

The 10 Commandments of Computer Security



TECHVERA

A how-to guide on keeping your personal and financial information guarded.



There is no such thing as too much security when it comes to your computer (and any electronic devices!). Most people use their electronics for sensitive activities like banking, paying bills, shopping, and emailing - making you enter and transmit personal and financial information constantly. Observe our 10 commandments of computer security now before your security issues grow to Biblical proportions.



THOU SHALT:



The 10 Commandments of Computer Security

1)

Install and Update Anti-Virus/Malware and Firewall Protection

Anti-virus and anti-malware software is an integral part of computer safety and security. If you use Windows, Microsoft has free protection in the form of [Microsoft Security Essentials](#) for Windows Vista and 7. Windows 8 and later come with the built in Windows Defender. If you're a light computer user then these free programs should be just fine for your needs, but if you use your computer daily and quite often, and have sensitive information to protect then you'll likely want to look into a paid anti-virus software. We recommend ESET which has home and business versions for both Windows and Mac users ([download here](#)).

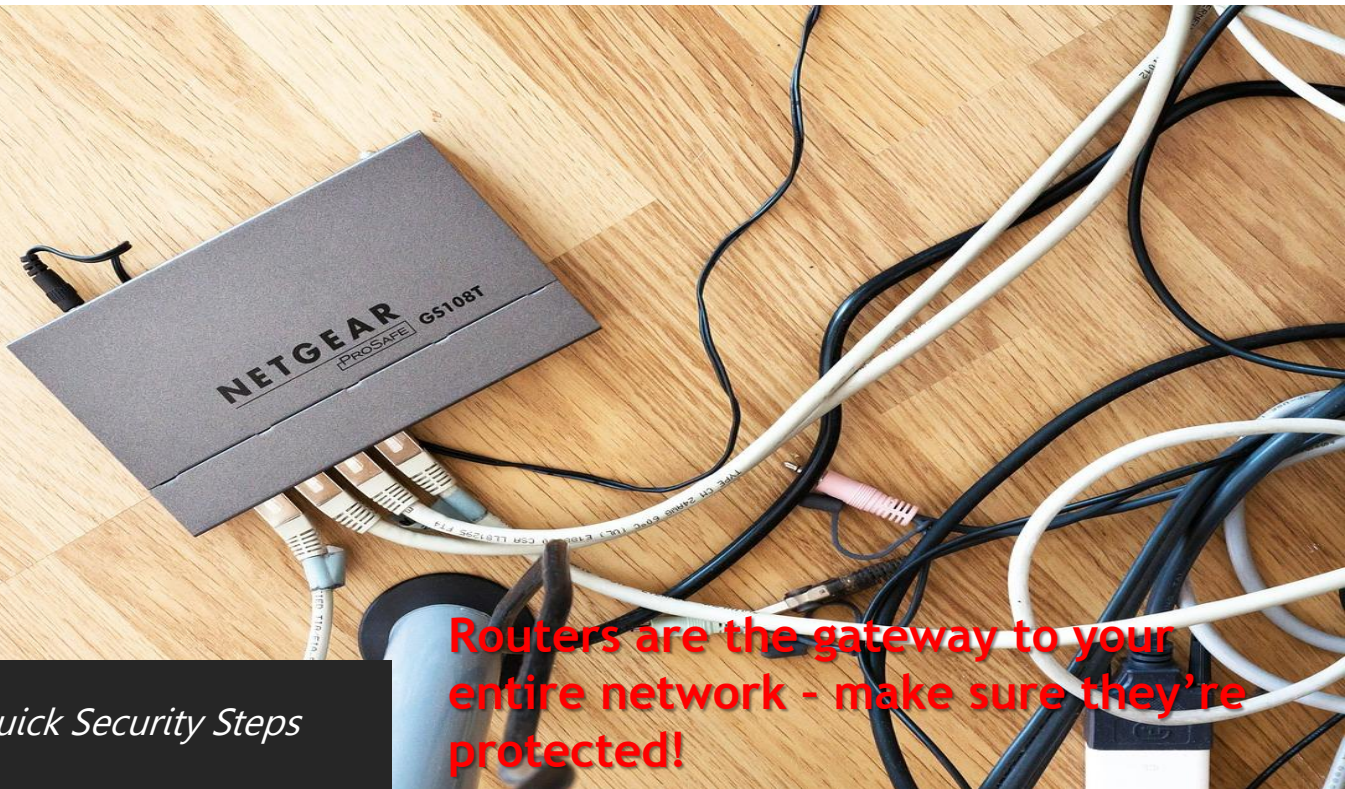


Paid anti-virus programs tend to have better support behind them along with faster updates and patches to protect against newly created malware and viruses. They also frequently offer multi-dimensional support to help protect emails, web browsing, other devices like phones/tablets, and more.

It's important to note however that having an anti-virus doesn't guarantee 100% protection against infections. Even the best program can't help if you accidentally approve the installation of a bogus application, click on an infected ad online, or let a scammer remotely connect to your machine. In addition to anti-virus, every computer should be protected with a firewall. "[A firewall is](#) a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the internet". Firewalls are meant to work in conjunction with an anti-virus program, whereas you should never run two or more anti-virus applications on your computer at the same time as this can cause errors. A program meant to work alongside your anti-virus to help boost protection is okay, such as [MalwareBytes Anti-Malware](#).

2)

Secure Your Router



Quick Security Steps

- ❑ Password Encryption – never leave your router open without a password, and encrypt your wireless signal.
- ❑ Turn off Broadcasting – keep others from jumping onto your network.
- ❑ Disable Guest Networks – for home use, you don't need guest networks.
- ❑ MAC Filtering – any device not on the filtering list will be blocked from accessing.
- ❑ Get a Network Monitoring App – a good idea to keep an eye on potential issues and security holes.

Routers are the gateway to your entire network - make sure they're protected!

Many people worry only about protecting their computers, when in fact routers are extremely easy to get into. Once connected to an unsecured router, someone can access any device connected to the network - potentially every single internet connected device you own. Who's On My Wifi has a great whitepaper outlining [5 steps you can take to make your router and wireless network very difficult to exploit](#). This can be a fairly intimidating process if you haven't had much experience configuring router settings, so if you're not confident doing this yourself it's highly recommended to either call your internet service provider or a trusted IT professional for help.

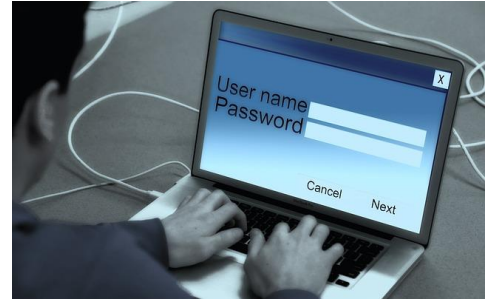
3)

Set Up and Use a Standard (Non-Administrator) Account

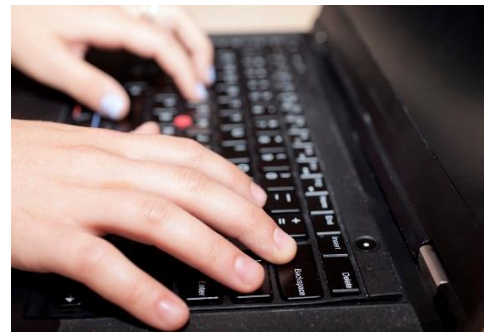
Stop using an administrator account for everyday use.

This is one of the quickest, most helpful steps to take to secure your computer. There are a few different types of Windows user accounts. The first is an administrator account. These are password-protected and required to be made during operating system setup (meaning every computer will have at least one admin account). It gives full control of Windows including changing settings and security features, installing programs, and just about anything else you could want to do on a computer without requiring a password. You can see how dangerous it would be for a hacker or infection to get control of an administrator account.

Many people use the administrator account for their every day use which is understandable. It has the most control and doesn't bother you every time you want to install a program or change a setting. However, with how infrequently most people need to do those administrator level tasks, it makes sense to only use one when needed (or simply type in your admin password when required on a standard account) and stick with a more secure standard account for daily use. Hackers or malware gain the rights of whichever type of account they've gotten access to, and when it's an admin account they have total control of your computer's settings and functionality. "If you're using an administrator account when a hacker takes control, a relative is on your computer or a virus gets on your system, then they can do anything they want. If you're using a standard account, however, then they can only do things that don't require administrator permission. That means a hacker or relative can't change major settings or install viruses, and viruses themselves can't install unless you enter the administrator password. You'll know right away something is up when your computer starts asking for permission to do things you didn't ask it to do". [Check out this page](#) for instructions on setting up each type of account depending on which version of Windows you're using.



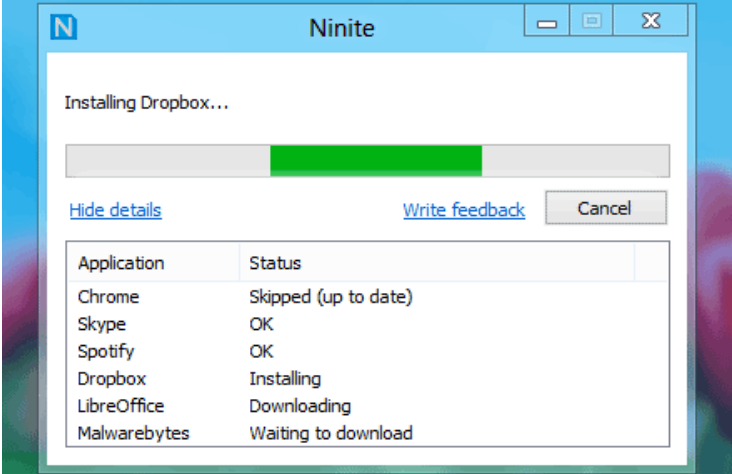
The second type of Windows account is a standard account and is more restrictive. It allows you to do all the basic functions most people need such as getting online, running and downloading files and programs. Standard accounts don't quite have all the features admin ones do though - "[you can't change](#) advanced settings or install programs unless you type in the administrator password". This means for example if a virus tries to install itself on your computer, you'll be prompted with a popup asking you to confirm it, helping you to quickly notice something's up and decline the installation.



On pre-Windows 10 operating systems there is a third account type called guest. These are the most restrictive and are great to set up for use by guests to your home, relatives, kids, etc who will want to use your computer without worrying about anything being messed up.

4)

Keep Your Software and Operating System Updated



Pictured: Ninite

Ninite is a great free tool for making sure the software you commonly use is kept up to date. Ninite only covers programs that are free to use and/or download though, so you will want to make sure that any programs you pay for (i.e. QuickBooks, Photoshop, etc.) are set to update yourself.

All the software we use is basically guaranteed to be riddled with bugs and security holes. This is why manufacturers regularly issue updates to patch these holes and keep software working correctly, without leaving your computer vulnerable. Attackers use vulnerabilities to infiltrate systems and plant malware, which is why it's so important to update software as soon as possible.

To keep updates set for Windows, leave Windows Update set to automatically update unless you're specifically instructed not to (i.e. by a system admin or IT department). Other software also has options to install updates automatically or manually, these should be set to automatic for the best protection. We also recommend a website called [Ninite](#) to quickly and easily update common programs. Simply go to the website, put a checkmark next to the programs you wish to update, click the "Get Your Ninite" button, and an installer will bundle each application install/update into one window without you having to do anything else. Ninite can be used for both initial installs and updates of programs already on your computer.

5)

Practice Good Password Use



Check Your Password Security

Wondering if your password is up to snuff? Head to howsecureismypassword.net to enter in any current or potential passwords you're using to get an analysis.

Secure passwords are the bane of every computer user's existence. Create a super secure one and risk never being able to remember it, or create a simple one and risk security breaches. There are a few ways to ensure you're staying protected without too much risk. One growing in popularity is to use a password manager. While you will still have to create and remember one ultra secure password, it will remember and fill in passwords for all your online accounts. [Check out PC Mag's reviews of the best managers for 2016 here.](#)

Think “passphrase”, not password

If you don't want to deal with setting up a password manager (or need to create a strong master password), just start rethinking the way you make your passwords. One way to do this is instead of a *password*, think *passphrase*. When you were in school trying to memorize an ordered list, such as the planets in our solar system, most students were given an easy to remember sentence where the first letters of it corresponded to the first letters in the ordered list. So for our solar system example, to remember Mercury, Venus, Earth, Mars, Jupiter, Saturn, Uranus, Neptune, and Pluto, a good memorization sentence would be “my very empty monster just swallowed up nine planets”. You can use this same sort of technique to create a strong passphrase. Pick a phrase that you won't forget, for example “My husband & I met on October 5, 2010 & we got married on April 20, 2014.” Take the first letters, capitalization and all, and symbols and numbers in that sentence and turn it into your passphrase: “Mh&ImoO5,2&wgmoA20,2.” You can customize your sentence any way you like or to make sure it falls within program or website specifications, and it is very long, random, and near impossible to guess plus easy for you to remember! You can even write the whole phrase somewhere you'll remember as a reminder without fear of anyone guessing it's your passphrase.

Another trick that many are turning to is a string of random words in a nonsensical order. The randomness of the words and their order, and the length of the passphrase are what make this a strong choice. “[For example](#), “cat in the hat” would be a terrible combination because it's such a common phrase and the words make sense together. “My beautiful red house” would also be bad because the words make grammatical and logical sense together. But, something like “correct horse battery staple” or “seashell glaring molasses invisible” is random. The words don't make sense together and aren't in grammatically correct order, which is good. It should also be much easier to remember than a traditional random password.” Most people aren't very good at coming up with sufficiently random strings of words, so this website, [Diceware](#), provides a numbered list of words. You roll a dice and match the numbers you get with their corresponding word list. This ensures a completely random set of words and ones that you might not even have thought of! Keep in mind that “[Diceware's creators now recommend using at least six words](#) because of advances in technology that make [password-cracking](#) easier”. But even with six words, it is still easier to remember than most users' current passwords.

6)

Create and Maintain Backups

Types of Backups

- ❑ Hard Drive (HDD) – cheap, easy to find with flexible sizing, the hard drive is a popular choice. Keep in mind however that all hard drives will eventually fail.
- ❑ Solid State Drive (SSD) & Flash Drive – these drives are known for fast performance and long life and are finally dropping in price. They are still relatively expensive though (especially for large backups) and are better intended for performance versus storage.
- ❑ CD/DVD – these are extremely cheap and simple to store. But with backup sizes growing as storage technology advances, they are becoming less of a practical choice for backups (the largest DVD size available is 8.5 GBs double sided – most computers have a minimum of 250 GBs of storage) They are also notoriously easy to damage.
- ❑ Cloud Storage – available from anywhere and any device, you’ve probably heard plenty about cloud storage. It’s become more secure as well, and convenience doesn’t get any better. Downsides are that backups can take a long time and bog down your PC’s performance. They also require a fairly good internet connection, and incur recurring costs.

Don’t learn the hard way that you should have made a backup.

Most people have valuable pictures, music, documents, and files on their computer that either can’t be or would be very difficult to replace. Backups used to be a pain to create, but they are easier and more flexible than ever. If your computer is ever too infected for a standard virus removal or your current hard drive fails, a backup will be the only way to save all your data. Whether you choose to use an external hard drive or a cloud service for your backups, making one before you need it is the best practice. It can also come in handy during a security breach or hack, you’ll be able to quickly factory reset your computer and reload your backed up data. This eliminates the worry that someone will gain access to your files.



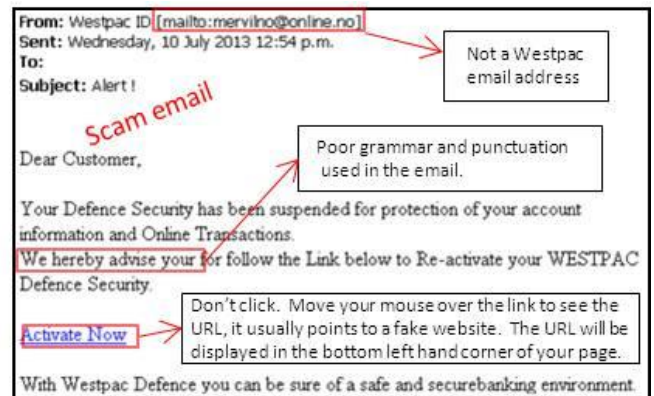
7)

Beware of Scams

Scams have been around for longer than the internet, but have found a popular home online. Phishing scams have become very well known – “a phishing attack is the equivalent of someone calling your phone, claiming to be your bank, and asking for your credit card number. Your bank would never call you and ask for this information, just as they would never email you and ask you to send the information in an email”. Phishing emails can appear to come from someone you know, your bank, an online retailer, your credit card company, and just about anyone else that handles your financial information. These companies have strict rules against asking for your information and will never do so in an email.

Another scam that has been very prevalent lately is what we call the fake tech support scam. A “customer support rep” will call you, claiming to be from a well know company like Microsoft or Norton, and tell you that they’ve found all sorts of issues, infections, errors, etc. on your computer. They’ll happily help you clean up your system if you pay them and allow them remote access into your computer. This can also come in the form of a scary looking popup on your machine telling you the same, and to call the displayed number immediately for help. This is always a fake – unless you have specifically paid for a monitoring service, no company has the manpower or resources to track every single user of its software. Never let these scammers onto your computer or pay them.

Scam Examples



Source: <http://www.westpac.com.au/>



Source: <https://blog.malwarebytes.org>

From: ANZ [mailto:notification@anz.co.nz]
Sent: Tuesday, 24 March 2015 1:17 p.m.
To: notification@anz.co.nz
Subject: Payment Notification

A payment has been made to your account.

To view the details of the payment, please open the attached PDF file.

You may require Adobe Acrobat Reader on your computer to open the PDF file.

Please do not reply as this email was sent from an unattended mailbox
Note: This message and any attached documents are for the named person's use only. It may contain confidential, proprietary or legally privileged information. No confidentiality or privilege is waived or lost by any miss-transmission. If you receive this message in error, please immediately delete it and all copies of it from your system, destroy any hard copies of it and notify the sender. You must not, directly or indirectly, use, disclose, distribute, print, or copy any part of this message if you are not the intended recipient. Omniston Hospital reserves the right to monitor all e-mail communications through its networks.

Source: <http://www.anz.co.nz/resources>

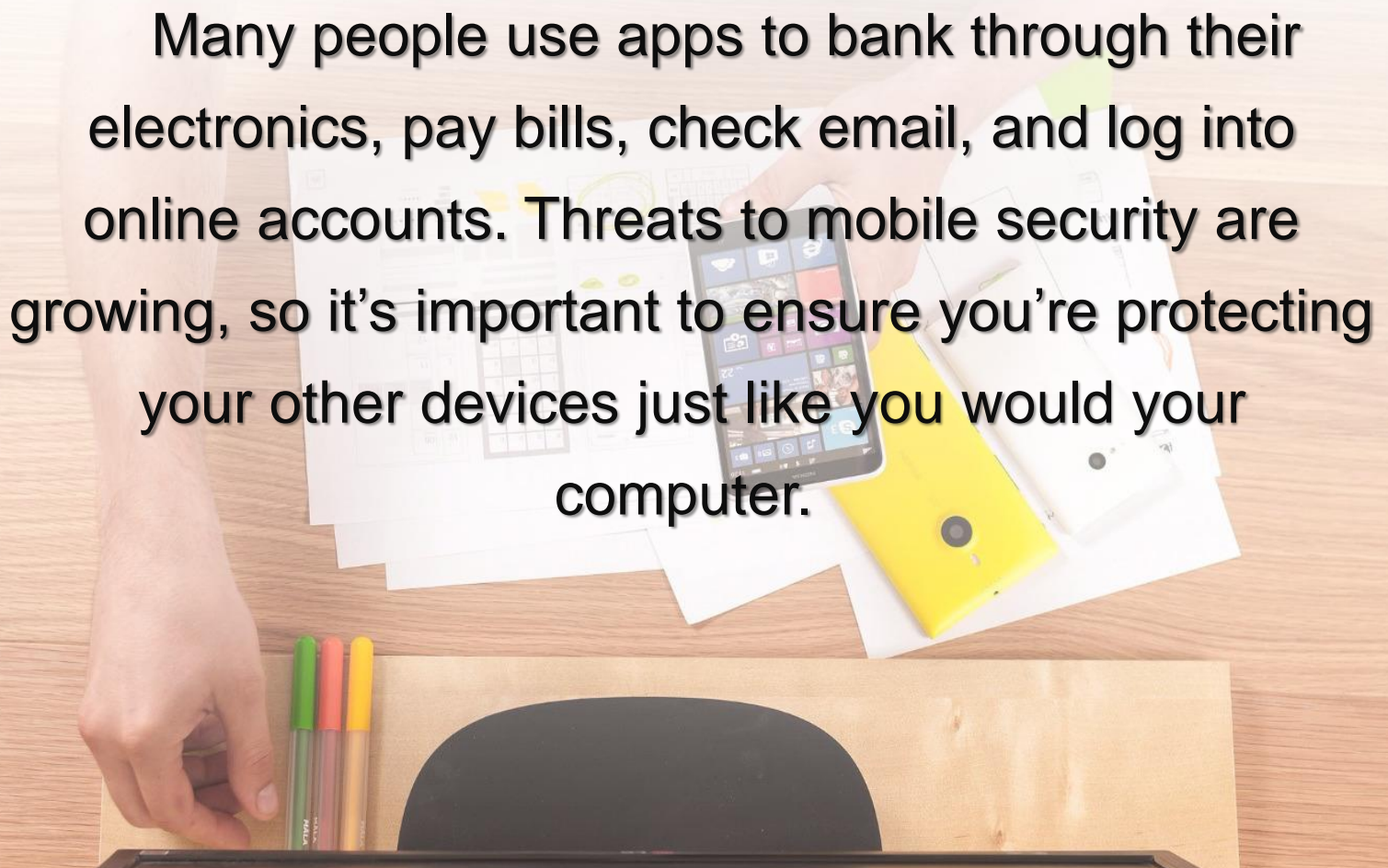
Most importantly, stay aware! Keep up to date on new scams and viruses going around and learn how they spread. Snopes.com has a [great webpage here](#) on virus hoaxes and realities.

8)

Protect Your Phones and Tablets

Phones and tablets are computers too, and can fall victim to infections and attacks.

Many people use apps to bank through their electronics, pay bills, check email, and log into online accounts. Threats to mobile security are growing, so it's important to ensure you're protecting your other devices just like you would your computer.

A hand is shown holding a smartphone over a desk. On the desk, there are several papers, a yellow smartphone, and a white smartphone. The background is a wooden desk surface.

Electronic Security App Links

- ❖ Protection/Antivirus Software – [Android](#), [Apple](#), [Blackberry](#)
- ❖ Extra Security Solutions – [Android](#), [Apple](#)

9)

Prevent Spying Through Your Microphone and Camera



Webcam Guards for Laptops and Phones

A more elegant way to ensure you're not being spied on, without leaving sticky tape residue on your devices. The one pictured is from thewebcamcovers.com.

Built-in webcams are great tools for video chatting, but can be hacked into without your knowledge. Normally an indicator light comes on when your webcam is activated, but this can be bypassed by someone with the know-how and used to spy on you and your surroundings. Many people choose to simply tape over the webcam when they don't need it.

As well as taking advantage of your webcam, built in microphones can also be hacked into to listen in on conversations. This is rare so don't feel too paranoid, but it has been known to happen. Laptops generally come with the microphone enabled by default. To turn yours off, launch the *Sound* app from the control panel or by typing "sound" into your Start Menu search bar. Click the *Recording* tab, select your laptop's built in microphone, click *Properties*, and change the *Device Usage* drop down to disabled.

10)

Clean Up After Yourself

When your computer or phone's time has finally come, ensure that you're not sending it off with all your information.

Even deleting everything off your computer or reloading the operating system doesn't mean someone knowledgeable can't recover it. If you aren't planning on donating the computer and the hard drive won't ever need to be used again, you can take the drive out and physically destroy it.

If the computer is being donated or gifted to someone else who will more than likely want a usable hard drive, you'll want to turn to software methods involving a secure-erase. There are a number of programs available for this, and different ones depending on the type of drive you're trying to wipe (hard drive, solid state drive, flash drive).

Secure Wipe Applications

- [Darik's Boot & Nuke \(DBAN\)](#) – free software recommended for slightly more advanced users as it requires burning to and booting from a CD. Will erase the contents of any hard drive it detects, so ensure you only have the drive(s) you want to erase in the machine when using.
- [Parted Magic](#) – multi-function tool for wiping, partitioning, benchmarking, cloning, and recovering data.
- [MediaTools Wipe](#) – professional level multi-drive secure erase utility.
- [Eraser](#) – very secure wipe utility, completely removes sensitive data by overwriting it several times.

Bonus Tip

Disconnect From the Internet (when it makes sense)



While a majority of computer usage is online these days, unless you have something like a server that needs to be connected to the internet 24/7, it is both safe and practical to disconnect from the internet when it's not being used.

“[Hackers](#) tend to prefer to exploit ‘always on’ connections, and if your internet connection is more sporadic, you’ll be less attractive to them”. Hackers and scammers likewise can’t remain connected to any computer that’s completely disconnected from the internet. This is helpful for things like the fake tech support scam that we mentioned above. If you’ve let someone into your computer and realize it’s a fake while it’s happening, you can disconnect from the internet to force them out of your machine. No one who isn’t physically in front of your computer can connect to it without an active internet connection, making this a powerful way to ensure nothing nefarious is happening behind the scenes of your operating system. So whether you’re worried about a possible security issue or just want to make yourself less of a target, turn those devices off when you don’t need them! For computers that are directly wired to your router via an Ethernet cable, you can also unplug one end when you don’t need online access to allow use of the computer while not having to worry about unknown people having remote access.

 **TECHVERA**
866.615.4335
Contact Us

We hope these tips help you feel safer while online and using your computer. We’re always here to help! Contact Techvera for professional assistance with any computer issue.