Practical Computer Security for Writers

By
J.T. Evans
http://jtevans.net/

Protecting Your Data, Files, Work and (in some cases) Livelihood

1. Upgrade/Patch ASAP
    a. Microsoft Tuesdays
        i. Second Tuesday of each month
        ii. Some “out of band” updates available
    b. Weekly for other operating systems
        i. Apple OSX
        ii. Linux
    c. Third party software. Weekly updates are usually sufficient
        i. Adobe (Flash, Acrobat, Creative Suite)
        ii. Office (Microsoft, OpenOffice, LibreOffice)
        iii. Java
2. Install Security Software
    a. Anti-Virus
        i. Symantec
        ii. McAfee
        iii. Kaspersky
    b. Personal Firewall
        i. Keeps your data in. Keeps Bad guys out
    c. Spyware Protection
        i. Prevents data leaks that can allow others access to your data
        ii. There are free options: You get what you pay for.
3. Like with other software, keep anti-virus up-to-date.
    a. **<u>Daily</u>**
4. Backups
    a. Full backups monthly
    b. Incremental backups weekly
    c. Cloud-Based Solutions (What are they doing with your files?)
        i. DropBox
        ii. Carbonite
    d. Network-Based Solutions
        i. NAS (Network Attached Storage)
            1. iOmega Home Media Cloud Edition
    e. Host-Based Solutions
        i. External Hard Drive
        ii. CD/DVD
            1. Degrades over time. Replace at least every 6 months
    f. Software
        i. Genie Timeline for Windows
        ii. Time Machine for OSX

Writing Computer Security in a Plausible Manner

1. Security is an onion.
    a. Many layers are built on top of each other
    b. If one layer fails, others should pick up the slack
2. Terminology
    a. Hardware
        i. The stuff you can touch. Mouse, keyboard, hard drive, monitor, etc.
    b. Software
        i. The programs that run on your hardware. Can't really "touch" them
    c. Malware
        i. Malicious Software
    d. Types of Malware
        i. Virus: Can alter existing software to replicate itself across media such as floppy disks, hard drives and USB flash drives
        ii. Worm: Can alter existing software to replicate itself across networks and email
        iii. Trojan: A program disguised to do one thing, but really does something else. Usually a payload for a virus or worm
        iv. Rootkits: Alters the base operating system to put in a "backdoor" to allow for "root" or "core" access to the computer without authentication
        v. Botnet: A large collection of machines infected with a worm. Usually used for DDOS attacks or massive spam campaigns
        vi. Spyware: A virus or worm that is specifically crafted to steal PII (personally identifiable information) or passwords
        vii. Adware: Injects advertisements into web sites or on to your screen to entice you to click through. A great revenue generation method
    e. Network
        i. Multiple computers linked together via some means
    f. Intranet
        i. A local network (aka: LAN, Local Area Network) or isolated network of machines
    g. "Internet" vs. "internet"
        i. An internet (no capitalization) is collection of intranets that are hooked together, usually over a broad geographic area
        ii. The Internet (note the capitalization) is a singular entity, which encompasses publicly available resources such as the World Wide Web, email, usenet, bittorrents, file transfers, streaming video/audio, online gaming and more. In this case "Internet" is a proper noun.
    h. Firewall
        i. Usually the front-line defense against attacks. Filters out Bad Guys. Allows in Good Guys.
    i. IDS
        i. Intrusion Detection System
    j. IPS
        i. Intrusion Protection System. Like an IDS and Firewall together
    k. HIDS/NIDS/HIPS/NIPS
        i. Host Intrusion Detection/Protection System
        ii. Network Intrusion Detection/Protection System

3. Attack Vectors Used by the Bad Guys
    a. DOS/DDOS
        i. (Distributed) Denial of Service attack
        ii. See recent attacks by "Anonymous" on various sites/locations as a form of "hacktivism."
    b. Weak Passwords
        i. Do not use the same password everywhere. If one site gets compromised, then your common, shared password is also compromised *everywhere*.
    c. Buffer Overflow
        i. Most common attack vector, but quickly being overtaken by SQL injection.
    d. SQL injection
        i. SQL is "Structured Query Language" and is a way to talk to databases. An attacker can "inject" code into a SQL statement to steal data, destroy data or alter data.
    e. Social Engineering
        i. "The man with a clipboard." Used to trick secret information out of people.
    f. Cross Site Scripting (XSS [CSS was already "taken."])
        i. Injecting malicious code into web sites to take control of a target's web browser.
        ii. Can create a "browser-based botnet" with this means along with a slew of other security issues.
    g. Cross Site Request Forgery (CSRF)
        i. Can trick your browser into clicking a link for you. Think of Amazon's one-click shopping. If someone can trick your browser into clicking the one-click buy, you'll soon be charged for and receive the item "you" bought. Yes. Amazon's one-click was, at one time, vulnerable to this.
    h. Lack of Encryption
        i. Open wifi at coffee shops or even (*gasp*) at your home.
        ii. Use VPNs if you have them.
        iii. Use SSL (https:// not http://) where possible.
            1. Browsers have many different ways to display the presence of quality SSL. Learn the tips for your specific browser.
    i. Network/Host scanning
        i. Scans a host or network looking for open vectors of attack.
        ii. nmap
        iii. Nessus/OpenVAS
        iv. Metasploit
        v. kismet
        vi. aircrack, aircrack-ng
        vii. WiFi Explorer
        viii. … countless others.
4. Additional Resources/Research
    a. https://www.owasp.org/
    b. http://www.sans.org/
        i. http://www.sans.org/security-resources/glossary-of-terms/
    c. http://www.eccouncil.org/
    d. https://www.isc2.org/
    e. http://www.microsoft.com/security/resources/
    f. http://www.wikipedia.org/ -- Good for delving deeper into some topics.