Essential Security Measures for Home Computers

Created by Corey Keating

Below is a list of security measures that I strongly recommend for all home computer users (whether using Microsoft Windows and Apple Macs). The items mentioned here 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, photos, and data (which means everyone!). Don't become a victim of **identity theft** or have all your files encrypted by **ransomware**!

If you think the above categories don't 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 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, tablets,** etc. Be very aware of the fact that these types of devices also need to be kept secure; if not more so! Many people have every aspect of their lives on their smartphone. 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 or financial loss. (See the "Smartphone Security" info on this site for details on how to secure your smartphone.)

This document also does not talk about "smart" devices that may be connected to the Internet and can be accessed remotely, such as security cameras, lightbulbs, power plugs, DVRs, etc. (And maybe even smart toasters, refrigerators, etc.) (These are collectively referred to as the **Internet of Things** [IoT].) Make sure to **(1) change the default passwords on all these devices, (2) periodically update their firmware, and (3) consider placing them into a DMZ on your home network.** (You may need someone with networking knowledge to help do this third item, but I highly recommend it.) They are being hacked into, manipulated, and used to wreak havoc on the Internet! Can you imagine what someone could do if they could hack into and control every electronic device in your house, car, and life? Don't just buy the cheapest "smart" device you can find; **insist on security controls to be built into every device you purchase**. (See the configuration items for IoT under "Other Excellent Resources" below.)

The first section of this document below is an **Executive Summary**, listing the steps you need to take to secure your computer. The number in front of each item corresponds to a larger explanation of the item given in the next section. If you need more detail, look in the "**Details**" section further on down.

Executive Summary/Checklist (see corresponding number in Detail section for more info)

Do These NOW!

1, 2, 3) Windows Computers: Run antivirus, antispyware, and a software firewall, (such as Bitdefender's Internet Security, Avast! Internet Security, or McAfee Internet Security.)

4) Mac Computers: Should run Mac versions of Antivirus software: Bitdefender, ESET, or Sophos.

5) Backup your Data (regularly!) (Try the online CrashPlan, Acronis, or Carbonite. Or use external hard drive with Acronis.)

6) Keep your Operating System and other software updated (e.g. "Windows Update").
- Remove unnecessary software from your computer as it creates security holes. Especially: remove Adobe Flash and Java if you can. If they are absolutely needed, then keep them updated!

7) Add a hardware firewall for home Internet connection. Change all hardware passwords.
If you are especially security conscious, then please see my document on "More Secure Home Routers".

8) Wireless networking: do wireless encryption (WPA2) and change password on wireless access point/router.

Other Critical Items

9) Be very careful when using public WiFi; only connect to known providers. You should use a VPN if doing banking, online purchases, downloading software, or sending personal information in a public location.

10) 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, such as LastPass, RoboForm, Dashlane, KeePass, (or 1Password if you use only Apple devices: Macs/iPad/iPhone).

11) Take care of physical security of devices, especially in public locations

Be Smart Online - Very Important Security Considerations

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

12) DON'T open attachments in email from people you don't know! And be cautious about email attachments from people you do know, especially if you are not expecting an attachment.

13) Understand Phishing and don't fall for it; e.g. your bank will NEVER ask for your password!

14) The greatest single attack vector, even for the Mac computer, is your web browser. Consider using a script blocking program: Google's Chrome with uBlock Origin or Firefox with the NoScript plug-in (or the one that comes with Kaspersky's Internet Security).

15) Don't believe a website pop-up that tells you that you have a virus, an outdated program, and urges to you "click here" to scan/clean/update. Use your already-installed, trusted antivirus program.

16) Consider the answers you use to password recovery services (i.e. "Forgot your password?). Consider lying for any site that does NOT need to know that truth! :-) (Just remember your fake answers.)

17) Only make online purchases from reputable sites (usually providing a phone number) and that offer purchases with "https". Use Credit Card or PayPal (not Debit Card) for all online purchases.

18) Don't forward "urgent/important" emails without first verify the information, e.g. www.truthorfiction.com

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

19) Children are vulnerable, and their innocence may lead them to give out personal info online to those seeking to harm them. Furthermore, we all need protection from the dark side of the Internet. Follow the steps recommended here to be aware of your kids online actions, especially on social networking sites like Facebook.
-- Why not purchase Circle (meetcircle.com) for simple, effective WiFi Internet filtering and control?

Further Suggested Measures - These may make your life easier!

20) Protect your computer and electronic equipment from electrical problems.
21) Recycle your computer the right way, deleting all personal information first.
22) Protect any sensitive data you keep on flash drives or backups - consider encrypting it.
23) Special considerations for traveling with a laptop or tablet.
24) Consider signing up for an Identity Theft Protection service.
25) 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 Bitdefender Internet Security, Avast! Antivirus, McAfee Antivirus, or Symantec/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 Bitdefender Internet Security, ESET Smart Security, Avast! Internet Security, or McAfee Internet Security. (I ***don't*** prefer Symantec/Norton's Suite although it works well for many people.)
   b) Some good **free** antivirus-only programs are: BitDefender Free, AVG Antivirus Free Edition, or Avast! Antivirus.
   c) Please note that I **don't** think that the free Microsoft Security Essentials or Windows Defender provides adequate protection, although Windows Defender should be run along with your third-party antivirus program.
   d) Unfortunately, I can **no longer recommend** using **Kaspersky's** antivirus software. Although it is still highly rated on many websites, it is operated out of Russia. As such, it was used for spying on the U.S. government. We cannot rule out the possibility of it being used maliciously in the future: For more details, please see: www.consumerreports.org/privacy/what-to-do-about-the-kaspersky-data-hack-/ or www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.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. The built-in firewall for Macs and Windows has improved and is probably adequate; just make sure they are turned on. Otherwise, they are included in many of the Suites mentioned in #1(a) above.
   a) Excellent **free** firewall options: Comodo Firewall Pro (and anti-virus) personalfirewall.comodo.com OR ZoneAlarm Free Version from www.zonealarm.com

Necessary Measures for Mac Computers:

4) Although Macs may not be as susceptible to viruses, Trojans, worms (and other malware) as their Windows counterparts, they indeed can be infected with spyware/malware (through Social Engineering if nothing else). Even if some argue that the Mac OSX can't get a virus, they can! It is also a fact that many of the programs you run on your Mac are vulnerable. As Macs are gaining more market share, they are becoming a bigger target for hackers. I suggest you run the antivirus software Bitdefender for Mac free

(www.bitdefender.com/solutions/virus-scanner-for-mac.html), Sophos Home free version (home.sophos.com/mac), or ESET Antivirus for Mac paid version (www.eset.com), (See "Mac OS X and viruses" under the "Other Excellent Resources" section below for more info if you need convincing here.)

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

5) **Back It Up!** 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 on Online in case of a major disaster.)
   a) The rampant outbreak of Ransomware makes backing up your data all the more urgent. (see www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx or www.dhs.gov/blog/2016/04/06/protect-your-data-against-ransomware)
   b) Be sure to backup emails and Internet "Favorites" if those are important to you.
   c) 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 (by encryption).
   d) For help in creating and implementing a backup plan, see my document, "**A Simple Backup Strategy for Home Computers**" available from www.computersecuritynw.com
      i) **OR** just choose an online backup solution like CrashPlan (www.crashplan.com), Carbonite (www.carbonite.com), or Acronis True Image Home (www.acronis.com).

6) Keep your operating system (e.g. Windows 7/8/10, 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) If possible, remove Adobe Flash and Java from your computer. If you must run them, keep them updated. If possible, disable these programs them in your web-browser until they are needed.
   b) You should no longer be running the outdated Windows XP (or Vista). It is no longer supported and is completely full of vulnerabilities that can easily be hacked by anyone. Get a new computer now!
   c) Also keep your other application programs updated periodically (**especially** ones such as Adobe Flash, Adobe PDF Reader, Java, Internet Explorer or Firefox, MS Office, etc.)

7) 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) Even though you have a Cable/DSL Modem that provides some of this functionality, these devices are often insecure. You need to add a "home router" to your home network!
   b) 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.
   c) For a secure Home Router, see the document, "More Secure Home and SMB Routers" on this site.

8) 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). (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 up bandwidth (slowing down your connection); 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. Businesses should NOT use WEP.

Other Critical Security Precautions:

9) 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. To set up a VPN, you need to contract with a VPN service provider. I recommend one of the following: Private Internet Access (www.privateinternetaccess.com), IVPN (www.ivpn.net), NordVPN (nordvpn.com), BolehVPN (www.bolehvpn.net), or Proxy.sh (proxy.sh).

      i) Note that the recommendation for these particular VPN services are NOT necessarily for someone living in country with a hostile government. These VPN services are great for general protection for someone wanting protection when using public Wi-Fi. .

      ii) Note that although using the PPTP protocol is better than nothing, it is considered "broken" by security experts and can be hacked into. If you do any traveling, you should use the stronger OpenVPN, SSL, or IPSec protocols.

   c) NEVER update programs like "Adobe Flash", when connected to a public WiFi, especially in high-traffic areas such as airports. Public access points are susceptible to hacking, then give you viruses.

10) **Manage your passwords.** Use "strong" passwords for all accounts, especially your financial ones. You actually need to think in terms of a "passphrase" rather than "password". For some great suggestions on "easy to remember" but "difficult to crack" passwords, see www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it Alternatively, you can take a long, personalized sentence and use the first letter of each word, with numbers and characters sprinkled in.

   a) Do NOT use the same passwords for all your accounts! If your email gets hacked then they have access to 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) Do NOT allow your web browser to store your passwords; it can easily be hacked into.

   d) 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 - www.agilebits.com) or
      - Dashlane (free with one device; must pay to sync in cloud) www.dashlane.com

      iii) You might also want to keep all serial numbers of software and other info in this program.

11) Most identify theft is due to **physical theft** of wallet/purse/personal identification or physical theft of your computer. Physical security is important! Don't leave our items unattended. Lock your computer to a table or desk if leaving it unattended (using a Security Cable Lock). Also, consider purchasing Lifelock (below). Details at this article: www.identitytheftjournal.com/common-causes-identity-theft

   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.lojack.com/Laptops

Be Smart Online - Very Important Security Cautions and Actions:

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

12) 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 from your friend's email account!
    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! You may not get what you ordered! And, the way to put spammers out of business is to not fund them by clicking on their links. Even going to a website advertised by spam could infect your computer.
    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, or saying they are traveling overseas that need money, 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.
13) 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/topics/consumer-protection/fraud-resources/internet-pirates.html
14) Your **Web Browser** (Internet Explorer, Firefox, Chrome, Safari, etc.) is one of the greatest attack vectors for your computer (even for Macs). So, for general web browsing (going to sites you don't know/trust), you may want to consider using Firefox with the NoScript plug-in (www.noscript.net); or Google's Chrome with uBlock Origin; these programs block many scripts from running in the background when you visit a webpage. (Just note that they sometimes block legitimate scripts, so you need to be willing to add "trusted sites".)
15) 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 it! Chances are this is scheme to get you to actually **install a virus**. This includes the situation where you are told to call a phone number and "don't reboot your computer". DO reboot your computer and do not call a phone number given to you in a website pop-up.
    a) In fact, even if you do get a legitimate email from your bank with a website link, it is best *not* to click that link. The habit of clicking web-links in emails is dangerous. You are better off just to open a browser and go to the website of your financial institution directly.
    b) 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/
    c) If you think you may have been phished/id stolen, go to www.ftc.gov/idtheft/
16) Most websites (like your bank or email accounts) have systems for you to recover or reset 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!). (Many public figures have had accounts hijacked. For example: www.wired.com/2008/09/palin-e-mail-ha/)

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.

17) Only make online purchases from reputable companies and always use your credit card or PayPal; 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.)

18) 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

Accountability and Protecting Your Children and Loved-Ones:

19) 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.netsmartz.org)

b) Put your computer in a common area of your home, such as in the den, where kids have no expectation of privacy.

c) Purchase the "Circle" internet filter and device that control the time spent on any social-networking site (meetcircle.com) – only works for wireless devices (computers, smartphones, etc.). See http://lifehacker.com/circle-is-the-parental-control-for-the-internet-ive-alw-1747520805 for detailed review.

i) Or (more difficult) 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.

ii) 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, Twitter, Instagram, or Snapchat; they may be unknowingly leading a stalker to their school or your house. Parent's Guide to Social Networking Sites: www.consumer.ftc.gov/articles/0012-kids-and-socializing-online and see: www.helpnetsecurity.com/2013/12/18/teaching-children-information-security-skills/

i) For **Facebook protection,** see hubpages.com/family/Children-on-Facebook and consider these items: www.parenting.com/gallery/social-media-monitoring-kids

e) What Parents Should Know about Safe Console **Gaming**: safelagoon.com/en/blog/parents-guide-security-gaming-devices or www.theguardian.com/technology/2017/may/11/children-video-games-parents-guide-screentime-violence (Older: www.pcmag.com/article2/0,2817,2337749,00.asp)

Further Suggested Measures:

20) 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".

21) 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.

22) 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.

23) If you leave the house with a **laptop** or **tablet** 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.consumer.ftc.gov/articles/0015-laptop-security . For extra tips when traveling see: advice.cio.com/al_sacco/lax_laptop_security_at_the_airport_how_not_to_become_a_statistic

24) 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/

25) Consider using Secunia, a free program that detects vulnerable and out-of-date software and helps download updates: http://secunia.com/vulnerability_scanning/personal/ - Even if you have your operating system updates turned on (which is critical; see #5 above), your system may have vulnerabilities that come from other software on your system, such as Adobe Flash, Adobe AIR, Acrobat Reader. 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) * Federal Trade Commission's guide to Online Security: www.consumer.ftc.gov/topics/online-security
2) * Security Awareness Newsletter for Everyone: securingthehuman.sans.org/resources/newsletters/ouch
3) * National Cyber Security Alliance's www.staysafeonline.org is a great place for tips and tools.
4) 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.
5) UK's government's initiative on staying safe online. Excellent source of consumer related **videos**, tips, etc.: www.getsafeonline.org
6) Bruce Schneier (a security superstar) on staying secure (in light of Snowden revelations): www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance
7) Mac OS X and viruses: www.reedcorner.net/guides/macvirus/
    a) "New MacOS Malware, Signed With Legit Apple ID, Found Spying On HTTPS Traffic": http://thehackernews.com/2017/04/apple-mac-malware.html
8) www.webopedia.com/TERM/p/phishing.html - Great information and links on phishing
9) www.fbi.gov/scams-and-safety - See the section entitled "On the Internet" for the FBI's suggestions on protecting your children online.
10) How to Protect Your Family's PC: http://download.zonelabs.com/bin/media/pdf/defendTheNet_howToGuide.pdf

11) Cyber Security Tips from U.S. CERT: www.us-cert.gov/ncas/tips

12) Configuring Internet of Things (IoT) devices: www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity and www.sans.org/reading-room/whitepapers/hsoffice/securing-home-iot-network-37717

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 level of expertise required to keep your valuable information protected, you would probably be wise to hire an outside computer security firm/consultant who specializes in providing security for businesses.
    a) A security specialist can help you: harden your network, install security software, perform a risk assessment, create security policies, run vulnerability scans, run penetration tests, create disaster recovery and business continuity plans, etc.
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/security-resources/policies
    a) 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.)
    b) Insist that employees use different passwords on all accounts, and NOT to use the same password on their personal and business accounts.
3) Make sure you are running a modern/current operating system with the latest security patches. E.g. Windows 7/8/10 or a recent release of Linux, Mac OS, etc. (not Windows XP/Vista!)
    a) AGAIN: Keep all software patched/updated! Especially: operating system, Adobe products, Java (if you must run it), and your web browser.
4) Keep offsite backups, but handle them as a valuable asset, making sure they are encrypted, and not allowing them to be lost or stolen.
5) Wireless networks *must* run strong encryption such as WPA2 (or WPA) with very strong passwords, not WEP!
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, or the free VeraCrypt: www.veracrypt.com).
    a) If your employees travel with laptops, you should 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 VeraCrypt.
7) Consider the sensitivity of electronic information you transmit (via email, FTP, Instant Messaging, on CDs, etc) and use encryption if interception of this information could cause substantial harm. Make sure your email is set to only transmit encrypted messages. Only use encrypted FTP (i.e. SFTP), etc.
    a) Consider implementing a Virtual Private Network (VPN) for all remote communication taking place over the Internet. If you have a more advanced router, it will most likely offer this function.
    b) Consider the free program GPG or the more complete program PGP for encrypting emails. It is more complex, but offers the best security.
8) You should use Uninterruptible Power Supplies (UPS) on all computers and/or networking equipment that should not be shutdown unexpectedly.
9) If needed, consider implementing a spam filter (centrally or on each computer individually)
10) Periodically run a security analyzer program, such as Microsoft's Baseline Security Analyzer (MBSA) to assess vulnerabilities
11) 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.
    a) Run vulnerability tests against all web-based software.

12) **Further Resources for Businesses**

a) FTC doc on reducing computer risks: www.ftc.gov/tips-advice/business-center/guidance/security-check-reducing-risks-your-computer-systems

b) "Protect Your Network from Internal Threats" (outdated, but still relevant) from PC Magazine: www.pcmag.com/article2/0,2817,2326281,00.asp?kc=PCRSS03129TX1K0000625