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 information 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 multimillion-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. Many newer Wi-Fi routers offer for you to create “Guest Network”; consider placing IoT devices on that network.) 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? Or use your smart baby monitor to spy on your kids! (It happens.) 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 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 listed in **The Details** section below.

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

Do These NOW!

1) Windows Computers: Run **antivirus**, antispyware, and a software firewall, (such as Bitdefender's Internet Security, ESET Internet Security, or McAfee Internet Security.)
   Note: On Windows 10: The built-in Microsoft Windows Defender Antivirus is adequate to protect against malware; if you want a free product, then it is already installed on Windows. However, it doesn't provide other features that these Suites offer, such as anti-ransomware features, phishing protection, advanced software firewall, URL ratings, VPN, etc.
2) Mac Computers: Run Mac versions of **Antivirus** software: Bitdefender, ESET, or Sophos.
3) **Encrypt** your computer's hard drive. If your computer is lost or stolen, even when you have a password, it is trivial to get all information on a computer if the disk is not encrypted. Both Windows and Macs have free encryption; just make sure it is turned on.
4) **Backup** your Data (regularly!) Try the online Acronis, BackBlaze, iDrive, Carbonite, or CrashPlan. Or use external hard drive with Acronis. (Or search online for best online backup solutions.) Encrypt your backups.
5) **Patch**: Keep your Operating System and other software updated/patched (e.g. install "Windows Update" or "Security Updates").
   - 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!
6) Use strong **passwords** for all online accounts (especially financial ones) and
   - DON'T use the same password for all your accounts. (See suggestions below for creating strong passwords/passphrases.)
   - Use a Password Manager program that encrypts your passwords, such as LastPass, 1Password, Dashlane, RoboForm, or KeePass. Don't keep passwords in a Word or Excel file!
   - Don't let your web browser store your passwords; these are easy for any hacker to steal! The only place you should store your passwords is in a Password Manager.
   - If you leave your computer unattended, make sure to lock your computer or logout of your Password Manager program.
7) Implement Multi-Factor Authentication (**MFA**) [also called Two-Factor Authentication (2FA)] on all your important accounts!

Other Critical Items

8) Add a hardware firewall for home Internet connection. Change all hardware default passwords.
   - If you are especially security conscious, then please see my document on "Secure Routers for Home and Small Business"
9) Wireless networking: do wireless encryption (WPA2) and change the default password on wireless access point/router at your home or business.
   - Consider purchasing a whole-home Wi-Fi solution that has built-in security features (for subscription) such as Netgear's Orbi or Eero's Armor/Parental Controls.
10) Be very careful when using public Wi-Fi; 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.
11) Take care of physical security of devices, especially in public locations. Your computer should have a password, and always lock it when you leave it unattended. (Consider using a physical lock.)

Critical – Beware of Social Engineering

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

12) Don't open attachments or click on website links in emails from people you don't know! And be cautious about email attachments & website links from people you do know, especially if you are not expecting an attachment or the email seems out of place.

13) Understand Phishing and don't fall for it; cyber-criminals are trying to steal your passwords. E.g. your bank will NEVER email you asking for your password!
- The same is true for a random text/SMS message. Don't click!!
- Never give out a text/SMS "verification code" to anyone! Your bank will not ask you to confirm the numbers they just texted to you!!

14) 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.

Be Smart Online – Other Important Security Considerations

15) The most vulnerable program on your computer, even for Macs, is your web browser. Consider using a script blocking program: Google's Chrome with uBlock Origin or Firefox with the NoScript plug-in.
- Don't let your web browser store your passwords; these are easy for any hacker to steal! Use a Password Manager.

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; store them in your encrypted Password Manager.)

17) Only make online purchases from reputable sites (usually providing a phone number) and that offer purchases with "https". Use Credit Card or PayPal or digital payment methods (e.g. Apple Pay or Google Pay), not a Debit Card, for all online purchases.

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

18) 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 below to be aware of your kids' online actions, especially on social networking sites like Facebook.

Further Suggested Measures - These may make your life easier!

19) Don't forward "urgent/important" emails without first verify the information, e.g. at www.truthorfiction.com
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, external hard drives, or backups - encrypt it.
23) Special considerations for traveling with a laptop or tablet.
24) Consider signing up for an Identity Theft Protection service.

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 daily. Most programs are automatically updated.)
   a) If you are running the latest version of Windows, then the built-in Windows Defender Antivirus provides good antivirus protection; you don't need to buy anything. (This didn't used to be true, but Microsoft has put a lot of effort into providing security solutions.)
   b) However, I still feel it is **best** to use a **security suite** from a reputable company that combines anti-virus, anti-spyware, software firewall, spam filtering, URL filtering, etc. Some excellent options

are Bitdefender Internet Security, ESET Smart Security, or McAfee Internet Security. (I ***don't*** prefer Symantec/Norton's Suite although it works well for many people.)

c) 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

Necessary Measures for Mac Computers:

2) 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):

3) **Encrypt** your computer's hard drive. If your computer is lost or stolen, even when you have a password, it is trivial to get all information on a computer if the disk is not encrypted. Both Windows and Macs have free encryption; just make sure it is turned on.
   a) Windows 10: Device Encryption or BitLocker. See: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d or https://www.windowscentral.com/how-enable-device-encryption-windows-10-home
   b) Macs: Turn on FileVault. See: https://support.apple.com/en-us/HT204837
4) **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 or Online in case of a major disaster.)
   a) The rampant outbreak of Ransomware makes backing up your data even more urgent. (see www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx or www.cisa.gov/stopransomware/ransomware-101)
   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 Acronis True Image Home (www.acronis.com), BackBlaze (www.backblaze.com), iDrive (www.idrive.com), CrashPlan (www.crashplan.com), or Carbonite (www.carbonite.com).
5) Keep your operating system (e.g. Windows 10/11, Mac OS X) updated with all the latest security patches. (Microsoft Windows and Macs are configured to automatically download updates. Don't change these default settings.)
   a) If you are running a version of Windows or Mac OS X that is no longer supported and cannot be patched by applying security updates, then you MUST upgrade!! Vulnerabilities are being discovered daily and hackers use these weaknesses to break into your computer. Don't run an unsupported version of software!

b) If possible, remove Adobe Flash and Java from your computer. If you must run them, keep them updated. If possible, disable these programs in your web-browser until they are needed.

c) Also keep your other application programs updated periodically (**especially** ones such as Adobe Flash, Adobe PDF Reader, Java, Firefox, Google Chrome, MS Office, etc.)

6) **Manage your passwords.** Use strong passwords for all accounts, especially your email and financial accounts. You should think in terms of a "passphrase" rather than "password". For some great suggestions on "easy to remember" but "difficult to crack" passwords, see www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases 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 allow your web browser to store your passwords/passphrases; it can easily be hacked into.

c) Do NOT keep your passwords/passphrases in an unencrypted document on your computer!

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:
- LastPass (free for single platform / for-pay for multi-platform - www.lastpass.com), or
- 1Password (no free account, but great for personal or family accounts - 1password.com) or
- Dashlane (free with one device; must pay to sync in cloud - www.dashlane.com)

iii) If you leave your computer unattended, make sure to lock your computer or logout of your Password Manager program.

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

7) Implement Multi-Factor Authentication (**MFA**) [also called Two-Factor Authentication (**2FA**)] on all your important accounts!

a) Microsoft says that users who enable multi-factor authentication (MFA) for their accounts block 99.9% of automated attacks: www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/

b) See this article for details of how to set up MFA: www.zdnet.com/article/better-than-the-best-password-how-to-use-2fa-to-improve-your-security/

Other Critical Security Precautions:

8) Get a hardware firewall for your Internet connection. (Ask at your local computer store. These are often referred to as "home routers".)

a) Even though your Cable/DSL Modem provides some of this functionality, these devices are often insecure. You need to add a "home router" as an extra layer of protection for 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 and hijack your network 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, "Secure Routers for Home and Small Businesses" on this site.

9) If you have **wireless networking** (Wi-Fi) 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) 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) Consider purchasing a security product built into your wireless networking gear, such as Netgear's Orbi whole-home Wi-Fi (Armor or Smart Parental Controls) or Eero Wi-Fi solution with their security add-on.

10) Be VERY cautious when you connect to **public Wi-Fi** access points! Only attach to what you know is the Wi-Fi offered by a local business/coffeeshop you trust; NEVER attach to a Wi-Fi point named "Free Wi-Fi" 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), ExpressVPN (www.expressvpn.com), or ProtonVPN (protonvpn.com).

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) 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, WireGuard, or IPSec protocols.

c) NEVER update programs, when connected to a public Wi-Fi, especially in high-traffic areas such as airports. Public access points are susceptible to hacking, then dishing out viruses.

11) Most identify theft is due to **physical theft** of wallet/purse/personal identification or physical theft of your computer.
- Even at home, if you use a Password Manager program, your computer should require a password and you should lock it when you leave it unattended. www.howtogeek.com/757776/how-to-lock-your-windows-11-pc
- Physical security is important! Don't leave your items unattended in a public location. Lock your computer to a table or desk if leaving it unattended (using a Security Cable Lock). See: nerdtechy.com/best-laptop-lock-cables (Note that although most laptops use a Kensington lock, some thinner Dell models use a Noble lock: www.noblelocks.com)
- Also, consider purchasing identity theft insurance (below). Details at this article: www.lifelock.com/learn/identity-theft-resources/ways-identity-theft-happen-can-happen

Beware of Social Engineering

Remember, YOU (your actions) are the most vulnerable aspect of a completely secure computer. :-)
See this Blog post on Social Engineering

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 a question about it or it looks suspicious, confirm with them (via phone/text) that they meant to send it to you; it could be someone 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 "check out this business opportunity", 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.

c) See this Blog post about not clicking a link in an unsolicited email.

13) Don't be caught in a "**phishing**" scam, where people steal your personal information or username/password for identity theft or other nefarious purposes. That is, **NEVER** click on links in emails sent to you supposedly from your bank, eBay, PayPal, Apple, Netflix, etc. 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 through an email 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 (or banking app) and go the site you know is legitimate or **call** your financial institution. For more info, please check out www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html

a) The same is true for a random text/SMS messages containing website links. Don't click!

b) Also, **never give out a text/SMS "verification code"** to anyone! This is your "second factor" in your multi-factor authentication. No service (especially financial institutions) will not ask you to confirm the numbers they just texted to you!! You can be sure this is a criminal trying to defraud you.

c) 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.

d) See docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

14) If you think you may have been phished or your ID stolen, go to www.ftc.gov/idtheft/ 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 actually get you to **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.

Be Smart Online – Other Very Important Security Cautions and Actions:

15) Your **Web Browser** (Internet Explorer, Chrome, Edge, Firefox, Safari, etc.) is one of the most susceptible programs on your computer (even for Macs), prone to being hacked. 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 the 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".)

a) As noted above, never let your web-browser store your passwords! These can easily be stolen just by visiting a booby-trapped website.

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 actually make it easy for

hackers to steal your passwords. For many of the questions in these Password Recovery services 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 encrypted Password Manager 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, PayPal, Apple Pay, or Google Pay (not a debit 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.)

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 protect your children. If you have a child old enough to get on the Internet, then please educate yourself by searching online for “online risks for children” and “how to protect children online.”

a) Educate yourself and your children about online dangers and appropriate online behavior. (Maybe start here: www.microsoft.com/en-us/windows/remote-resource-center/keep-your-family-safer-online or www.pcmag.com/how-to/things-every-parent-with-a-connected-kid-needs-to-know) www.weforum.org/agenda/2021/10/overcoming-the-growing-risks-to-kids-online

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

c) Get an internet filter or parental controls
   i) -- Why not purchase Circle (meetcircle.com) or Bitdefender’s Box (www.bitdefender.com/box) for simple, effective Wi-Fi Internet filtering and control?
   ii) -- Or, purchase Netgear's Orbi whole-home Wi-Fi solution that comes with Smart Parental Controls (www.netgear.com/home/services/smart-parental-controls)
   iii) -- Or, purchase Eero Wi-Fi solution with their security add-on: (eero.com/eero-secure)
   iv) - OR You can use a free/cheap DNS web-filter which will control all websites available through your home internet connection. (Although these may require some technical skills to install.) Try: CleanBrowsing.org or www.opendns.com/home-internet-security or www.safedns.com/en/home-plans-pricing
   v) See “How Your Kids or Outsmarting All Your Parental Controls”: lifehacker.com/how-your-kids-are-outsmarting-all-your-parental-control-1848249586
   vi) 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. Although no software is flawless, it helps - and can provide some valuable accountability. Just search online for “best parental controls software"
   vii) x3watch (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 www.parents.com/parenting/better-parenting/advice/why-its-never-too-early-to-teach-your-child-good-social-media

e) What Parents Should Know about Safe Console **Gaming**: Again, do a search online for a parent's guide to children online gaming. Here is one article: parentzone.org.uk/article/gaming-parents-guide

Further Suggested Measures:

19) 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

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.consumer.ftc.gov/articles/how-protect-your-data-you-get-rid-your-computer Summary: 1) Backup your files, 2) Sign out of all accounts and 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 coffeeshop. Here are some general security tips for keeping your laptop safe: www.thetravelblogs.com/how-to-keep-your-laptop-safe-while-traveling , www.thesparkmag.com/travel-tips-for-your-laptop , or quantumpc.com/tips-securing-laptop-traveling

24) Consider signing up for an identity theft monitoring service like LifeLock (www.lifelock.com), Complete ID (especially for Costco members) (www.completeid.com), Identity Force (www.identityforce.com), or Identity Guard (www.identityguard.com).

a) Compare services and sign up at this website to get a discount: www.identitytheftlabs.com

b) Some great identity theft information: www.idtheftcenter.org

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) * Surveillance Self-Defense: ssd.eff.org/en
5) * The WIRED Guide to Digital Security: www.wired.com/2017/12/digital-security-guide
6) 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.
7) UK's government's initiative on staying safe online. Excellent source of consumer related **videos**, tips, etc.: www.getsafeonline.org

8) 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
9) Password Security: www.consumer.ftc.gov/articles/password-checklist
10) 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
11) www.webopedia.com/TERM/p/phishing.html - Great information and links on phishing
12) www.fbi.gov/scams-and-safety - See the section entitled "On the Internet" for the FBI's suggestions on protecting your children online.
13) How to Protect Your Family's PC: http://download.zonelabs.com/bin/media/pdf/defendTheNet_howToGuide.pdf
14) Cyber Security Tips from U.S. CERT: www.us-cert.gov/ncas/tips
15) 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 incident response plans, disaster recovery and business continuity plans, etc.
    b) Consider implementing the CIS Critical Security Controls (www.cisecurity.org/controls/v8). Start with Implementation Group 1 (IG1), then mature from there.
2) You MUST educate yourself on how to protect against **ransomware**. Start here: www.cisa.gov/StopRansomware
3) Create **security policies** 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 or the NIST Cybersecurity Framework Policies at: www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf
    a) Insist on the use of strong passwords (impossible to guess) for all employees. (This includes using a password at least 8 [but most likely 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.

4) Make sure you are running a modern/**current operating system** with the latest security patches. E.g. Windows 10/11 or a recent release of Linux, Mac OS, etc.
   a) AGAIN: Keep all software **patched**/updated! Especially: operating system, Adobe products, Java (if you must run it), and your web browser.
5) You should never expose Remote Desktop Protocol (**RDP**) to the Internet. You are just inviting criminal hackers to break into your network. You should instead provide a hardened VPN solution if you need people to reach into your network from the Internet.
   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. Otherwise you can purchase a dedicated device for this function.
6) You must implement multi-factor authentication (**MFA**) for ALL external access to your internal network or to any Cloud resources you operate.
7) Keep **offsite backups**, but handle them as a valuable asset, making sure they are encrypted, and not allowing them to be lost or stolen. Design your backup solution with "recovering from ransomware" in mind.
8) **Email security**: If needed, consider implementing an email **spam filter** (centrally or on each computer individually) and train your employees to not fall victim to **phishing emails**.
9) **Wireless networks** *must* run strong encryption such as WPA2 (or WPA) with very strong passwords, not WEP!
10) 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 , or compress with 7-Zip with the Archive option www.7-zip.org)
    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.
11) 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 the free program GPG or the more complete program PGP for encrypting emails. It is more complex, but offers the best security.
12) You should use **Uninterruptible Power Supplies** (UPS) on all computers and/or networking equipment that should not be shutdown unexpectedly.
13) Periodically run a **vulnerability analyzer program**, such as Microsoft's Baseline Security Analyzer (MBSA) to assess vulnerabilities, or implement a more robust vulnerability scanning program from a company like Tenable (Nessus) or Qualys.
14) 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) Hardened your website. E.g. owasp.org/www-project-top-ten
    b) Run vulnerability tests against all web-based software.
15) **Further Resources for Businesses**
    a) CIS Critical Security Controls: www.cisecurity.org/controls
    b) NIST Cybersecurity Framework: www.nist.gov/cyberframework
    c) FTC doc on reducing computer risks: www.ftc.gov/tips-advice/business-center/guidance/security-check-reducing-risks-your-computer-systems
    d) "Protect Your Network from Internal Threats" (outdated, but still relevant) from PC Magazine: www.pcmag.com/article2/0,2817,2326281,00.asp?kc=PCRSS03129TX1K0000625