Computer Safety Advice

The best advice I can give is

Backup Backup Backup Backup oh….. Did I say Backup

I can assist you in backing up your computer in the best possible way.

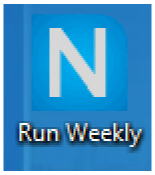
If you do not have an EXTERNAL hard drive I can sell you one for $69.00

ALWAYS use an alternative web browser to browse the web or to use email such as “Firefox” or “Google Chrome” which generally poses less of a security risk.

Firefox and Chrome *have been configured by me to block AD’s and Malicious web sites.*

Do not bypass or disable these protections.

I have placed an ICON on your Desktop you need to RUN on a WEEKLY BASIS without fail that will keep your most vulnerable 3rd programs up tp date.



Email is a common way of getting infected

While you can safely open an Email, **NEVER click on a link within it or open an attachment** that you are not positive is from a trusted source.

Here are 2 scenarios

1. **You get an Email from someone you DON'T know.** You open it. It tells you (or, persuades you) to click on a link in the Email. You do so. That is when you get infected. Frequently, the Email appears to be from a bank or a shipping company or a company you know. Do not fall for this Businesses do not normally send unsolicited Email.
2. **You get (what appears to be) an Email from someone you DO know.** Unknown to you, a virus generated that Email (and not your friend). It could be that your friend's computer is infected, but, not always. Obviously, the actual Email writer doesn't know you and cannot say anything personal to you, so, typically, it says something like "Click on this link for some important information… ". You are now infected.

If in doubt, delete the Email.

Instant messengers: The same caution should be used with opening links and attachments as Emails.

Web sites

Visiting Adult, free game or gambling sites pose a high risk of infection. In addition, do not download software or "Add-ons" from web sites that you are unfamiliar with. This includes sites such as "Facebook" **Do Not click on those Sponsored ad's**

Do not click on sudden pop-up windows while browsing the internet.

Pop-Ups and FAKE "call now" Microsoft warning pages

ANYTHING that pops up and says to call some phone number are 100% ALWAYS fake.

To protect yourself from serious malware infection, you must be extraordinarily careful about how you close a pop-up window. Specifically, you should never click anywhere in a pop-up window. Even buttons labeled "Cancel" or "Close" or a red-X button in the upper-right corner are dangerous to click; doing so could trigger an infection–the opposite of what you'd expect.

To safely close a pop-up window, locate the button in your Taskbar that corresponds to the pop-up. Normally, the button and the pop-up will have the same title. Right click on the button and select **Close**

Phone calls saying there is something wrong with your computer are 100% ALWAYS fake.

Microsoft Phone scams. Don't fall for them.

- Microsoft will never call you to let you know your computer is having problems. These scammers are saying "we are from the Windows team" or "We are Windows calling" or something like that, to scare you into letting them into your computer. These "fake technicians" AKA "Computer Terrorists" as I like to call them, always usually have a foreign accent.
  • Be careful when you Google for help, be sure the companies are reputable and be sure you are calling the right companies. Nowadays, you can Google "Microsoft support" and get a fake company! This is VERY common.
  • Do not call the numbers on pop up ads when you are browsing the internet, these are fake alerts that you have a virus.
  • Never let anyone remote in your computer that called YOU. If you called me for an appointment, this is OK , but just someone calling you out of the blue is NOT OK.
  • If you called them and are not sure, just hang up and call ME and I will let you know if it's a scam or real. 210-549-6477
  • If your guts says no or you feel weird, hang up or turn off your computer immediately. Even if you allowed them in your computer, they will say things to scare you into paying. Turning off the computer and calling a professional IT company or me immediately is what I recommend. Remember, if they are in the computer and you don't pay, this is when this happens…
  Destruction and deletion of data, Computer inoperable
  • Do they steal your data? From what I have heard… this is not common but a maybe, they mostly they want to get your credit card and charge you for fake services. If you did this, you can call your credit card company and they should charge back that service. Remember if they are remoted in and you don't pay, it is TOO LATE. They will destruct data or lock you out of your computer!
  • Do they destroy your data? YES!! Usually this happens if you ask for your money back and they are remoted in. This just happened to one of my clients. He said he wanted his money back and i went to see what happened, all data gone.
  • Do they lock you out of your computer? Yes, and sometimes they put a virus on your computer if you don't pay or say you want your money back
  Please share this with your parents, friends and family. Anyone that you feel will benefit from this information.

The phone scams are still going on and getting worse and are more destructive then in years past. These fake scammers rely on the fact you and your friends and family do not know what is going on…. and they feed on it. They expect you to NOT KNOW. And now you do.

Now that you have a clean PC, it's time to keep it that way.

Avoiding crapware is pretty easy once you become familiar with the tricks installers use to get you to agree to them. Here are some things to keep in mind as you download and install new programs:

- **Always download programs from their home page, if possible**. Many download sites (like Download.com) will create their own installers with bundled crapware, even if the original download didn't have it.
- **Watch for checkboxes on the download page**. Sometimes the option to avoid crapware may not be in the installer, but on the download page of the app itsel Adobe, for example, offers you the chance to decline installing McAfee on its download page. Other apps may offer an installer with crapware, but a portable version without it.
- **Don't click Next over and over without reading!** If you don't pay attention to what you're installing, you're bound to install crapware. Carefully read each page of the installation wizard before you click Next.
- **Always choose the Custom Install option**. Never choose Automatic. Custom install with almost always offer you the opportunity to decline crap
- **Read every checkbox**. Sometimes they'll hide it on an otherwise unrelated page of the install Read every checkbox and uncheck anything that wants you to install something you didn't ask for.
- **Don't Click Every "Agree"**. Sometimes, an installer will make the "crapware agreement" look like the original software's terms of servic Your brain wants to click "Agree" thinking it's the only way to continue with the installation—but read closely. If the "terms" are for a program other than the one you downloaded, you can safely choose "Decline" and continue the installation.
- **Watch Out for Multiple Offers**. Just because you've avoided one piece of crapware doesn't mean you're done— there could be more bundled apps waiting for you, or multiple offers for the same toolbar in the same installer!

It seems like this is complicated and not worth the trouble, but once you get the hang of it, it's a breeze—you'll be able to outsmart any tricky installer that comes your way. FreewareGenius has a great guide to some of the tricks you'll see, with examples for each, so check that out to familiarize yourself. I installed **Unchecky,** which will automatically uncheck those boxes for you—**but it's no replacement for due diligence. Good luck and safe downloading!**

A list of dubious practices and how you can avoid them:

Note that the list below is sorted based on how dubious and deceptive the practice is.

1. Inserting ‘I accept’ or ‘I agree’ in the navigation BUTTONS
2. Making crapware installs look like you are approving the program’s privacy policy
3. Offer asks twice, with the wording REVERSED the second time around
4. Inserting the crapware in the ‘custom install’ section
5. Persistent offer after offer (after offer)
6. Hiding offers close to the program’s license agreement

Stay away from file-sharing sites.

Sites that distribute illegal software, music, or movies are known to be riddled with viruses. This includes torrents or other forms of P2P activities **(LimeWire/Bit Torrent for example)**. Staying away from these sites and programs is in your computer’s health’s best interest, as well as a good way to avoid being sued for copyright violation.

Why bad guys DO want your computer

Some people tell me, “I’m not really too concerned about hackers getting on my computer… there’s nothing on there that anyone would want anyway!”

Not true.

Your computer has value to a cyber-criminal in a variety of different ways that you might not even be aware of.

Here are a few things the bad guys could do with your computer:

1. **Using your online buying and selling accounts**

Before you say, “I really don’t do much of that” think about purchases you have made in the past. If you have ever purchased anything through Barnes and Noble’s website, Amazon, eBay, or any other online retailer, you have an account there. A lot of these companies even offer the convenience of storing your payment information in their servers, so that you can make purchases without typing out your credit card number each time (like Amazon’s “One Click” ordering process)

How this could be used: The thief could log in to your eBay account. First thing he would do is change the email address on file, so that any notifications would go to an email account that he controls (so you don’t see that anything is happening). He then sets up a fake auction for an expensive item along with instructions that payment gets sent to him, not to you as the eBay account owner. It’s even better for him if you have had the account for a while and built up a good positive feedback rating. But when people have paid and then don’t receive their item, they will be coming to you for an explanation.

2. **Using your email**

Oh, you only use your email for chatting with friends and family, right? You would never send any confidential or critical information by email, since it's not secure. But what if someone with malicious intentions got control of your account? Anything that got sent out would seem, for all intents and purposes, to be coming from you.

How this could be used: Think about all the people in your email contacts list – friends, children, other family members, co-workers, other people. What if you sent every one of them an "emergency" email, explaining that you are stranded somewhere (even in another country), you had your cash stolen, and you just need a few hundred dollars to check out of your hotel and get back home. Probably most of them would know that something was amiss. But this is actually a common scam, and a certain percentage of recipients fall for it. They send the money via Western Union, the scammer collects it, and that cash is gone forever.

3. **Using your credit card/debit card info**

You might be very careful to instruct the online stores where you shop to NOT store your credit card

information. You make sure to not keep your card numbers saved on any documents in your computer. These are what some people see as obvious precautions to take. But without proper protection, your card info is still at risk.

How this could be used: Obviously we know that if someone gets your credit card information, it can be used to make fraudulent purchases or cash advances (at least until you discover it and report it). But how would they get this information? Keylogger software. A keylogger runs silently in the background, recording every keystroke you make on your computer. So when you type in your credit card number, it is stored and sent back to whoever had the keylogger program installed. That's when the shopping spree begins!

4. **Using your computer for a DDoS attack**

"DDoS" is an acronym for Distributed Denial of Service. When you have this little malware program installed on your computer, you don't even see it running – in fact, your computer appears to be functioning fine. But on command, that software can direct your computer to visit a particular website on a specific day and time. You probably wouldn't notice anything happening then either.

How this could be used: You know how sometimes you go to a website and if it's a really busy time of day and a lot of other people are visiting the same site, the website becomes really slow? This is sort of the same process that criminals use to overwhelm a website with so much traffic that it breaks and is no longer working on the web. So how do they send all that traffic to a particular website? By having their little program secretly installed and running on hundreds of thousands of computers. When all of those computers go to the same website at the same time, the site can't handle it and just shuts down (computers like that are called "Zombies" or "bots", and the group as a whole is commonly referred to as a “botnet”). Your computer could be a part of that and you might never know it.

5. **Using your computer for illegal purposes**

It’s not pleasant to talk about, but your computer is capable of accessing things that you would never want to be involved with. If someone wants to get into activities that are completely illegal, they obviously would not want to use their own computer because it could eventually lead back to them getting caught. If they have control of your computer, they can use it instead – so the authorities come knocking on **your** door with a few questions for you to answer.

How this could be used: If the FBI came to you with evidence that your computer’s IP address was used in distributing or selling child porn, what would your response be? “Oh no, Mr. FBI Agent – there has been some mistake! My computer has not been used for that!” Or the scenario could include illegal gambling activity, maybe some threats to assassinate a public official, or plans to commit a terrorist act. If any of this is traced to your computer, you will be faced with the expense of hiring a lawyer just to defend yourself.

How do you prevent your computer from being infiltrated by any of this? Proper security software, and good habits.

For security software, I use and recommend ONLY 2 primary programs:

1. My antivirus program is **Windows Defender (For Win 10) Already Installed**. It’s free and does a great job.

1. My Anti-Malware program is **Malwarebytes Premium** – the paid version , not the free version. It is **already installed and configured**. It will run all the time, blocking a lot of bad stuff from coming in to your computer, and also blocking you from inadvertently visiting a malicious site that will infect your computer.
2. Please call me when your Malwarebytes renewal is due to renew your subscription. 210-549-5477

Malwarebytes
Authorized Reseller

As far as “good habits”, that is mostly common sense. Don’t click on a link unless you know where it will take you. Don’t download something free from the internet unless you know it is legitimate. Don’t let any downloaded software install anything “extra” that you weren’t looking for originally. As a general rule of thumb, if you search Google for “free” anything, you will not be happy with the results.

Again I need to say this again…… Use an alternative web browser such as “Firefox” or “Google Chrome” which generally poses less of a security risk. Already installed and ready.

Data Privacy/Commonsense safety

Data

What information do you store on your computer?

Home computers have rapidly become the storage place not only for personal correspondence but also for financial data, including bank records and government tax return forms. This information in the wrong hands can, and does, result in identity theft

What information do you share on social network sites?

Facebook is one of the largest social network sites where people connect with not only friends and family but also acquaintances. These acquaintances may be people they “met” at other sites, forums or through friends and family. However, they are only known virtually.

Not only is the information you share on sites like Facebook data, so is your home town, where you went to school, when you graduated, your birth date, address and telephone number as well as names and birth dates of family members. If this information is public, it is the very information that identity thieves can use.

What about your smart phone?

Do you check in at every location as you go about your daily travels and share it on Twitter or Facebook? Do you announce and document business or family trips?

Information stored on your computer or shared on social networking sites includes data that needs to be safeguarded to protect your privacy.

Safeguarding Data

The message about having an up-to-date antivirus software and firewall has been well received by home computer users. When helping with malware removal, it is has been a very long time since I have seen a computer without antivirus software and a firewall. Computer users are also getting much more conscientious about installing security updates and keeping third-party software updated.

This is all good news, but malware writers are very clever and manage to find a way to infect computers. In addition to the standard antivirus, firewall, updating what else can you do to safeguard your data?

In addition to keeping your computer and software programs updated, following are a some general suggestions for protecting the data on your computer:

1. Protect your wireless router with a strong password.
2. Don't open e-mail, instant message or Facebook attachments you are not expecting.
3. Do not click anywhere on a pop-up or warning from a program you did not install. Use the keyboard shortcut **Alt + F4** to close the window.
4. Pay close attention when installing soft Do not blindly click through the screens or you may end up with more than you expected.
5. Whenever possible, only download software programs from the vendor sit Keep in mind that free is not always free.
6. Always scan any file you download from the Internet.
7. Have a back-up plan in place, particularly for documents, pictures and other files that cannot be replaced.
8. Use a complex password, not a "dictionary word" or family name

Backup Backup Backup Backup oh Did I say Backup

What about safeguarding the data you share on social networking sites like Facebook?

Facebook makes it easy to connect and share information with friends and family. However, it is critical to ensure that you are not openly sharing personal information that could make you a target of identity theft.

Another resource that is helpful for Facebook users is Facecrooks, a source for not only privacy information but also the latest hoaxes that regularly circulate on Facebook.

A few easy steps will keep both the data on your computer as well as the information you share both secure and private.

Safety tips for online shopping

1. If it's too good to be true, it probably is. Many malware developers know now is the time to target online shoppers and they will use intriguing "deals" to generate clicks. Whether it is ads offering free products, or a "new" website that has the best deals out there. Chances are you'll never receive the product, but a stolen identity instead.
2. Look out for fake delivery confirmation emails. These typically contain malware and can compromise your computer. If you ordered online, it is best to go directly to the website

you ordered from, obtain your tracking number there and then go to the appropriate delivery service website to track the package.

3. Social media sites have become a popular platform to target potential customers. Be on the lookout for fake ads, coupons, or freebies offered. This goes for emails offering prizes or gift cards too! Many times not only will these “deals” result in hackers stealing your payment information, but also could include malware to infect your computer.
4. Avoid using public WiFi while making online purchases. This means, don’t do your online shopping while sipping your pumpkin spice latte at Starbucks. Get it to go, and shop from your couch! Using public WiFi’s are not secure, leaving the door open to hackers.
5. If you shop online, use a credit card. That way, if your information is stolen the cyber criminals are not tying up your personal funds from your checking or savings account.

Quick tips for avoiding all scams

Quick tips for avoiding all scams

- If it sounds to good to be true, it probably is.
- Read carefully, scams almost always have improper grammar or spelling mistakes which you won’t normally see in a legitimate message.
- Check the email it was sent from, it will often be easy to spot that the email didn’t come from support@amazon.com for example.
- If you click a link and are taken to a page looking for personal information, turn around. No company will immediately request that information from you to get a deal.

Now we’re here, it’s finally time for the list. Lets get rolling:

5. Fake Charity Emails

There is no doubt that during the holidays we tend to give more as a society. We’re all feeling happier, and are more willing to spread the cheer during the “giving season.” Cyber criminals are always on top of their best chances to scam you out of money and may even try to do it using fake charity emails. These could come in looking to get donations out of you, and may appear to be legitimate at first. Make sure to read carefully through the emails and look for their typical mistakes (typos, poor grammar, etc.). To be extra careful, if you’re looking to donate to a charity that came from a suspicious email, open your browser and manually navigate to their website. Using this process you ensure you’re not being fooled by any fake webpages and can continue to spread holiday cheer!

4. Fake Shipping Notifications

This scam attempt is very popular at all times of the year, but even more so during the holiday season. We all tend to order more things online during the holidays which means UPS and FedEx are ramping up their deliveries to get all the packages out on time. Cyber criminals look to target this aspect by alerting you that your packages were not able to be delivered and you need to fill out forms with personal information to reschedule the delivery. As we all know, if UPS attempts to make a delivery and can't they will leave a note on your door. You can also sign up for programs UPS and FedEx offer to monitor packages being sent to your address. This will allow you to skip over these shady emails and go right to your account to check a delivery status.

3. Black Friday or Cyber Monday Extravaganzas

We're not the only ones who get overly excited for the steal of the year on that flat screen TV, cyber criminals look forward to Black Friday and Cyber Monday just like consumers. Cyber criminals have been preparing for this time of year and are often putting some serious dedication into their scams. In previous years entire "Black Friday Deals" websites have been created trying to lure customers into buying fake products on their fake website. These sites are showing even lower prices than normal stores are offering to try to prey on customers looking for the best deal wherever they can find it. Be sure to always purchase directly from retailers no matter what sites you see deals on.

2. Fake E-Greeting Cards

E-greeting cards are not something that really caught on as a popular trend but they're still used as a cute way to spread some holiday cheer and happiness. They're even sometimes sent out by businesses as a way to spread some cheer to customers and wish them a happy holidays. Because of this, criminals are out looking to take advantage of your holiday spirit and trick you into clicking their malicious links.

Sometimes these E-Greeting cards will come loaded with malware as an attachment (as a PC Matic customer this will be blocked easily), however they also may try to get you to give up personal information. This type of attack is focused on social engineering and will attempt to get you to enter personal information to win a "holiday contest", or another silly excuse they come up with. Remember to avoid giving out personal information on the internet when possible, especially if it is solicited through a shady email or pop-up.

1. Fake Last Minute Shopping Deals

This year specifically be on the lookout for scams that could involve Wal-Mart or Amazon. They are two of the big powerhouses in retail store and online shopping, and cyber criminals see pretending to be them as an easy target. These scams could come in the form of last-minute sales or coupons that will often sound to good to be true. If you see a deal like this and want to see if it's legitimate, go directly to Amazon.com or Walmart.com and see for yourself. If they're emailing about a deal it will most likely be on the front page of their site.

Another way the criminals try to scam people with shopping related deals are free gift cards, that's right FREE GIFT CARDS. They'll often exclaim this offer in full caps to you in an email or malicious pop-up. A good rule of thumb for this one is no store is ever going to give you a free gift card for filling out a form with personal information. There are some instances where stores offer gift card deals with a purchase, these are legitimate and are often done by stores like Target.

Final Tip……….Wait for it

The best advice I can give is

Backup Backup Backup Backup oh….. Did I say Backup

I can assist you in backing up your computer in the best possible way.