Safety, Security, Privacy

In the age of widely distributed electronic data we need to protect our data and ourselves from risks online and on all our devices. With a little bit of information and a large dose of attention and common sense we can ameliorate a large amount, but not all, the danger of living in a modern information society.

These articles will separate the risks and procedures into three overlapping categories of **Safety**, **Security**, and **Privacy**.

- **Safety** applies largely to protecting data from accidental or malicious loss or damage. Getting hit by a bus while crossing the street is not included.
- **Security** gives techniques to store and share certain sensitive data with those who should see it while not also sharing it with those who shouldn't.
- **Privacy** will primarily help avoid having people looking over your shoulder or following you around and gaining information by correlating relationships.

==== = ====

Safety, Security, and Privacy

Safety starts with two best practices that have been around since, if not dawn of personal computing, at least from soon after. They are antimalware and backup. Although install-and-forget utilities can go a long way toward satisfying their need, it may take more than just accepting the settings and programs that come with a new computer. The software solutions need to be combined with policies and procedures to ensure they are allowed to perform their jobs. Sometimes a computer just fails from either mechanical or software issues.

Antimalware

__Malware__, and it's "__anti__," refers to what used to be called "__virus__." In fact, there is a whole constellation of software that act in various modalities to cause problems with the desired operation of a computer, and are now called malware.

Major antimalware providers often refer to their flagship consumer products as "internet security." When they perform a system scan they can claim to "protect you" from tens of thousands of "infections." Most of these items are internet cookies, including those that allow a website to identify you as a returning subscriber or customer with a shopping cart.

The good news is that problems with classical viruses are largely solved. Most modern operating systems are hardened against the type of malware that plagued individuals and businesses around the turn of the century. Windows 10 comes with Windows Defender; not the best, but generally an adequate antivirus program. Windows Defender or Microsoft Security Essentials are the same program. Under one name or the other, it is available for Windows 7 and 8 also.

If you have a basic antivirus program installed, the biggest concerns are for users to develop good practices that don't allow the bad guys to get a foothold into their computers.

How to avoid malware

Don't allow malware to get installed.

Most malware, and particularly the most destructive malware, today requires some sort of user interaction to get activated.

When you say "yes, go ahead;" you've allowed the malware to do what it wants to.

Actually, you won't see a message to "install this virus in your computer." More likely the message will be something like "install this plugin to view this web page" or "download pictures in this email." Some programs will install themselves merely from your action of opening an infected document.

Once you enable actions like those, the bad guys can get around other protections built into the operating system and even some antimalware programs.

1) <u>Be a limited user.</u>

One protection is to always log into the computer as a *standard* or *limited* user. Most programs (undesirable or desirable) require *administrator* rights to fully access the contents of the computer. If malware encounters a limited user the evil it can do will be limited – although it still could be devastating.

When you first set up a consumer Windows computer you have to create a user ID. This first account is always an administrator – there must be at least one administrator for the computer. You can then go to the <u>user accounts</u> section of Settings or Control Panel to create more accounts. All of the accounts should have a password so malware, or inquisitive children, can't stumble or easily break into files not intended for their account.

Our recommendation is to create at least 2 administrator accounts separate from standard accounts for all the regular users. When you really *need* to have administrator rights to install a program or change settings, Windows will give you a dialog box to enter your admin password and temporarily allow the action.

It is important to know what at this point is asking for permission. If the description in the dialog box is not clear and you have not just started to make a change, don't allow it. The worst that will happen is you'll have to restart an install you do want.

2) <u>Practice safe surfing</u>.

Being online is the easiest way to deliver malware to susceptible computers. The malware finds the computer when a user encounters an infected webpage. Then something on the page – a picture, document, ad, link, search, even something "invisible" – delivers the punch. Don't forget that any object on the page – not just words in blue – could be a link to something else.

The first rule of safe surfing is *doing go there*. If you don't need a particular product or research, if you're not interested in a topic; don't click on it. If you're just killing time, read a book; don't randomly surf video, chat, or gossip sites.

Especially if you must participate in dicey activities, consider using a sacrificial computer to do so. Pornography, unregistered pharmaceuticals, gray-market merchandise, special purpose software, and other products may not be illegal. But they often exist in a shadow market that also attracts less benign activities. A search or a site may be as likely to host malware as what you really want.

When you are using a search engine, be aware that the top links are usually paid advertising. There may not be a good way for the site that's showing the ad to know whether the destination is legitimate or not. Always give preference to advertisers or sites you are familiar with or that have good reputations.

If you're looking to download software from the internet, be extra careful that you get what you wanted. Many of the sites distributing multiple types of software clutter their pages with other products than what you came for. Read the "download now" button carefully to ensure that you're not getting something else. Even major publishers will try to "co-install" other products to earn a commission as you install their free version.

Much of what you get in these cases is not malicious; but it is unwanted. It may slow down your computer or try to direct you somewhere you don't want or need to go.

3) Practice safe email.

Most email is essentially a web page so all the rules for web surfing apply to email. Don't give anything that might be suspicious permission to run. Don't click on links before you've vetted their legitimacy. And especially, don't even touch anything that doesn't apply to you.

All email clients will display the sender and subject line and most can be configured to show a preview of the message before you open it. If you do open a message, it may block pictures and links until you explicitly allow them.

Take the opportunity to delete unwanted messages before you read it. Estimates are that 80% to 90% of email traffic on the internet is spam. Most of this is blocked by your mail provider before you even see it. By looking at sender and subject lines you can delete spam and other unwanted emails; spending only seconds each on 20% to 80% of the emails that do make it to your inbox. Not only will you protect yourself from potential malware, you'll also save time.

For the best safety, you can configure your email client to only display your messages as text only. This will strip out anything that tries to run on its own or is clickable or otherwise hidden or obfuscated. It also destroys the richness of the message with no pictures or textual formatting. Links that were part of the text will still be displayed and may be clickable, but you can see the entire link before you click.

Many businesses – particularly those that might accept customer service requests by email – have a policy that they don't open attachments or click links in an email. This is, of course, the safest policy. Barring that level of strictness, you should validate any attachment you open.

In general, webmail is likely to be safer (not "safe") than bringing your whole mailbox into your computer. Malware that tries to run automatically may be restricted to your host's system and not yours. Google's Gmail is known to make an effort to protect their users. Presumably other major providers have followed their example.

Don't forget that anything said about email also applies doubly to other messaging methods. Since their proliferation is relatively recent the programs are less mature in their inherent safeguards. They also demand extra care precisely because they are used more casually. If your correspondents are lax, you have to diligent.

4) Other risks.

There are a myriad of other ways malware can get into your computer. If you are aware of where there might be risks, you are less likely to step in the mud hole.

Any time you connect to the internet, your computer is at risk of attack. The first point of protection is a router which acts as the front door and blocks anything you haven't invited in. Fortunately, most computers connect through a local router and have that protection.

However, when you connect to a public internet portal such as an open WiFi, you can't tell for sure that there is a router. Even if there is a router, if it's controlled by someone you don't know it may be acting maliciously. Even in your favorite coffee shop there could be a rogue

WiFi pretending to be the merchant's. When Windows asks if a new network is home, work, or public, it's trying to protect you from some of the risks between your computer and the greater internet. Always select "public" unless the network is controlled by someone you know you can trust. This is especially true at large public facilities such as a hotel or event facility. Consider not using the free public WiFi, instead relying on a cellular connection with your own account or even forgoing being online for the interim.

Even at home, when you set up a program that automatically updates from the internet, when you install a game machine or any other Internet of Things device; you've opened that door a little, to those apps or devices. Once malware can attack that device, it may be able to jump to other devices on your network.

The original method of infection was file sharing. Know your source, but verify its content any time you bring a file you did not create into your computer. Historically files were shared on a physical medium: a diskette or thumb drive. Then they came over an electronic connection: attached to an email or downloaded from a website. Now files can be automatically inserted onto your computer through file sharing or subscription services. When you install one of these services, you are allowing someone else to directly transfer files to your computer without your further permission or knowledge.

Nothing is certain, but it's always advisable to run an on-demand virus scan on every file you receive from anywhere but a trusted source. Your installed antivirus should be doing so as it comes into your computer, but it's reassuring to get that green check explicitly if you have any doubts. You can do an on-demand scan with your usual software or, many vendors offer a free stand-alone scanner. Under any circumstance, be sure it has up-to-today updates to its virus signatures.

We admonish you to always know your source before you give anything a chance to attack you. Unfortunately, just about any source identity can be spoofed. This applies to web addresses, email senders, information sources, and even critical website pages. Read the "No phishing" * post for how to identify a bogus URL.

5) Apps that keep you safe.

Some programs have been notoriously susceptible to allowing malware into your computer. Some of the riskiest over the long term have been Internet Explorer, Microsoft Office, Adobe Acrobat Reader, and Adobe Flash Player and Oracle JAVA These are extensively used when you access the internet. This listing is not to indict specific products – they are most likely to be attacked because they offer the largest number of potential victims. Other programs may have as many vulnerabilities but not as many attacks because value of the return for the attackers is lower.

You may be able to reduce your risk by finding alternative programs for the same function. There are a number of other internet browsers and .PDF readers to substitute for the big names. No one matches the wealth of functions and breadth of experienced users as Microsoft Office, but there are alternatives; both to install on your devices and to use online. And newer programming techniques can provide most of the functionality of Flash and JAVA on the web.

Meanwhile, many contemporary programs work to protect you from classical risks. Most browsers will not run risky plug-ins automatically but require you to confirm the action. The same applies to .PDF readers and Microsoft Office. They usually warn you before clicking on a link or running an automated action. It's a small nuisance for the user, and a big one for the malware creators.

No app can protect you against the newest malware if you're using an old version. Just as you have to change the oil in your car, you need to ensure *all* of your software is updated regularly. Your OS and Microsoft Office are usually configured to automatically update every month. The major browsers do so whenever new features or protections are available. Other popular programs may give you an alert that you need to go to their website for the update. Still others may be updated occasionally but you'll never know it unless you check on it periodically.

6) <u>What about cookies</u>?

Cookies are bits of information websites store on your computer and your computer gives it back when the same website asks for it back. Every browser keeps its own cookies; often some place deep in the system.

Antimalware and other programs might scan your computer and report "we found 10,372 potentially risky files...". Usually when the number is this large they are reporting all the cookies they found. Many of these will be innocuous such as identifying your shopping cart at a retailer or keeping you logged in to a blogging site. Others may be "undesirable" such as ensuring you keep getting ads for camping gear or links to cat videos; but will only lead you to legitimate websites that just waste your time.

A few of the cookies may be truly malicious or dangerous such as containing your identity at a valuable website or marking you as a likely target for other attacks.

The best remediation for cookies is to periodically purge your system. Most browsers will allow you to remove all or individual cookies.

If it allows you to <u>block third party cookies</u>, you should choose that option. Third party cookies came not from the news site you're reading, but the ads alongside. While the news' cookies can only be used by them, third party cookies allow the ad publisher (not the advertiser, but the agency that places ads for thousands of products) to track you from the news site to a shopping site or anywhere else they have an ad.

Protection and remediation

You've done everything possible to avoid an infection but something that may infect your system still slips through. But don't worry because your computer is doing its best to stay safe. These should be thought of as the last line of defense, not the first.

1) <u>Active antivirus</u>.

Antimalware (or "antivirus") software watches your computer continuously for something to come by that it identifies as unfavorable. When it sees that something, it prevents the action from having any effect on your system.

You're probably aware of the Norton / Symantec or McAfee antivirus suites. There's a good chance one of them was installed on your computer when it was new. You're protected now and don't have to worry any more? *Wrong!*

The preinstalled software is probably just a short-term demo version. The reason it's there is to entice you to *buy* a subscription. If you don't do so, in one to six months the demo subscription will expire.

Aside from a reminder to presubscribe, you may not notice any change in your computer. The icon is still on your desktop and the program opens when you click on it. Unfortunately, malware is constantly changing and the antivirus publishers are constantly sending updates so it will hopefully recognize the new malware – as long as you keep your annual subscription current.

But you don't have to use one of the Big Two. There are many other publishers of antimalware, some of which are well rated and free. By far the easiest free solution is Windows Defender (sometimes referred to as "Microsoft Security Essentials") from Microsoft. It's probably already on your computer, but may not be activated as long as you have the demo program.

Running more than one antivirus at a time can cause problems so you need to *completely* remove the existing program before installing another. Because of how antivirus works, uninstalling it can be difficult. You should research the process and, possibly, use a special utility to do so. Then you can install the free program.

Remember that between uninstalling one antivirus and installing another you are unprotected. Do this only while you're on a trusted internet connection and don't run any other programs until the new one is up and running. Allow sufficient time as the process will probably require multiple reboots and some time for the new program to get its updates since it was created.

2) Updates.

As we've already pointed out, most programs need to be updated somewhere between constantly and occasionally to avoid possible exploits. Fortunately, antivirus is in the class that takes care of its own updates.

For all the other programs on your computer though, you should occasionally check to verify that they are getting their updates. That includes verifying that your antivirus is updated and running normally. A virus could still slip through the protection and disable the antivirus so it can do its thing unimpeded.

3) Firewalls.

Your router acts as the best firewall you can use against the internet. However, you want to ensure there is a firewall running on your local computer to protect you from threats that are already inside the router. These could come from other computers or devices such as a game box. It's also possible someone could have hacked into your WiFi from nearby and be infected.

Verify that your computer's built-in or add-on firewall is running. Search "firewall" from the Settings panel and verify that it is on for all networks.

Some security suites may include a firewall and when they are installed they turn off any other firewall. If you uninstall one suite to use another one, it probably won't turn another firewall on. Always check the settings that either the OS's firewall or another firewall is running.

4) Protect your network

The router is your first line of defense against something coming in to your computer from the internet. But if anything you don't control can get on your own network it can't do its job. There are four risks from inside your network: your computers and portable devices (phones), your "non-computers," guests' computers and devices, and outsiders breaking into your network.

First you must control what connects to your network. You know what devices you plug in, but most devices now connect through WiFi. You may install "non-computers" and then forget that they connect to the internet and can get infected without you noticing.

Of your computers, you know (or should know) that they have the best protection available and everyone who uses them has been trained with good practices. Similarly you may have close guests that you also trust to be on your network. That may not apply to your children's friends or your poker group. You allow them access to your guest network or keep them out with a good password on your WiFi.

The good password will also slow down drive-by hackers who try to attack you from the curb. In addition, you need to disable WPS connectivity on your router. This is a simplified way to connect to the internet intended for devices like printers. The device or computer can connect when you push a button on the router or use a separate 8-digit number instead of a password. Unfortunately, this system is trivially easy to break into.

“Non-computers” are devices like TV boxes, baby monitors, and security cameras today. In the near future they will include the entire constellation of Internet of Things. These might include thermostats, door locks, lighting controls, and, famously, your refrigerator. Their problem is that you invite them onto your network but have no control over what they bring with them. You can’t install an antivirus or even know what information they’re sending out about you. Again, you need to connect these devices to your securely separate guest network.

The best way to create a guest network on your network is with the three router solution. This can require some effort to set up and will require additional equipment and cost. Alternatively, you may use a router that features a separate guest network for the devices you don’t want on your primary network.

5) On-demand scans.

We suggested running a manual virus scan whenever you receive a file from an unknown source. If you have a flash drive or non-commercial disc, you should scan the entire device immediately after inserting it. Don’t forget that a phone or other portable device could also harbor malware waiting for your computer.

The easiest way to start a scan is to *right*-click the file or removable media in doubt and choose “Scan with [your antivirus tool].”

Your running antivirus tool usually schedules a periodic scan of your entire system – usually during an unusual time such as Sunday overnight. Open the program and you can change the schedule to ensure you don’t turn the computer off at that time. You can also start an on-demand scan of the entire computer at any time. Be aware this may take hours and slow down whatever else you are doing. But the nuisance is much less than actually having malware.

If you think you are infected but your usual antimalware can’t find it, you may be able to eliminate it another tool. Every program misses some malware that another might find. Most of the major antivirus vendors offer a tool for a one-time scan – often for free. Malwarebytes is a favorite for this purpose. Some vendors may also offer a tool that creates a self-booting disc so you can scan without starting your OS. This is valuable because better malware can hide from normal scans.

Whatever on-demand scanner you use, you want to be sure it is functional and not corrupted itself. You should download it from another computer that is known to be clean. Then run any updates for the tool so you are sure you are protected from the latest risks.

A special case: Ransomware

A generation ago, the purpose of malware was simply proving it could be done, or at worst, vandalism. With the ubiquity of electronic data and the internet, the value is stealing your data. Whether it’s a million credit cards from a retailer, information from a business, or a cute handle on a social site; the hacker wants something you have.

More recently the scariest attack is ransomware. Its creators don’t just copy your data for their use, but take the use of it away from you. Then they offer to give your data back – for a price. What would you pay to get back your children’s baby pictures, ten years of emails, or your financial records? The price for an individual usually runs between $300 and $1,200. If a business gets attacked the price quickly runs into tens of thousands of dollars.

The ransomware most often is delivered in an email with a link you have to click on and allow the program to run. Unfortunately there are also means to deliver and install it merely by displaying an ad on a website.

If you get hit with ransomware it encrypts all of your data files. All of your programs still work. The files are still sitting on your computer. But all the documents, pictures, music – anything potentially irreplaceable – are just gibberish. Everything, that is, except a message to send the attacker money.

Although some versions of ransomware don't work correctly – either the encryption is easily cracked, or even the perpetrator can't decrypt it – most attacks deliver on their promise. Your data is really gone and you will get the key to get it back if you pay up within the deadline.

If you are getting hit with ransomware, **unplug your computer immediately**! Most people should not try to recover their data but call a computer professional. And remember, there may be a clock ticking on how long you can wait to pay the ransom before the perpetrators "kill the hostage."

If you have a good backup of everything you value, you may be able to thumb your nose at the criminals. But, if your backup system constantly backs up every change as you make it, it will dutifully backup the corrupted files. To reliably recover most of your data you need to have a backup process that saves not only the changes from an hour ago, but also a copy from yesterday or last week.

A final word.

Years after he first published them, the best protection against malware is still found in Brian Krebs' 3 Basic Rules for Online Safety:

Krebs's Number One Rule for Staying Safe Online: ***"If you didn't go looking for it, don't install it!"***

Krebs's Rule #2: ***"If you installed it, update it."***

Krebs's Rule #3: ***"If you no longer need it, remove it.***"

Everyone should read his complete blog posting elaborating on these rules. Living by these simple practices can protect you from many of the risks of using a computer.

==== = ====

Backup

Backup is a form of digital insurance: use it to protect something of value or usefulness that you can't afford to replace. Economic insurance may pay for the physical computer, but there's all your data that may qualify as irreplaceable if electronic files are lost. To protect this, you make a copy of your files and protect them from physical destruction.

Why do you need backups? Storage media may seem totally reliable, but any single component could fail after 10 hours or 10 years of use. Equipment could be damaged in an accident or maliciously. Portable, and even desktop computers, could be stolen or lost. Files could be inadvertently or intentionally deleted or overwritten or attacked by malware.

Under any circumstance, you may want to get back something you worked on yesterday, last month, or last year. There may even be something you haven't looked at for decades and realize you wish you had again. An example may be your parents' wedding picture you scanned once and forgot about until your home had a disaster.

The classic mantra of backup is that you want *3 copies of your data, on 2 different types of media, 1 of which is offsite*. You might also want a copy from *yesterday, last week, and last month* for active data such as your banking database or the manuscript to the Great American Novel. This will protect you if you unintentionally change or delete a critical file.

What to backup

If your hard drive fails or the computer is destroyed or lost, you will either get Windows preinstalled or have to reinstall it on a new drive. Most new computers don't provide discs for the original installation but include a utility to create the discs for a complete restore. This should be one of your first tasks after you get a computer up and running.

Similarly, you can't just copy software, but must install it on the new drive. It's tedious, but you'll install the software from the original discs or download it again from the distribution website. Either way, you should keep an electronic file listing your programs, the source of the installation files, and their serial numbers and put this file in a location that is backed up. You may also want to record program customizations you have made to speed up your work. Don't forget the email accounts built into your mail client and any registrations you may have that are automatically delivered to their client.

While you're at it, if you use a password vault or other means to document your passwords, be sure that a recent copy of it is backed up. If you trust your browser to store your passwords, use something else. But do be sure to save your browser's favorites so you don't have to recreate them.

Beyond the business end of the computer, you want to back up your documents and media. If you faithfully save all your work in **My Documents**, that seems simple. Don't forget there are document folders for each user on the computer and a public documents folder as well. In addition, music, pictures, and videos may be in a different folder and may also be distinct for each user.

That should cover the files that you *actively* saved. However, some programs don't obviously ask where to save their data. In my experience, programs that create their own database are particularly problematic with hiding their files. Some examples of the class might include the likes of Quicken, Outlook, or iTunes. Recent versions of these programs are more likely to conform to the **My Documents** standard, but be sure you know what they are doing, especially if you upgraded from an older program.

Another rogue player for randomly stashed files could be … you. Remember that the **Desktop** is a place for shortcuts, not files. And the **Downloads**, **Favorites**, **Recent**, and other places you go frequently for files may not be in My Documents, or any other place you can easily grab them. They may even be virtual locations that actually point to files in many other real locations.

How to backup

1) <u>Make and keep your own backups.</u>

You could just copy important files to a flash drive or DVD and stick it in your pocket. But that depends on you being reliable in identifying files, regularly copying them, and protecting the disc you copied them to. It's best to use an automated program that will take responsibility for making daily or weekly backups with settings that were previously configured. Then the most you have to do is to change the media periodically.

Most programs start by backing up everything you have selected and then, on a schedule, back up only the files that have changed. Restoring all your files used to require going through all the incremental backups and finding the most recent of each; but smarter databases have resolved that issue.

Some programs will create a *system image* that would allow you to recover Windows and all your programs as well as current data. Using this backup as default could result in a huge amount of data that you have to find a place for. These should always go on one or more dedicated external hard drives. You should make an image of a new computer after installing and customizing all of your programs and updates. Then you can repeat at long intervals as a base to restore your computer in case of a catastrophe.

2) <u>Keep your data in the cloud.</u>

Microsoft, Google, Dropbox, and many others offer services that allow you to store some of your data in their data farm. Some may require a continuous internet connection while others also keep your files on your local drive so you can work offline if needed. Because they follow data center best practices, you should be able to trust that your data are adequately backed up and protected against physical or software disaster.

You may think that qualifies them as a backup system, but using them doesn't isolate your working data from backup. Because their product is synchronization, as soon as you make a change on your computer the modification is almost immediately transmitted to the cloud. While this protects your final exam if someone steals your computer in the library; it also means if you accidentally delete your research folder, you're out of luck.

You also have to be able to trust the provider of these services. Historically, many have gone out of business suddenly; giving minimal opportunity to make other arrangements for preserving data. Even a reliable provider may change policies and pricing on a moment's notice, so you need to be aware of any communication from them.

3) <u>Use a dedicated backup provider.</u>

A close relation to the cloud file sync-and-share services are dedicated cloud-based backup systems. Typically they monitor selected folders and mark them whenever files are changed. Then they may upload them immediately or on a schedule such as overnight or once a week. While they may have a well-designed online interface to recover individual files, you would have to download them manually. Ideally, if a file is deleted, the latest version should remain easily available for at least 30 days. If a file is corrupted, finding the last good version should be possible, but may not be quite as simple.

Using these cloud services can be almost as easy as the sync services or could be strictly for high-end administrators. At the simplest, you create an account, install their app, and forget about it until you have a disaster. Others sell you the program and then require you to select a storage provider for your data and pay the provider directly. Companies such as Amazon and Microsoft sell the storage per gigabyte per month in a market designed for enterprises but accept small accounts as well.

<u>Backup conclusions</u>

Whatever your choice of mechanism, the important point of is that your critical data should get backed up frequently and consistently. The goal is to protect against equipment failure, physical damage, and malicious or inadvertent corruption. In other words: If you delete a file by mistake, if your hard drive fails, or if your house burns down. If your data are on a laptop, you need to be particularly diligent with frequent backups because the computer is inherently more susceptible to damage or theft.

And don't forget unique data on your phone. With this ultra-portable device becoming many people's primary computing device and camera, be sure that everything you care about is copied to the cloud at least as often as you connect to WiFi. Losing your electronic communication archives may be a nuisance; losing the photos of a significant part of your life could be devastating.

Oh, and save your documents frequently. Don't type for an hour and then trip over the power cord.

***Disclaimer**: I am a dealer for Carbonite online backup not because they pay the best commission, but because, after research, I felt it* *was the best solution for myself and most personal users. If you decide likewise, please contact me to purchase your subscription or use the link http://s.zaitech.com/CarboniteHome.*

Computer failure

There are times the computer just won’t run, or it runs very poorly, or fails when asked to do something it could do yesterday. This could represent a simple – or very involved – mechanical or software problem. There are some basic best practices that could have alleviated these issues. But usually this is not anybody’s fault; it just reflects the complexity of a computer and its installed software.

While these comments may not protect you from a catastrophic failure, hopefully they will allow you to alleviate or mitigate it and reduce your frustration. There’s a difference between having enough warning to boot your computer once or twice more and being in the situation of “I hate getting a new computer.”

These tips generally apply to desktop and portable computers with a typical consumer configuration. Business-grade, gaming, specialty, or significantly customized computers may need or deserve other care.

Simple things

There are a number of minor components that can keep a computer from getting to the logon screen; most of which can be inexpensively replaced in a desktop computer by someone comfortable with a screwdriver. Portable computers have the same components, but they may not be accessible without special tools or skills. Check with your manufacturer’s website for troubleshooting tips. Then research online at the manufacturer’s site and elsewhere for replacement procedures.

External components.

House power is an obvious starting point if nothing comes on, but the mouse, keyboard, and monitor also may be failing and causing problems. Fortunately these items are generally generic and you can test them by borrowing them from a different computer. (Windows and Apple accessories may not be interchangeable.) Don’t forget to test any removable cable as well as the primary component.

Internal components.

If the case can be opened without special tools, there are a few internal components that are easily replaced. Before working inside a computer, always disconnect it from the power (remove a laptop’s battery, too) and hold the power switch for 15 seconds – twice – to remove any residual charge. Then remove any static charge on your body by touching grounded metal before opening the case. Be sure you know how to reinstall anything you take out or unplug. A good tip is to take detailed pictures and label everything you touch along the lines of “cable A” to “socket A” and “component B” to “slot B.”

There is a small **battery** that protects the circuitry that gets the computer started. If this fails, the result may be as minor as the clock being in error or it may not allow anything else to move forward. Check your documentation for instructions.

Bad **memory** may give anomalous problems if as little as a fraction of one chip out of 16 or more has failed. There are utilities available from your manufacturer and elsewhere that will give your memory a deep test to find these flaws. Replacement is straightforward and individual units are inexpensive. Often just removing and reseating the module will solve a problem. Be careful because you may have to remove other components to remove the modules and the sockets can be stiff.

Memory can also be an easy and inexpensive upgrade to improve performance. Always check the recommendations first as your computer may not support more memory. It may also be constrained by other components that would reduce the value of upgraded memory.

When the **hard drive** fails, it has usually given warnings that many users may miss. Some indicators may be an increase in the time to boot up or save files or errors reading random files. Even an unexplained error with a single program could indicate a damaged part of the drive. Problems could be caused by damage from heat, vibration such as carrying a laptop while it's running, or simply age. Time is especially wearing if it has seen a high number of power-up cycles such as turning off your computer every time you walk away from it during the day.

If you recognize these symptoms, the easiest solution is to clone your system to a new hard drive before it fails. Many programs can do this for an experienced user or any computer shop should do so for a moderate labor charge. Once you have a total failure, your only option may be to reinstall your operating system and applications and restore your data from your backup.

SpinRite (https://grc.com) *is a reliable program to maintain spinning and solid state drives. It has even been known to resurrect totally "failed" drives, at least long enough to retrieve critical data. While it may seem expensive, the cost is far less than it might be for a third party to recover your data or the nuisance of restoring it from a backup.*

Disclaimer*: I recommend SpinRite because it works. It is also unique in what it does with no effective competitor. Also, because the publisher has a plethora of free apps and information that was the impetus for much of this book.*

A failing **power supply** could result in a hard stop, or other problems after the computer starts up. Although the replacement is strictly mechanical, it has many cables connected at many points and working inside the case you could disconnect or damage other components. Since it's external, between the wall and the computer, the most difficult part of replacing a laptop power supply is paying for it.

Heat

Even before issues related to bad quality power such as spikes; heat can be a major degrader, and eventually killer of electronic components. It is a particular problem if there is insufficient air flow such as in a laptop or very compact desktop computer. Even a large tower can overheat if crammed with high-performance components or clogged with dust. See my blog post for one description of the problem.

In every computer from a room-sized mainframe to the one in your pocket the major sources of heat from the main processing unit traditional spinning hard drive when they're working hardest. The battery in a portable device or laptop also releases heat when in use and much more when it's charging.

Fortunately, heat represents wasted energy and every manufacturer wants to increase their efficiency. Each generation of chip uses less energy; except the savings are usually counterbalanced by including increased capability or speed. Solid state hard drives (SSHD) are moving into the consumer market and fewer systems need the mechanical components of a spinning disc.

Unfortunately, more devices now are portable and users demand more performance and more battery life in less space with less weight. Manufacturers have to cram more chips in less space and seal it with no cooling airflow. Then they push the battery technology to store more energy and combine it with higher charging rates. All of these strategies stress the device's capacity to eliminate damaging heat.

The best way to protect against excessive heat is to allow it to dissipate into the environment. For a larger device, don't restrict airflow to fans, vents, or the case if it radiates heat directly without a fan. Even in the cleanest house or office, every device will collect dust to block vents or be drawn inside by a fan. At least annually, clean the case and environment and blow it out with clean air. If you can open the case, blow the dust from every direction (never use a vacuum cleaner not rated for electronics).

For portable devices, keep them clean and resist cases that could hold heat in. If it's feasible, use a scheme that charges the battery at a slower rate and stops before it reaches 100%, or even 90%. Your battery and electronics will last longer and be more reliable.

Software

The programs that make your computer useful can also make it unusable. Each computer represents a unique combination of hardware components, programs, peripherals, and configurations that may interact in an unexpected or untested way. Even the sequence in which programs or updates were installed could affect how the computer runs.

If you install a program or printer and something else stops working you have a pretty good idea what might have caused the problem. The first solution is to uninstall the program or device.

However, regular updates to an operating system or some programs may be installed automatically and all you know is you can't browse the internet any more. Some OS updates have even been discovered to completely kill some models of computers. These may be more difficult to isolate because they were installed without your interaction and the culprit may have come in a bundle with the components poorly described in tech-speak that it's impossible to identify one thing that caused a problem.

Device drivers are code that allows the OS to talk to other components such as printers or the audio system. They can have a bad interaction that suddenly makes a feature stop working. Since most users are unaware of what they do, or even that they exist, they are rarely updated. But a change in the OS or other devices can unexpectedly make them not work.

In Windows, the easiest solution to troublesome OS update or driver installation is System Restore. This can roll most software that has been installed back to a previous point. It may even help eliminate some intrusive malware, although it can rarely restore the damage the malware may have done. Verify that your computer is automatically creating restore points and also manually create a restore point before installing any software from anywhere but a trusted, mainline source.

The mere age of the computer may also affect its usability. An older computer may not have the memory or disc space to support a required update. Maybe a new program requires a more modern main processor or video system to function. Some components in some computers can be easily upgraded; others are integral to the entire system. In these cases, the best solution may be to either replace the computer or just accept that you will live in past technology.

If you choose to live with a less capable computer, the one capability you must not do without is updates to the operating system or other software. If installing updates is not possible, consider using it only for special purposes such as running one old program that will not work on newer equipment. Also, severely limit its access to the internet and the rest of your network in case it does acquire an infection.

==== = ====

End of writing – 10/8/16

Section I "Safety"

- 30 -

Spellchecked 10/8 11:55

page 13 of 15 ... Created 8/1/16; Rev 10/12/16; backup 10/8/16 11:58 am; words 7,775

File m1 Edited in master document (outline view > Master menu section > expand subdocuments > page view

Safety, **Security**, Privacy

In the age of widely distributed electronic data we need to protect our data and ourselves from risks online and on all our devices. With a little bit of information and a large dose of attention and common sense we can ameliorate a large amount, but not all, the danger of living in a modern information society.

These articles will separate the risks and procedures into three overlapping categories of **Safety**, **Security**, and **Privacy**.

- **Safety** applies largely to protecting data from accidental or malicious loss or damage. Getting hit by a bus while crossing the street is not included.
- **Security** gives techniques to store and share certain sensitive data with those who should see it while not also sharing it with those who shouldn't.
- **Privacy** will primarily help avoid having people looking over your shoulder or following you around and gaining information by correlating relationships.

==== = ====

Safety, **Security**, and Privacy

Security assumes you've already protected your computer and its data from physical destruction. After ransomware that flat out asks for money, the most valuable thing to an outsider is the *information* that you store and transmit electronically. We may have once believed in "security through obscurity" or "no one wants to search through hundreds of bits of information about thousands of customers to find my carelessly emailed credit card number." Unfortunately, wholesale data collection and high-speed automated pattern matching mean that credit card number *will* be found if it was protected merely by sticking it in the haystack.

The two core technologies that protect data security are *encryption* and the *passwords* that drive the encryption. Like any technology, they need to be properly implemented to actually be effective. If you have sloppy encryption or weak passwords you actually have no protection.

Encryption

What is encryption?

Encryption is a means to take the bits of one document and change them to another set of bits. Your "Ovaltine decoder ring" did this by replacing each letter with the letter a number of spaces forward in the alphabet. A character frequency analysis would break the process quickly. The World War II Enigma similarly used the alphabet, except that it could change the settings – the replacement alphabet – with each press on the keyboard. Thus "speed" might come out "kmhte" and a couple paragraphs later the same word would be "yfpug"; making it impossible to simply count "e"s and "t"s.

Modern encryption takes the complexity much farther working at the bit level with a much larger and more dynamic substitution table. The results of encryption are indistinguishable from pure randomness. The major methods of encryption have been mathematically analyzed estimating that breaking the cyphertext (the encrypted gibberish) will take millenia.

You might read that a particular encryption method using a 1024-bit key has been cracked. The industry's solution is that everyone starts using 2048-bit keys. This, relatively straight-forward upgrade does not mean the encryption is twice as difficult. Actually, it will be a number with 309 digits times as difficult. It will be a few more years before the new standard is broken.

Since cracking the original encryption was reported by a group with the resources of a research environment, hackers won't catch up until the system has upgraded to the stronger keys.

While the *mathematics* of encryption is provable, any good standard can be poorly implemented. If the programmer doesn't properly use standard practices, the best encryption can fail.

Also, the best standard practices of the past may no longer be valid. We knew 1024-bit keys were beyond current technology in 2005, but could anticipate that wouldn't be so come 2025 or 2050. The shorter keys were a best available technology in 2005 because computers of that time couldn't efficiently use the 2048-bit keys which would become commonplace a decade later.

Where is encryption used?

Even if you think you have never used encryption, your data is frequently encrypted transparently for you. Encryption is used extensively in internet communications between you and the website. If a company is storing private or valuable information, *hopefully* it is encrypted on their system. If you use a backup service to protect your computer files against loss, they should encrypt your data. Many password managers encrypt your individual passwords with a master password while it's on your own computer or in the cloud. Most portable devices encrypt all their contents when the screen is locked.

Every time you connect to a website with **HTTPS**, the data you send and the pages you receive are encrypted as they pass through the internet. The encryption is critical to protecting your data from any snoops along the way who may want to steal your bank account or password. It is also one example of law enforcement's claim that "the web is going dark." If criminals can't read your data, neither can anyone else except the intended recipient.

Your password is encrypted when sent to a website via HTTPS and once it gets there, *all* of your personal information should be encrypted such that if hackers attack the site they will not be able to determine your password or read your information.

File m2 Edited in master document (outline view > Master menu section > expand subdocuments > page view