



Easy Steps to Improve Your Computer Security

1. Install and Use Antivirus and Antispyware Software.

Installing an antivirus and antispyware software program and keeping it up-to-date is a critical step in protecting your computer. Antivirus and antispyware software can detect the presence of malware by looking for patterns in the files or memory of your computer. They use virus “signatures” provided by software vendors to look for malware. And because new malware is discovered daily, vendors provide new signatures often, generally every week. An out-of-date antivirus scanner is only marginally better than no scanner at all, so make sure your solution auto-updates and check that it automatically scans your device regularly — every week or so is good.

If you don’t currently have one in place, make sure to do some research. Most free anti-virus solutions are as effective as the purchased ones. If at all possible, make sure the solution you use scans all downloads automatically for malware. Be aware that some programs are definitely easier to set up than others and some so dominate your computer’s system that it bogs down, so read reviews before selecting your solution.

NOTE: It is *not* a good idea to have two different antivirus products installed at once, because they tend to fight with each other. More is not merrier when it comes to antivirus solutions.

2. Make Sure Your Firewall is on.

Almost all modern devices — computers, tablets, smartphones, and the like — include a firewall. And these days, most devices have the firewall set to “on” or “enable” by default, which is a good thing. Refer to your user’s guide for instructions on how to verify that your firewall is enabled and properly configured.

3. Apply Software Updates and Enable Automatic Updates.

Software needs regular updating, either to add functionality or to fix security vulnerabilities. Because hackers can exploit software bugs to attack your computer, keeping your software updated is a very important step to help prevent infection.

When most people think of patching, they think of the operating system. If you have a Microsoft device, make sure that Windows Update is turned on; if you have an Apple device, use Software Update — these tools will insure your operating system is fully patched and you’ll get updates automatically.

But your device’s other software or “apps” also need to be maintained. Whether Microsoft Office, Java, Adobe’s Acrobat Reader, your favorite web browser, or anything else, they all require periodic patching. Check under the application’s “Help” or “About” tab for an update button or go to your software vendors’ website to check for and install all available updates. Then enable automatic updates if possible; otherwise, make a habit of checking on a regular basis — maybe quarterly.

Be aware of your sources: only download software updates directly from a vendor’s website, through automatic updating, or directly through the application’s “Help” or “About” tab.

4. Remove Unnecessary Software.

Since hackers generally attack computers by exploiting software vulnerabilities, the less software you have installed, the fewer ways hackers can get in. Plus, when you uninstall software you don't use, you provide additional space for the software and files that you really do use.

So check to see what software is installed on your computer. Most computers come with lots of unnecessary software you may never use. If you don't know what a software program does and don't use it, research it online to determine whether it's necessary. Then uninstall any software you don't use.

5. Back up Your Data.

Because accidents happen and hackers are at work, your best defense against the loss of your family photos, music library, tax returns, resume, and all the other files you have is to make a backup that isn't stored on your computer. In today's world, use a USB device – a flash drive or portable hard drive – or a “cloud solution” to back up all your important files. Make sure to do this regularly, once a week or every few weeks. If you use a cloud solution, you may be able to automate the process.

Remember, once you're hacked or infected, it may be too late. Back up your data today.

6. Use Good Passwords.

Passwords don't need to be hard to remember; they just need to be hard to guess. So only use strong passwords: those that have ten or more characters, a variety of uppercase and lowercase letters, and at least one symbol and number. Don't use passwords based on information people can easily find online, like your birthday or anniversary, your child's name or grandmother's. Password cracking software uses entire dictionaries in seconds in what's called brute-force attacks, so don't use words found in a dictionary, though combinations like “cucumbesrock” might work, especially if you then incorporate numbers and symbols, as in “cucumber\$rock.” The longer and more complex a password is, the harder cracking tools have to work. Don't be an easy target.

Websites including banks, social media, and webmail use security questions for both password retrieval/reset and for sign-in verification. When setting up your answers to these security questions, choose questions for which it is unlikely that an internet search would yield the correct answer; better yet, make up a nonsense answer. What's your mother's maiden name? “Pizzaglu%” What was your first pet? “Pizzaglu%” Where were you born? “Pizzaglu%.”

And finally, avoid “cascading hacks” — where bad guys steal or crack credentials from one account and use them to crack dozens of others. You can prevent this from happening to yourself by doing two things. First, use a different password for every account you have. And second, to help manage all those passwords, use a password manager or “vault.” This is just a little encrypted database of all your passwords that you can store on your computer, your smartphone, a USB flash drive or even in the “Cloud.” Password managers take the pain out of remembering hundreds of unique passwords by doing that for you. All you need remember is one master password and your password manager will take care of the rest. There are many free ones available, and some excellent ones you can purchase. Simply search online for “password manager” to find one that's right for you.

7. Learn to Spot Phishing and Spam.

Spam is the number one way hackers spread malware and it comes in many varieties, from ads for pharmaceuticals to nonsense gibberish and worse. While some is just anonymous advertising, a surprising percentage of that unwanted

email is really designed to compromise your computer, access your bank account or steal your identity, generally by getting you to do one of two things:

- clicking on links embedded within the messages, which may take you to harmful websites.
- downloading infected attachments, which only appear to be zip files, Word documents, PDF's images, or whatever. Remember that innocent-looking files can be dangerously infected.

Phishing is hackers' favorite way to compromise a computer. "Phishing" refers to an attempt to get you to divulge sensitive information – usernames and passwords, credit card information, your social security number, etc. – by tricking you into thinking you're in communication with a trustworthy person or organization, from the IRS to UPS, your bank to LinkedIn, the Red Cross to Microsoft. It can be very difficult to know who's really sending these messages and the fake ones can look remarkably real.

So, to protect yourself, don't open attachments or click on links in email unless you're certain they're safe, even if they come from a person you know. If the sender's a friend or colleague, why not give them a call or email asking what it's about? If it appears to come from a business, call Customer Service or check their official website by entering the mail website address in the address bar, rather than clicking on the link. Be especially wary of attachments with sensational names, emails that contain misspellings, or ones that try hard to get you to click on a link or attachment urgently (for example, "Password about to expire!" or "Provocative pictures" or "Act now for free iPhone.").

8. Secure Your Web Browser. An increasing number of hacker attacks take advantage of web browsers, so before you start surfing the web, secure your browser by doing the following:

- Investigate browsers and install the one you find is most secure, responsive, and reliable. Don't just settle for whatever came with your computer.
- Always ensure you're using a secure website whenever submitting credit card or other sensitive information via your browser. Look for "https:" (the "s" is for "security") and other signs, such as a lock icon. (Signs of security vary depending on which browser you use.)
- Disable Java, JavaScript, Flash, and ActiveX on websites you're not familiar with. While a few websites might not work as they should, the vast majority will be just fine and your surfing will be that much safer.
- Disable options to always set cookies, those little files websites place on your computer. Attackers could log onto a site you've visited — like a banking site — by accessing the cookie with your login information. To prevent this, configure the browser to ask for permission before setting a cookie, allow cookies for sessions only, and disable features that keep you logged in to a site or that retain information you've entered.
- If you're using Internet Explorer, set the security levels for trusted sites (websites you most often visit and trust) to the second highest level. At the highest level, websites may not function properly.

9. Restrict User Privileges

On a Windows or Linux computer, there are various kinds of user accounts. While the "administrator" can install software and hardware, configure security settings, and make changes to the operating system and all its various settings, "standard" user accounts are more limited. While they can use all the installed software and customize their profile, they can't make changes to the computer system as a whole. Using standard accounts can protect your computer by preventing users from making changes that affect everyone.

Log in as administrator and set up standard accounts for you and for each person who'll use the computer, and then only use the standard accounts, making sure to password-protect each account (with different passwords, of course). Then, if you need to make a major change to the system, like installing a program or an update, you'll be prompted for the administrative account information; simply enter it and you'll be able to complete the action. And think twice about sharing the administrative password with your game-paying, curious teenager.

By limiting privileges, you'll find that there's a lot less to worry about. You'll be better protected against "drive-by downloads," where malware gets installed just by opening an infected website, and other kinds of attacks just because the hackers won't have administrative access to your system.

10. Secure Your Home Network

Once your computer is connected to the internet, it's also connected to millions of other connected computers, which could allow attackers to connect to your computer. Information flows from the internet to your home network by first coming into your modem or router — these days, most people have a single device that is both — and finally to your computer. So be sure your router is secure.

To make the following changes, you can consult the user's guide, go to the manufacturer's website, or check YouTube for instructions. You'll discover that the default configuration offers little security (though things are slowly improving) but a secured router is one of your best lines of defense.

To secure your router, use a network cable and connect it to your computer, then open your browser and go to a predefined URL or IP address — again, check those resources — where you can do the following:

- Because the router's administrative credentials are published in manufacturer's guides and on-line, change the default login username and password and make the password extra-long.
- Disable the ability to administer the router wirelessly. That way, a hacker would have to be physically connected to your home network to change your settings.
- The SSID is the network name that your wireless router broadcasts. And because it's being broadcast, change it to something meaningless — not your name, not your address, not the brand of the device; try something like "tomato," "leaveusalone," or "cobblestone." You'll know what it means, but no one else will.
- Configure your router to use WPA2-AES encryption. It's the only encryption that's hard to crack.
- Make sure the firewall is turned on.
- Consider using an alternate DNS provider, such as OpenDNS, to filter out malicious webpages.

Great General Security Resources

- StaySafeOnline.org — Simple steps, practices, and resources you can use to learn the basics on how to better secure their home computer from cyber threats.
- OnGuardOnline.gov — This web site provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.
- FTC [Tips & Advice](http://FTC.Tips&Advice), The Federal Trade Commission is a major source of information about identity theft and how to avoid scams and protect your rights.
- [Stop Think Click](http://StopThinkClick), 7 Practices for Safer Computing — Excellent general information for keeping your family and friends safe online, from NIST, the National Institute of Standards and Technology
- ["Phishing" Fraud](http://PhishingFraud): How to Avoid Getting Fried by Phoney Phishermen, a helpful description of what to look for and how to protect yourself, from the U.S. Securities and Exchange Commission