21 WAYS YOU CAN FIGHT CYBERCRIME

21 WAYS YOU CAN FIGHT CYBERCRIME

William G. Perry, Ph.D.

William G. Perry, Ph.D.

Published by:

William G. Perry, Ph.D.

Lake City, FL

www.computer-security-glossary.com

Library of Congress Cataloging-in-Publication Data
Perry, William G., 1947 -
Code / William G. Perry

Publications by William G. Perry are available to booksellers and distributors world-wide.

21 Ways You Can Fight Cybercrime

Do you worry about the growing threat from cybercrime? Me, too.

The problem is getting worse. The losses due to cybercrime now exceeds the amount of money being made in the illegal global drug trade (i.e. 1.5 trillion dollars). The number is dramatically increasing and projected to grow to six trillion dollars by the year 2021.

Law enforcement can do very little to help protect you.

Why do we find ourselves in this situation? First, cybercrime is a low-risk high pay off criminal activity. Second, the Internet is an easy target that wasn't built for security. Third, the number of today's interconnected devices and the power of computing devices is dramatically increasing. And fourth, attacks are becoming more targeted and sophisticated.

Everyone is a target. We must raise our level of security awareness and take proactive steps to protect our private and critical information assets. Cyberattacks are becoming more numerous and sophisticated. People and businesses must be aware of

the risks they face every time they turn on a digital device from a smart phone to a tablet or desktop computer.

We must become proactive and follow the **security best practices** that are outlined below:

What Are Security Best Practices?

1. Use complex passwords – Cybercriminals have access to powerful computers and programs that can quickly break conventional passcodes. A complex password should be at least eleven characters in length and contain one uppercase and lowercase letter as well as at least one special character or symbol like $ or # - and at least one number. Users should also avoid using words that can be found in the dictionary, your name, birthday or any other words that are associated with you or family members.

Your password should be changed frequently and avoid using the same one to access different accounts.

Some experts suggest that you consider using a pass-phrase that includes numbers and special characters. For example: **??12FlowersInWinter??**

2. Consider using "multi-factor authentication" – This phrase means you should use more than one method to verify the identity of a user wishing to gain access to private information resources. Multi-factor authentication is a more rigorous way to provide computer security. An example would be requiring a user to select a complex password as well as a randomly generated number (e.g. from a service like Good Authenticate) or a biometric factor such as a fingerprint.

3. Regularly update your software and install patches – Computers, laptops, tablets and smartphones use two types of software.

One type is known as *operating system software*. It spells out the rules by which hardware can be used to accomplish work. **Windows 10™**, for example, is operating system software.

The second type is known as *application software*. It performs specialized work on your data (i.e. the way Photoshop can be used to alter images).

Computer hardware manufacturers and software publishers frequently update operating system and application software Registered customers are notified when

changes are made. Software patches and updates sometimes add capabilities or "plug" security holes.

4. Purchase and use malware protection software – There are a number of anti-malware programs on the market. You should research the various products and read multiple online reviews to help you in your research.

Several of the key features you would want in malware protection are for it to be easily updated and that it is capable of scanning your system.

Purchase the product that best meets your needs.

A malware protection suite should work to combat Trojans, Worms, Viruses, as well as Adware/Spyware. The security software you choose should ideally monitor and report any unauthorized attempts to access your system, or install unauthorized programs and should flag malevolent sites.

5. Use a firewall – There are two types of firewalls. One is a software application and the other is a hardware device. The function of a firewall is to monitor incoming and outgoing communication between your computer and the Internet.

A software firewall is installed on your computer. You can customize the settings to make it work the way you want. Software firewalls help you to fight off attacks and keep hackers from gaining control of your digital resources. Most people would be able to make use of a software firewall on his or her personal computer or laptop.

A hardware firewall is a physical device that is placed between your computer and the Internet and it protects the computer or network computers from attacks originating outside of your computer. Firewalls, typically, are used by businesses that operate computer networks.

6. Use extra security precautions associated with social media – You can become a victim of cybercrime while using social media. Malicious individuals and cybercriminals troll social media platforms to gather and exploit any information that they can obtain on unsuspecting targets. Seriously consider what you post on social media sites like Facebook™ or Twitter™. Avoid revealing confidential information online that can be used by cybercriminals.

Ignore messages or requests from people you don't know. Avoid clicking on unfamiliar links that are sent to you and don't post personal information.

Investigate and understand the privacy settings on the social media platforms you use. Avoid using any application that shares your exact location on the Internet. Disable any services offered by social media that you aren't using.

Use a password manager for your social media accounts as well as for websites that you access regularly. Password managers encrypt the multiple passcodes that you have and stores them. You would only have to remember one password.

Be aware and very cautious when using social media.

You might want to consider purchasing an identity protection service that insures you against any losses you might suffer from identity theft.

7. Avoid visiting "questionable" websites – Many cybercriminals deliberately set up fake and malicious websites to entice and trap computer users and target their system for an attack. Hackers hang-out on the Web looking for targets.

Avoid visiting gambling and pornographic websites. Also, especially avoid visiting sites that offer users free software tools and extensions. They frequently contain malware that can be downloaded onto your computer. The bad guys usually push the idea that the free download is a useful "add on" for major browsers and applications.

Your device(s) could be infected with malware and effectively taken over by malicious users when you install the free tool.

8. Avoid "clicking" on unfamiliar links – Unknown links frequently contain malware (such as key loggers) that could be downloaded onto the hardware of unsuspecting users. They record every key stroke you make and 'phone home' to report back what was discovered on your system. Your "clicking" on such a link would authorize (unbeknownst to you) the downloading of malevolent software onto your computer.

Key logger malware can capture your keystrokes and compromise your computer. The bad guy could possibly gain total access to your information assets.

9. Adjust the security settings on your browser and application software to the highest possible level – Doing so allows you to customize the level of security you want your presence on the Internet to be.

Browsers are basically released with pre-determined security settings (e.g. Javascipt being allowed to run by third party software etc.). The settings remain the same unless

you change them. You should examine your browser settings and disable any that you don't want.

Controlling browser settings require initiative on your part and enhances your security.

10. Terminate or exit your Internet session when you are through browsing - You establish a persistent connection on the Internet when you log-on. Cyber criminals scan the Internet searching for an open connection. Failing to terminate an Internet session could leave your device vulnerable to malicious users who can enter your computer and exploit any number of known vulnerabilities.

11. Lock your keyboard when you leave your device unattended – Failing to power-down your computer or to lock your keyboard allows passers-by, visitors or third parties to have instant access to your system.

Disabling or locking your keyboard – is a necessity.

Each operating system locks the keyboard in a different way. Check with the manufacturer of your computer, tablet or smartphone and learn how to lock it down.

12. Analyze the cyber threats that you will likely face and address them – You encounter unique threats when you surf the Internet or log-on to social media sites. You also are confronted with threats that emerge from other sources. Each person is unique. Be aware of what can happen to you and take the steps necessary to counter the danger.

A partial list of the threat groups that you might face is shown below:

a. Unintentional human error
b. Malicious code introduced into your system
c. Unauthorized access intended to do harm
d. Third-parties or services that have access to your system
e. Social engineering
f. Cyber criminals and organized crime
g. Commercial espionage
h. Disaffected people or disgruntled employees
i. Destruction by fire, floods or natural disasters
j. Nation states
k. Ransomware
l. Identity thieves
m. Denial of service attacks
n. Email attacks
o. Trojans, worms and a host of other malware attacks
p. Spoofing

Each of the threats mentioned above present unique challenges. Become familiar with them and take steps to face the challenges.

13. Identify any vulnerabilities that exist in your system and eliminate them – Vulnerabilities can arise from a variety of sources. Failing to update your software, for

example, to a new edition of application software can leave open "doorways" to your computer through which cybercriminals can enter.

Listed below are a number of common vulnerabilities:

a. The Internet
b. Connections and cabling
c. Application software weaknesses
d. Backup weaknesses
e. Disinterest in security
f. Failure to destroy outdated information
g. Defective hardware and software
h. Equipment malfunction
i. Weak security software
j. Incompatible hardware and software
k. Lack of appropriate physical protection and controls
l. Misconfiguration of your hardware or software
m. Poor mobile computing practices
n. Password weaknesses
o. Lack of security awareness
p. Unauthorized use of software
q. Vandalism
r. Poor workspace security

14. Turn off any application software services or features that you aren't using – Leaving Bluetooth "on", for example, can be a significant vulnerability. Bluetooth services that are enabled can make it possible for a cybercriminal to connect to your system to cause you significant problems. Security experts recommend that you definitely disable the ability of your Bluetooth to accept incoming communications without your knowledge.

15. Back-up your critical information – You will be attacked by malicious users. It's only a question of when. Backup your information frequently and consider keeping multiple copies of your critical data in different locations. Loss or the destruction of your valuable financial data, photographs or music is devastating.

You can backup your information on a separate storage device in the cloud or other form of storage. One threat alone, ransomware, makes it very worthwhile to maintain a current back-up of all of your information.

Ransomware encrypts your system and data files and the cybercriminal demands payment to give you the key to be able to regain control of your device. The victim who is without backup has very little choice. You should know, however, that if the ransom is paid the victim is without a guarantee that the encryption "key" is given in exchange for the ransom being paid.

16. Change any pre-set or default settings used by your hardware, network and software – Manufacturers and publishers frequently ship products with default passwords and settings. Cybercriminals make it their business to be aware of the automatic or default access codes and settings for different brands of hardware and software. If you fail to change pre-shipped settings the bad guys can exploit the opening and easily gain access to your machine.

Software frequently ships with much of its capabilities (or services) enabled. You should decide whether you want everything left that way.

17. Consider encrypting your data and using a VPN (Virtual Private Network) – Data that is "moving" can be encrypted or scrambled to make it unreadable to anyone who might be able to access and try to steal your information. Should your data stream be intercepted it is useless to the bad guy.

A VPN is an end-to-end encrypted "channel" used to send information to another computing device or network. Upon receipt of the encrypted data it is then decrypted. A VPN may accurately be thought of as a third party solution to encryption.

Make sure, also, that your stored data (that is "at rest") is also encrypted and made unreadable on your storage device.

18. Avoid using public Internet "hotspots" or accessing the Internet at hotels – Malicious crackers routinely monitor public wireless access points and watch for openings to exploit. Computers in hotels are frequently targeted and compromised by cyber thieves. Infected or compromised systems can literally lie in wait in a business

center for an unsuspecting user to activate the malicious software and infect their computers.

19. Avoid downloading tempting free software, opening unknown attachments and information from unknown publishers – Cybercriminals use enticing offers of free software or salacious ads to trick people into "clicking" through and installing programs that contain malware on their computers. Malware, in the form of viruses, Trojans or adware, can be installed (without your knowledge or permission) onto your hardware.

Computer users would be much better off purchasing software to accomplish what they want to do rather than seeking out and installing "free" software.

20. Only share media and files with trusted sources – Media that is owned by others (e.g. an external drive or USB drive) may have viruses and malware installed upon it that can be transferred to your computer by physically connecting it to your computer. Simply, don't share media!

A significant breach of computers at the Pentagon, for example, occurred by means of infected flash drives that were left on the ground in the parking lot. Many people were delighted to find a storage device lying on the ground and they quickly inserted it into

their machines when returning to their work stations. Malware was downloaded and spread to other computers.

You would be wise to avoid sharing any media with others – that includes trusted co-workers and family members. You are simply unaware of where the media has been or what has been stored upon it.

21. Limit the "line-of-site visibility" of your electronic devices from nearby people, visitors or passersby – Cybercriminals can "shoulder surf" your keyboard, screen or "sniff" your communications. Cyber theft can easily occur in cramped quarters. Skilled lawbreakers can steal critical information like passwords and account numbers.

You are better off to avoid logging into your hardware when others are close by (e.g. like in an Internet café or other public hotspot). If you must do so, at least consider encrypting your data as mentioned earlier or use a screen filter that blocks much of the information from being seen on your laptop or tablet's screen.

Summary:

Cyber security is <u>your</u> responsibility.

You must make it a practice to stay up-to-date on developments related to cyber security. Develop an information security mind set. Follow computer security best practices. You must take proactive steps to limit the chance that you become a victim of cybercrime.

Aggressively adopt best practices.

Learn more about computer security and how to protect yourself.

Additional Computer Security Resources:

- Computer-Security-Glossary (www.computer-security-glossary.org) website glossary and articles)
- www.OnGuardOnline.gov
- StaySafeOnline.org (a security website for personal and business)