Securing Your Computer to Maintain Your Privacy [1]

Posted May 17 2012
Revised Jun 07 2018

1. Introduction

Please note that the mention of any specific products does not constitute an endorsement by PRC.

Computer security is the process of preventing and detecting unauthorized use of your computer. Unfortunately, maintaining the security of your computer can be challenging task. Hackers often seem to be one step ahead of computer users, even those who are following the best security practices. However, securing your computer is essential to protecting your privacy, reducing the risk of identity theft, and preventing hackers from taking over your computer.

The best computer security practices require you to take a multi-pronged approach. They involve protecting your sensitive information by preventing, detecting, and responding to a wide variety of attacks.

2. Your Operating System

Your computer's operating system is the main program on your computer. It performs a variety of functions, including determining what types of software you can install, coordinating the applications running on the computer at any given time, and allowing your software applications (web browsers, word processors, and email clients) to operate. When you buy a computer, you are usually also choosing a specific operating system.

Manufacturers typically ship computers with a particular operating system. Most **PCs** ship with the latest version of the **Windows** operating system. The current Windows operating system is Windows 10. **Apple** computers use the Mac operating system (currently macOS High Sierra). Apple will release its newest version, macOS Mojave, later this year.

Windows operating systems traditionally have been targeted with malware more often than other operating systems. This may be due to the larger base of Windows installations, which makes it a more attractive target. However, Apple's Mac operating system is definitely not immune to security flaws. In fact, as more consumers purchase Apple products, malware makers have begun to target the Mac operating system.

Some computer security professionals consider Linux and other lesser known operating systems to be the most secure, primarily because they tend not to be targeted. For those interested in trying out the Linux operating system, many recommend Ubuntu [2], a free, open-source Linux distribution.

No matter which operating system you use, it's important that you update it regularly. Windows operating systems are typically updated at least monthly, typically on so-called "Patch Tuesday." Other operating systems may not be updated quite as frequently or on a regular schedule. It's best to set your operating system to update automatically. The method for doing so will vary depending upon your particular operating system.

If your computer uses Windows XP or Vista as the operating system, it's very important to be aware that Microsoft support for

Windows XP ended on April 8, 2014 and support for Vista ended on April 11, 2017. This means that you will no longer receive software updates from Windows Update, including security updates that can help protect your computer from harmful viruses and malware.

3. Your Internet Browser

Many privacy advocates regard the **Mozilla Firefox** browser as superior to other browsers. One advantage of Firefox is that it is an "open source" program. This allows security professionals to become involved in fixing bugs and building stronger security features. Another important advantage of Firefox is its so-called extensions, which can be used to strengthen Firefox's built-in security and privacy features. Three Firefox extensions that we recommend are NoScript, Disconnect, and HTTPS Everywhere.

NoScript. When you install NoScript [3], executable contents or "scripts" such as JavaScript, Java, Flash, and others, are blocked by default. You can allow these scripts to run on a site that you trust (for example, your bank) through a simple mouse click. You can "whitelist" or authorize scripts for a particular session or permanently if you trust a website.

NoScript helps protect against so-called "drive-by downloads" where simply *visiting* a particular website can cause malware to be downloaded and executed on your computer. Hackers can use programming flaws in browsers to get malware onto your computer via a "drive-by download" without you ever noticing. For example, this can occur when visiting a legitimate site that happens to unwittingly host an advertisement containing malware.

Disconnect. The Disconnect [4] extension can help to block the otherwise invisible websites that track your search and browsing history. It blocks over 2000 tracking sites.

HTTPS Everywhere. The browser extension HTTPS Everywhere [5] ensures that you are connecting to a site through an encrypted connection whenever possible. Without HTTPS, your online activities are vulnerable to eavesdropping and your accounts are vulnerable to hijacking. HTTPS Everywhere makes it easier for you to keep your user names, passwords, and browsing histories private. Sites that encrypt the connection between themselves and your browser are generally identified with an "https" prefix and a lock icon in the address bar.

No matter which browser you use, it's important that you update it as newer versions come out which address security vulnerabilities. The Firefox browser will automatically deliver updates on a fairly frequent schedule, typically every few weeks.

4. Your Software

In the past, computer security experts regarded operating systems as the "Achilles' heel" of computer security. More recently, some experts have come to regard commonly installed software programs as the greater threat to security.

Be cautious when downloading software. Unwanted software may infect your computer if you don't take care when downloading a new program. Be sure to obtain software from legitimate sources and watch for "bundling" of additional unwanted programs with legitimate software.

Java. If your computer has Java installed, the Department of Homeland Security has recommended that you disable it. It's unlikely that a typical computer user will ever need to use Java. Java has been responsible for a large number of malware attacks on the computers of unsuspecting users. You can disable Java [6] easily.

Adobe Flash Player. Many computers have Adobe's Flash Player installed. Users are running an older version of Flash Player that may contain numerous security vulnerabilities. Be sure that you set your Flash Player to update automatically. Flash has largely been replaced by HTML5, which is generally regarded as a safer. Some browsers will automatically block Flash content as a security precaution.

PDF (portable document) readers. Most people use Adobe Reader to read and print portable documents (.pdf files), such as forms and publications. Like Internet Explorer, the Adobe Reader is extremely popular, so it has become a target for hackers. Adobe tends to be slow in patching security vulnerabilities. Many security experts believe that you are safer using alternative document readers.

Update your software regularly. Utilize automatic software updates when available. Personal Software Inspector [7] is a security scanner which identifies programs that are insecure and need updating.

5. Anti-virus and Anti-malware Programs

The term *malware* is short for malicious software. The more common types of malware include viruses, worms, Trojans, spyware, and adware. The damage inflicted by malware may range from minor annoyances to more serious problems including

stealing confidential information, destroying data, and disabling your computer. It's not really necessary for you to understand the technical differences [8] between these threats. There are literally dozens of different varieties.

Anti-virus programs. A virus is simply a computer program. It can do anything that any other program you run on your computer can do. A computer virus is a program that spreads by first infecting files or the system areas of a computer and then making copies of itself. While some viruses are harmless, others may damage data files, some may destroy files, and others may just spread to other computers.

Detailed reviews of anti-virus software are available from AV Comparatives [9], an independent anti-virus software testing organization.

Anti-malware programs. Malware is a broad category of computer threats including spyware and other unwanted programs that may be installed without your knowledge or consent. Spyware can secretly gather your information through your Internet connection without your knowledge. Once spyware is installed, it may deploy numerous files onto your system. Some of these files are so well hidden that they are difficult to find and remove.

Spyware programs may be included with other software you want. When you consent to download a program, such as a music sharing program, you may also be consenting to download spyware. You might not be aware that you agreed to the spyware installation because your consent is buried in an end-user-license agreement (EULA).

Be cautious about clicking on pop-up boxes. Spyware programs may create a pop-up box where you can click "yes" or "no" to a particular question. If you click on either choice your browser may be tricked into thinking you initiated a download of spyware.

Anti-virus and anti-malware programs are important elements to protecting your information. However, they are not guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk. Some anti-virus programs also contain anti-malware capability. However, given the increasing sophistication of malware programs, it's best to use two different anti-malware programs in addition to an anti-virus program. Each one looks for slightly different sets of threats, and used together they may offer increased security.

According to a *Consumer Reports (CR)* article [10], free programs should adequately protect most computer users from malware. Consider paying for software mostly for convenience and some extra features. The best free package in CR's security software ratings was Avast! Free Antivirus [11].

Security software will only protect you against the newest threats if it is kept up-to-date. That's why it is critical to set your security software to update automatically.

6. Firewalls

Any computer that's online will find its ports being scanned from other computers looking for vulnerabilities. It's therefore important to have a firewall. A firewall helps to prevent data from entering or leaving your computer without your permission. It helps make you invisible on the internet and blocks communications from unauthorized sources.

Every computer that is connected to the internet should run a firewall at all times. There are two types of firewalls—software and hardware. You can run both simultaneously. In fact, it is a good idea to use both a software and hardware firewall. But never run two software firewalls simultaneously.

Some operating systems have built-in **software firewalls**. An example of a software firewall is the one built into most Windows operating systems. You should leave the Windows firewall turned on unless you replace it with third-party firewall software. Other software firewalls are supplied by outside vendors, or may be part of a commercial security suite. A software firewall must be properly configured in order to be effective.

Hardware firewalls can be purchased as stand-alone products or may be found in broadband routers having firewall features. A router sits between your modem and your computer or your network. It is hard to hack your computer or a network when it is hidden behind a hardware firewall box. However, it is important to properly configure your router, particularly by changing the default password to one that is difficult to crack. To ensure that your hardware firewall is properly configured, consult the product documentation.

7. Tips for Using Your Computer Safely

Beware of email attachments from unknown people. Don't open unexpected email attachments from unknown persons. Just because an email message looks like it came from someone doesn't mean that it actually did. Scammers can "spoof" the return

address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. To open an attachment, first save it to your computer and then scan the file with your antivirus software.

Don't click on links embedded in email messages. It's usually safer to go to the company's website directly from your browser than by clicking on a link in an email message, unless you are absolutely certain that the email was actually sent by the person or company claiming to have sent the message. This will help you avoid becoming a victim of "phishing". **Phishing** is the fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity. Phishing is typically carried out by email and often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Spear phishing is a type of phishing attack that appears to be from a colleague, employer or friend and includes a link or something to download. Spear phishing often targets senior executives at organizations that may have valuable information stored on their computers. These messages may be personalized with publicly available information about the recipient to make them look genuine. They are therefore more difficult to detect than ordinary phishing. The links or downloads included in such a message can be malicious, and might include viruses or fake websites that solicit personal information.

No matter how official an email message looks, never access a financial account by clicking on an embedded link. If the email is fraudulent, a scammer could use the account number and password you enter to steal your identity and empty your account. One way to protect against this is to use an incorrect password on the first try. A phishing site will accept an incorrect password, while a legitimate site won't. You should also avoid calling any telephone number in an unsolicited email unless you have confirmed that it is a legitimate number.

Passwords. Passwords are frequently the only thing protecting our private information from prying eyes. Be sure to use a strong password computer's user account and your router or modem. Never use the default password that comes with a router or modem.

In addition, many websites that store your personal information (for example web mail, photo or document storage sites, and money management sites) require a password for protection. However, password-protected websites are becoming more vulnerable because often people use the same passwords on numerous sites. Strong passwords can help individuals protect themselves against hackers, identity theft and other privacy invasions.

Whenever you have an opportunity to create and use a password to protect your information, make sure that you use a strong password [12]. In most instances, it's safe to ignore admonitions to regularly change your passwords. While once considered a security "best practice", changing your passwords regularly ranks relatively low as a means of protecting your accounts. Of course, if you believe that your password has been breached or compromised, it is essential to change it immediately.

Password recovery methods [13] are frequently the "weakest link", enabling a hacker to reset your password and lock you out of your account. Make sure your security questions aren't easily answerable. It's also a good idea to have your password resets go to a separate email account designed for resets only.

Unfortunately, experts warn that the security of passwords has never been weaker. New hardware and techniques have contributed to a sharp rise in password cracking by hackers. Our Online Privacy guide [14] contains a list of password "dos" and "don'ts".

Account privileges. Do not log into a computer with administrator rights unless you must do so to perform a specific computer maintenance task. Running your computer as an administrator may leave your computer vulnerable to security risks.

Keep your software up-to-date. Computer hackers are always finding new ways to penetrate the defenses of your software programs. Software vendors respond with patches that close newly found security holes. To stay protected, you need to download and install patches for both your operating system and your software applications whenever they become available. Software patches or updates often address a problem or vulnerability within a program.

Sometimes, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. It is important to install a patch as soon as possible to protect your computer from attackers who would take advantage of the vulnerability. Attackers may target vulnerabilities for months or even years after patches are available. Some software will automatically check for updates. If automatic updates are not available, check your software vendors' websites periodically for updates.

Shut it down. Shut it down, lock, log off, or put your computer to sleep before leaving it unattended. Make sure that your computer requires a secure password to start up.

Protect sensitive information. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. Don't send sensitive information over the internet before checking a website's security.

Avoid social engineering attacks. Social engineering can be defined as the process of obtaining information from other people through the application of social skills. The objective of social engineering is to deceive the computer user into compromising his/her system and revealing sensitive information.

Social engineering ploys take advantage of human nature by tricking people into installing malware or revealing personal information. The user is tempted to carry out a necessary activity that damages their computer. This occurs when the user receives a message directing him/her to open a file or web page or watch a video. Often, these ploys relate to celebrities, natural disasters, or popular events.

One common trick includes showing a fake virus scan that indicates your computer is infected and encourages you to download a tool to remove the infection. Another ploy offers to display a video, but only after you install a plug-in that is "required" to view the content.

Back up all your data. While your computer may be an expensive asset, it is replaceable. However, the data and personal records on your computer may be difficult or impossible to replace. Whether or not you take steps to protect yourself, there is always the possibility that something will happen to destroy your data. One important risk to your data is **ransomware**. Ransomware can prevent you from accessing your data by locking your computer's screen or locking your computer files unless you pay a ransom. Ransomware can be downloaded onto your computer if you visit a malicious website or open a malicious email attachment.

There are many hardware and software alternatives for backing up your data including USB flash drives and external hard drives (hardware) as well as archiving and disk imaging programs (software). Each method has its own advantages and disadvantages. For a simple solution, important files can be saved to an encrypted USB flash drive. It's a good idea to keep your backup media in a locked and secure location.

Encrypt files on your computer, laptop or portable device. Encryption is a way to enhance the security of a file or folder by scrambling the contents so that it can be read only by someone who has the appropriate encryption key to unscramble it.

Computers are lost, stolen or hacked every day. As a result, your personal information can become available to anyone and may lead to privacy invasion and identity theft. Many computers and other devices contain sensitive files such as financial records, tax returns, medical histories, and other personal files.

Many computer users rely on laptops and other portable devices because they are small and easily transported. But while these characteristics make them convenient, they also make them an attractive target for thieves. Make sure to secure your portable devices to protect both the machine and the information it contains. It's important to encrypt any sensitive data on such devices.

USB flash drives pose security risks for similar reasons. Use them cautiously. Some flash drives offer built-in encryption features.

Unencrypted files on your computer can be read by anyone *e*ven if your computer is password protected. There are methods by which a person who has physical access to your computer can read unencrypted files without entering your password. So it's important to encrypt sensitive files even if they are on a password-protected computer.

How to Encrypt All Your Data [15] provides seven tips for encrypting the data you store and share across your devices and the internet. Are Your Online Messages Safe? [16] focuses on messaging apps that use end-to-end encryption.

8. Resources

Privacy Rights Clearinghouse Consumer Guides:

· *Online Privacy: Using the Internet Safely [17]*

· *Online Shopping Tips: E-Commerce and You [18]*

· *Social Networking Privacy: How to be Safe, Secure and Social [19]*

U.S. Government Resources:

The U.S. Computer Emergency Readiness Team [20] (U.S. CERT) offers numerous computer security resources. It's Tips Page [21] is especially useful.

The Federal Trade Commission's *Start with Security: A Guide for Business [22]* describes 10 practical lessons businesses can learn from the FTC's data security settlements.

Other Useful Resources:

Krebs on Security [23] provides many useful resources including *Tools for a Safer PC [24]* and *Krebs's 3 Basic Rules for Online Safety [25]*

California Attorney General, *Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents [26]* (February 2014)

Source URL (modified on June 7, 2018): https://www.privacyrights.org/consumer-guides/securing-your-computer-maintain-your-privacy

Links
[1] https://www.privacyrights.org/consumer-guides/securing-your-computer-maintain-your-privacy
[2] http://www.ubuntu.com/
[3] https://noscript.net/getit
[4] https://disconnect.me/disconnect
[5] https://www.eff.org/https-everywhere
[6] http://www.infoworld.com/article/2613458/web-browsers/how-to-disable-java-in-your-browsers.html
[7] http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/
[8] http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
[9] http://www.av-comparatives.org/
[10] http://www.consumerreports.org/cro/news/2014/04/free-security-software-keeps-you-safe-online/index.htm
[11] https://www.avast.com/index
[12] https://mediatemple.net/community/products/dv/204644370/strong-password-guidelines
[13] http://lifehacker.com/5932501/strong-passwords-arent-enough-how-to-to-ensure-the-apple-and-amazon-exploit-never-happens-to-you
[14] https://www.privacyrights.org/consumer-guides/online-privacy-using-internet-safely#passwords
[15] http://www.dailydot.com/layer8/encrypted-email-messaging-apps/
[16] https://www.privacyrights.org/blog/are-your-online-messages-safe
[17] https://www.privacyrights.org/fs/fs18-cyb.htm
[18] https://www.privacyrights.org/node/1321
[19] https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social
[20] http://www.us-cert.gov/
[21] https://www.us-cert.gov/ncas/tips
[22] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
[23] https://krebsonsecurity.com/
[24] http://krebsonsecurity.com/tools-for-a-safer-pc/
[25] https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/
[26] http://oag.ca.gov/cybersecurity