

Essential Security Measures for Home Computers

Created by Corey Keating

Here is a list of security measures that I strongly recommend for all home computer users (both Microsoft Windows and Apple Macs). These items are crucial if you do any online banking or keep personal information on your computer or don't want to permanently lose all your computer files and data (which means everyone!). Don't become a victim of identity theft! If these categories do not already include you and you don't think the information on your computer is important, then please **be a responsible computer user! By not maintaining basic security on your PC, you are most likely allowing your computer to act as a zombie, controlled by hackers to perform large-scale attacks on other computers** (by background processes you are not even aware of). Many hackers today are coordinated teams involved in multi-million dollar hacking/scamming businesses. The power of the hacker at disrupting businesses and Internet communications comes from the ability to use large numbers of zombie computers in coordinated attacks against others. Don't unwittingly and unknowingly allow yourself to be a part of their scheme!

Please be aware that this document only covers laptop/desktop computers, not mobile devices, such as SmartPhones, iPads, etc. Be very cognizant of the fact that these types of devices also need to be kept secure. If you keep personal info on these devices and they are compromised or stolen, your computer accounts may also be at risk and you may suffer identity theft.

I urge you to employ these technologies and practices on your home computer. I welcome all feedback.

Executive Summary/Checklist (see corresponding number below for more details)

Do These NOW!

- 1, 2, 3) Windows Computers: Run antivirus, antispyware, and a software firewall.
- 4) Backup your Data (regularly!)
- 5) Update your Operating System
- 6) Hardware firewall for home Internet connections
- 7) Wireless networking: do wireless encryption and change password on wireless access point/router

Other Critical Items

- 8) Be very careful when using public WiFi; only connect to known providers. You should use a VPN if doing banking, online purchases, or sending personal information in a public location.
- 9) Use strong passwords for all online accounts (especially financial ones) and don't use the same password for all your accounts (see suggestions for creating strong passwords). Use a program that encrypts your passwords.
- 10) Use the free Web of Trust software that will rate every website you visit and warn you of dangerous sites. The greatest single attack vector, even for the Mac computer, is your web browser. Firefox with NoScript.
- 11) Take care of physical security, especially in public locations

Be Smart Online - Very Important Security Considerations (Your Actions!)

- 12) Don't believe a website pop-up that tells you that you have a virus and urges to you "click here" to scan/clean. Use your already-installed, trusted antivirus program.
- 13) Only make online purchases from reputable sites (usually providing a phone number) and that offer purchases with "https".
- 14) Understand Phishing and don't fall for it; e.g. your bank will NEVER ask for your password!
- 15) Don't open attachments in email from people you don't know; and be cautious about email attachments from people you do know.
- 16) Don't forward "urgent/important" emails without first verify the information, e.g. www.truthorfiction.com
- 17) Consider the answers you use to password recovery services (i.e. "Forgot your password?").

Protect your Children (and other Loved-Ones) - Online Accountability

- 18) Children are vulnerable and often their innocence leads them to give out personal info online to those seeking to harm them. Follow the steps recommended here to be aware of their online actions, especially on social networking sites like Facebook.

Further Suggested Measures - These may make your life easier!

- 19) Protect your computer and electronic equipment from electrical problems.
- 20) Recycle your computer the right way, deleting all personal information first.
- 21) Protect any sensitive data you keep on flash drives or backups - consider encrypting it.
- 22) Special considerations for traveling with a laptop
- 23) Consider signing up for an Identity Theft Protection service.
- 24) Use the free software Secunia to help find and update out-of-date software on your computer.

See the Sections below providing online [Resources for Research](#) on any of these topics and [Further Considerations for Small Businesses](#).

-----The DETAILS-----

Absolute Necessary Measures for Microsoft Windows Computers:

- 1) Run a reputable anti-virus program, with updated definition files. (You should update your virus definition files once a week, if not daily. Most programs allow for automated updates.) Some programs I would suggest are Microsoft Security Essentials, McAfee Antivirus, Trend Micro PC-cillin, or Norton Antivirus.
 - a) It is **best** to use a security suite from a reputable company that combines anti-virus, anti-spyware, software firewall, spam filtering, etc. (**Includes #1, 2, & 3 of this list.**) Some excellent options are ZoneAlarm Internet Security Suite, McAfee Internet Security Suite, Panda Internet Security, Kaspersky Internet Security, or possibly Norton Internet Security. (I highly recommend and prefer **ZoneAlarm Internet Security Suite**; I *don't* prefer Norton's Suite and will never use it again.)
 - b) Some good **free** antivirus-only programs are Microsoft Security Essentials (www.microsoft.com/en-us/security_essentials/), AVG Anti-virus Free Edition (free.avg.com), Avast Antivirus (http://download.cnet.com/Avast-Free-Antivirus/3000-2239_4-10019223.html), or Avira Antivir (http://download.cnet.com/Avira-AntiVir-Personal-Free-Antivirus/3000-2239_4-10322935.html)
- 2) Run anti-spyware software. Microsoft's Windows Defender is a must for Windows-users. In addition, you should *periodically* also run Malwarebytes (www.malwarebytes.org), and/or possibly one of these: Lavasoft's Ad Aware, Webroot's Spy Sweeper, (or Spybot's Search & Destroy, or Javasoftware's SpyBlaster): most of these can be downloaded for **free**.
- 3) If you use a laptop that you connect to the Internet outside of your home/office or you do not have a hardware firewall for use at home, then you must run a software firewall, such as ZoneAlarm (my preference), McAfee Internet Security Suite, or Norton Internet Security (not my preference).
 - a) Excellent **free** firewall options: Comodo Firewall Pro (and anti-virus) personalfirewall.comodo.com OR PC Tools Firewall Plus from www.pctools.com/firewall/ OR ZoneAlarm Free Version from www.zonealarm.com

Absolutely Necessary Measures for All Computers (Macs and MS Windows PCs):

- 4) Keep all your data in one location on your computer (e.g. My Documents) and back it up regularly. (As an added protection, consider keeping a copy offsite in the event of a major disaster).
 - a) Be sure to backup emails and Internet "Favorites" if those are important to you.
 - b) You can backup to an external hard drive, on CDs/ DVDs, USB flash drives, or via an "online backup". Be aware that backups contain personal info that needs to be guarded.
 - c) For help in creating and implementing a backup plan, see my document, "**A Simple Backup Strategy for Home Computers**" available from www.computersecuritynw.com

- 5) Keep your operating system (e.g. Windows XP/Vista, Mac OS X) updated with all the latest security patches. (For Microsoft Windows users, go to windowsupdate.microsoft.com.) You can also allow settings to automatically update your computer, or ask/inform you of updates.
 - a) Also keep your other application programs updated periodically (especially ones such as Adobe Flash, Java, Internet Explorer or Firefox, MS Office, etc.)
- 6) If you have a fulltime connection to the Internet, such as through DSL or Cable, then you should get a hardware firewall. (Ask at your local computer store. These are often referred to as home "routers".)
 - a) Change the default password on all networking hardware/equipment (or a hacker will for you!). Do this NOW! Hackers can re-route all your network traffic without you even knowing about it. This can result in your banking and other personal information being stolen.
 - b) If you have a device that will allow you to connect multiple computers to the Internet through your cable modem (or DSL modem) then it probably already includes a hardware firewall and provides adequate protection for home use (by using "NAT" technology).
- 7) If you have wireless networking (WiFi) at home, then (1) you need to enable the strongest wireless encryption technique that your equipment will support. The best is WPA2-PSK with a very strong password (long passphrase), but you can use WEP. (You will see these options if you enable encryption on your wireless router.) If you don't do this, you probably have your neighbors (or criminals in their cars) connecting to your network. At best, they are using your connection bandwidth; at worst, you have given them open access to all information on your home computers.
 - a) You must also (2) change the default administrator password on your wireless routing device.
 - b) Note that "WEP" can be easily broken by any persistent hacker, but it will keep your neighbors honest and you are probably safe enough on a home computer if this is all your equipment currently supports - but consider upgrading so you can use WPA2-PSK.

Other Critical Security Precautions:

- 8) Be VERY cautious when you connect to **public WiFi** access points! Only attach to what you know is the WiFi offered by a local business/coffee-shop you trust; NEVER attach to a WiFi point named "Free WiFi" unless you know who is offering it, especially in high traffic areas like airports.
 - a) Furthermore, never do your **online banking** or make **online purchases** in a public place (unless using a VPN-see below). Be VERY careful about doing ANYTHING that sends your personal login information/password in a public location, unless using a VPN.
 - b) A VPN is a "Virtual Private Network" that encrypts all your network traffic and makes it secure, even in a public location. You need to contract with a VPN service provider. I use and recommend StrongVPN: <http://strongvpn.com/>, which works all over the world, costs \$55/year [or monthly contract], works with Windows/Mac/Linux/iPad/iPod/Smartphone/etc., has excellent tutorials, great tech support, etc. (I have also read good things about Wifi Guardian, but not used them: www.hotspotguardian.com/ \$50/year: Windows Only. US and UK only)
- 9) **Manage your passwords.** Use "strong" passwords for all accounts, especially your financial ones. For some great suggestions on "easy to remember" but "difficult to crack" passwords, see how to "Create a strong, memorable password in 6 steps" at www.microsoft.com/protect/yourself/password/create.mspx
 - a) Do NOT use the same passwords for all your accounts! (However, you can use the same strong base password and modify it slightly for different programs, websites, etc.)
 - b) Do NOT keep your passwords in an unencrypted document on your computer!
 - c) Use a password encryption program to store all your passwords (for bank accounts, websites, etc).
 - i) Simple, free program: KeePass (Windows: www.keepass.info ; Mac: www.keepassx.org)

- ii) If you have a Smartphone/iPhone, consider a version that will keep passwords on these devices in-synch with those on your computers, such as:
 - * "RoboForm Everywhere" (for-pay for multi-platform - www.roboform.com), or
 - LastPass (free for single platform / for-pay for multi-platform - www.lastpass.com), or
 - 1Password (mainly for Mac & SmartPhones - agilebits.com/products/1Password/)
 - iii) You might also want to keep all serial numbers of software and other info in this program.
- 10) Your **Web Browser** (Internet Explorer, Firefox, Safari, etc.) is one of the greatest attack vectors for your computer (even for Macs). I HIGHLY recommend you install the "Web of Trust" software (www.mywot.com). It gives you ratings for every website you visit and will advise you as to how safe they are. You need to download a separate version for each different web browser.
- a) For general web browsing (going to sites you don't know/trust), do not use Internet Explorer (IE); instead use Firefox with the NoScript plug-in (www.noscript.net), or use Google Chrome.
- 11) Over 75% of all identify theft is due to **physical theft** of wallet/purse/personal identification or physical theft of your computer. Physical security is important! Consider purchasing Lifelock (below). Details at this article: www.net-security.org/secworld.php?id=8461
- a) If you travel a lot or are especially concerned about physical recovery of a stolen laptop (or remote data deletion), consider LoJack software for your computer: www.absolute.com/products/lojack

Be Smart Online - Very Important Security Cautions and Actions:

Remember, YOU (your actions) are the most vulnerable aspect of a completely secure computer. :-)

- 12) If you click on a website and a pop-up comes up telling you that your computer is infected with a virus and they can clean it for you, don't believe them! Chances are this is another scheme to get you to install a virus. See here for more info: www.symantec.com/norton/theme.jsp?themeid=mislead
- 13) Only make online purchases from reputable companies and always use your credit card; most credit card companies protect you from bearing the cost of any non-authorized purchases or at least limit any possible financial losses. (Most reputable companies will give you a phone number to contact them.)
 - a) Only purchase from sites that provide "secure transactions". The URL in a secure transaction will start with "https", not just "http". (Also, the little 'lock' in the bottom right-hand corner of your browser should appear locked. These transactions are using SSL encryption and no one should be able to read your credit card number in transit.)
- 14) Don't be caught in a "phishing" scam, where people steal your personal information for identity theft or other nefarious purposes. That is, **NEVER** click on links in emails sent to you supposedly from your bank, eBay, PayPal, or other institutions asking you to logon and verify your information. **Your bank has no reason to ever ask you to verify your login or account information and will *never* do so. I know people who have responded to supposed emails from their bank and have literally lost all the money in their bank account!** If you think it might be legitimate, open your Internet browser and go the site you know is legitimate or **call** your financial institution. For more info, please check out www.occ.gov/consumer/phishing.htm.
 - a) See <http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx> and Six Simple Ways to Avoid Scams and Phishing: www.addictivetips.com/miscellaneous-tips-and-news/6-simple-ways-to-avoid-email-scams-and-website-phishing-attacks/
 - b) If you think you may have been phished/id stolen, go to www.ftc.gov/idtheft/
- 15) Don't get a virus or Trojan program by opening email from people you don't know and trust, especially if they have attachments. Just delete them without opening them. Even if someone you know sends you something, if you have any question about it, confirm with them that they meant to send it to you; it could be a program sending a virus to your friend's email addresses! Furthermore, don't respond to "great sounding business opportunities" sent to you by someone you

don't know - most are not only spam, they are scams that can be used for identity theft. (You can also run a spam filter like the ones that come in most software security suites mentioned above.)

- a) NEVER buy anything advertised in a spam email! The way to put them out of business is to not fund spammers. Even going to a website advertised by spam could compromise your security.
 - b) If you receive an apparently random email from a friend only containing a website address without anything else OR a "check out this business opportunity" email from a friend, it may very well be that their email account was hacked into. (1) Don't click on that link! (2) Let your friend know their account may be compromised. They should at minimum change their password.
- 16) Everyone gets emails about "urgent issues" that sound very legitimate and convincing; many of these are hoaxes and only waste time and resources. Before forwarding these emails that urge you to "send to everyone you know", please check them out at some reputable site such as www.snopes.com or www.TruthOrFiction.com
- 17) Most websites (like your bank or email accounts) have systems for you to recover your password in case you forget them. These "forgot your password" links make easy ways for hackers to steal your passwords. I have been changing all my questions/answers for these Password Recovery services for all of my accounts, especially important ones such as bank, investments, email, etc. For many of the questions I have been "consistently lying" :-). In other words, why put my real "place of birth"? If I know the answer I give for this (made-up, thus not in any public records), then no one can look it up online and take over my accounts. Want to know my favorite color or my pet's name? They are surely not the ones I use for password recovery questions! Please take action on this now (before someone else does!). (It happened to Sarah Palin. Read about it at: www.pcmag.com/article2/0,2817,2330937,00.asp)
- a) BUT, don't forget the answers you use! I keep these "fake" answers in my password encryption program [see below], so I can refer to it in case I forget the answers I give.

Accountability and Protecting Your Children and Loved-Ones:

- 18) The Internet can be a dangerous place for children (or anyone!). There are many online stalkers actively seeking personally identifiable information about your children. Every parent should take the responsibility to actively protect your children. If you have a child old enough to get on the Internet, I urge you to read this recent article from PC Magazine entitled "Do You Know Where Your Kids are Clicking?" at www.pcmag.com/article2/0,1759,1979163,00.asp If that doesn't get you to take action, then just tell your kids to go play in the street. :-). See their "10 Essential Tips for Parents" and "The Best Websites for Keeping Your Kids Safe". You might want to start with these ideas:
- a) Educate yourself and your children about online dangers and appropriate online behavior. (Maybe start here: <http://www.microsoft.com/security/family-safety/default.aspx> or www.netmartz.org or www.ftc.gov/bcp/edu/pubs/consumer/tech/tec08.shtm)
 - b) Put your computer in a common area of your home, such as in the den, where kids have no expectation of privacy.
 - c) Install software that will filter what your children access, can record Instant Messaging chats, restrict program access, limit the time kids can spend online, and send weekly reports of online activity. I suggest either "for pay" www.BSecure.com or www.SafeEyes.com , or the **free** K9 Web Filtering (<http://www1.k9webprotection.com/>). Although no software is flawless, it helps - and can provide some valuable accountability.
 - i) x3watch (<http://x3watch.com/>) is **free** software that offers accountability without filtering; we can all benefit from accountability!
 - d) Be aware of what kind of personal information your kids post on **Social-Networking sites** like Facebook or MySpace; they may be unknowingly leading a stalker to their school or your house.

Parent's Guide to Social Networking Sites: www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm

Six simple steps for social networking protection: www.net-security.org/secworld.php?id=7952

- i) For **Facebook protection**, consider installing Social Networking protection, like ZoneAlarm's SocialGuard (read about here: <http://www.pcmag.com/article2/0,2817,2383917,00.asp>) and read <http://www.squidoo.com/protect-your-children-on-facebook>
- e) What Parents Should Know about Safe Console **Gaming**:
www.pcmag.com/article2/0,2817,2337749,00.asp

Further Suggested Measures:

- 19) At a minimum, use surge suppressors to protect all your electronic equipment from normal power surges. Even better, you can use an Uninterruptible Power Supply (UPS) that will allow you to use your computer even if you lose power at home ("blackouts") and protect hard drives from crashing during power "brownouts".
- 20) Recycle Your PC the Right Way: www.pcmag.com/article2/0,1759,2276111,00.asp "Don't just toss out your old machine when you buy a new one. Here's the eco-friendly way to get rid of old hardware." Summary: 1) **Backup your files**, 2) **Wipe your hard drive clean**, 3) Salvage what you can, 4) Find a reputable recycling location (like BestBuy), and 5) Spread the word.
- 21) If you store sensitive information on your computer (especially on a laptop) or a flash drive, please read about using private key encryption software under the section for small businesses below.
- 22) If you leave the house with a **laptop** computer, you need to take special security measures. First of all, laptops are more prone to being lost, dropped, stolen, etc. You should be sure to backup your data more frequently and especially before going on trips. There are thousands of laptops stolen each week at airports. You need to provide physical security to protect your laptop from being stolen. I lock my laptop to a table when at a coffee shop. Here are some general security tips for keeping your laptop safe: www.ftc.gov/bcp/edu/pubs/consumer/tech/tec03.pdf . For extra tips when traveling see: http://advice.cio.com/al_sacco/lax_laptop_security_at_the_airport_how_not_to_become_a_statistic
- 23) Consider signing up for an identity theft monitoring service like LifeLock (www.lifelock.com) [which is what I use], Zander Insurance (www.zanderins.com/idtheft/idtheft.aspx), or Trusted ID.
 - a) Compare services and sign up at this website to get a discount: www.identitytheftlabs.com
 - b) Some great identity theft information sites: www.allaboutidentity.com/ or www.idtheftcenter.org/
- 24) Consider using Secunia, which is a free program that detects vulnerable and out-of-date software and assists in downloading updates: http://secunia.com/vulnerability_scanning/personal/ - Even if you have your operating system updates turned on (which is critical; see #5 above), many times your system has vulnerabilities that come from other software you have installed on your system, such as programs that enhance your web browsing experience (like Adobe Flash, or Adobe AIR). You may not even know you have these program installed and you may not realize how important they are to keep updated! This is especially true for Mac computers.

Other Excellent Resources for More In-depth Information

- 1) Hacker Proof: Guide to PC Security: <http://www.makeuseof.com/tag/download-hackerproof-guide-pc-security/>
A no-nonsense, easy to understand guide that provides a history of and terminology related to PC security, what security options to run, backing up, how to recover from malware, etc.
- 2) UK's government's initiative on staying safe online. Excellent source of consumer related **videos**, tips, etc: www.getsafeonline.org
- 3) See this link for specific security suggestions for Windows Vista, XP, and for Macintosh computers:
Securing a Personal Computer: safecomputing.umn.edu/studentchecklist.html
- 4) More Wi-Fi Security Tips: www.techrepublic.com/blog/security/10-wi-fi-security-tips/364 or www.practicallynetworked.com/support/wireless_secure.htm or <http://www.appolicious.com/tech/articles/7737-five-ways-to-protect-your-wi-fi-network-from-hackers>
- 5) www.webopedia.com/TERM/p/phishing.html - Great information and links on phishing
- 6) Free Microsoft tech support related to viruses/spyware, call 1-866-PCSafety. (I have never tried this service; I would love to hear about your experience if you do.)
- 7) www.cert.org/homeusers/HomeComputerSecurity/ - Excellent suggestions from a leading security organization. (Includes technical details: www.cert.org/tech_tips/home_networks.html)
- 8) www.securityfocus.com/columnists/220 - Don't like the list of security measures presented in this paper? Please look at this online checklist - excellent for providing even more security. (By the way, this site is also a great place for in-depth research on any security topic.)
- 9) www.fbi.gov/scams-safety - See the section entitled "On the Internet" for the FBI's suggestions on protecting your children online. (For more research on this topic, please see the list at www.bsecure.com/Resources/Resources.aspx)
- 10) National Cyber Security Alliance's www.staysafeonline.org is a great place for tips and tools.
- 11) How to Protect Your Family's PC:
http://download.zonelabs.com/bin/media/pdf/defendTheNet_howToGuide.pdf
- 12) Cyber Security Tips from U.S. CERT: www.us-cert.gov/cas/tips
- 13) www.microsoft.com/athome/security - Great info and solutions for viruses, spyware, spam, email, online safety for children, protecting personal information, backups, fraud, passwords, etc.
- 14) www.pctools.com/guides/security Windows Security Guide - Articles and Utilities
- 15) rusecure.rutgers.edu - A great resource for home or small business users.
- 16) Excellent firewall review for home users: <http://www.consumersearch.com/firewalls/review> Also see www.firewallguide.com for a great site for best practices, comparisons, news on firewalls, antivirus, and security in general.

Further Considerations for Small Businesses (in addition to above info)

- 1) Security is not a state, but a process. With how fast the industry is changing and the expertise required to keep your valuable information protected, you would probably be wise to hire an outside computer security firm whose expertise is providing security for businesses.
 - 2) Create a security policy that makes sense for your organization. If you don't take the time to specify what information and assets are important to you and outline steps to protect your organization, then there is a high probability that you will overlook crucial issues and your business will remain vulnerable to attacks. For some great ideas and a roadmap, check out The SANS Security Policy Project at www.sans.org/resources/policies/
 - 3) Wireless networks *must* run strong encryption such as WPA2 (or WPA) with very strong passwords, not WEP!
 - 4) Make sure you are running a modern/current operating system with the latest security patches. E.g. Windows XP/Vista or a recent release of Linux, Mac OS, etc. (not Windows 98 or older)
 - 5) Keep offsite backups, but handle them as a valuable asset, not allowing them to be lost or stolen.
 - 6) Don't ever store sensitive information on flash drives or other portable media without employing private key encryption (such as Folder Lock: www.newsoftwares.net/folderlock, NTI Ninja: www.ntius.com/ninja.asp, or the free TrueCrypt: www.truecrypt.com). See here for detailed directions for TrueCrypt: www.makeuseof.com/tag/download-lockdown-secure-files-truecrypt/
 - a) If your employees travel with laptops, you should probably encrypt the entire hard drive. Both Windows and Macs have built in capabilities to provide this; or you can get a third party utility such as TrueCrypt.
 - 7) Insist on the use of strong passwords (impossible to guess) for all employees. (This includes using a password at least 8 [or more] characters long, with upper and lower case characters, and including numbers and non-alphanumeric characters - like {}[]:;<>* ^ % ~ ` + =, etc.)
 - 8) Consider the sensitivity of electronic information you transmit (via email, FTP, Instant Messaging, on CDs, etc) and use public key encryption if interception of this information could cause substantial harm. Consider the free program GPG or the more complete program PGP for encrypting emails.
 - a) Consider implementing a Virtual Private Network (VPN) for all remote communication taking place over the Internet.
 - 9) You should use Uninterruptible Power Supplies (UPS) on all your computers and equipment.
 - 10) If needed, consider implementing a spam filter (centrally or on each computer individually)
 - 11) Periodically run a security analyzer program, such as Microsoft's Baseline Security Analyzer (MBSA) to assess vulnerabilities
 - 12) If you host a web server accessible from the Internet at your place of business, put it in a Demilitarized Zone (DMZ). Otherwise, keep your website at an ISP and let them put it in a DMZ.
- ### 13) Further Resources for Businesses
- a) FTC doc on reducing computer risks: www.ftc.gov/bcp/edu/pubs/business/idtheft/bus58.shtm
 - b) "Protect Your Network from Internal Threats" from PC Magazine: www.pcmag.com/article2/0,2817,2326281,00.asp?kc=PCRSS03129TX1K0000625