cell Carriers Website

Holistic Vision

Defense in Depth

- Defense in depth – Using many layers, technologies, techniques and processes to help mitigate/reduce the risk of any one component of an information systems being compromised.

Conclusion

- Use the many tools and processes at your disposal
- Change your habits and behavior for a more secure future
- Be vigilant and aware
- Stay safe out there!

Let's Connect

- Joseph Guarino
- Find Me on Social Media
- Company Website
- https://www.evolutionaryit.com

Thank You

- Cambridge Science Festival
- All of You!