Gary Eikenberry Consulting
122-1010 Polytek Drive, Ottawa, ON, Canada K1J 9J1
Phone: 613-878-7485; E-mail: garyeik@geconsult.com; Web site: http://www.geconsult.ca

Tips for Safe Computing

Whatever your operating system or computing environment, a few simple habits can help protect you from **malware and other threats** which can transform your computer into a portal into a nightmare of hijacked email, ransomed data, stolen passwords or even stolen identities and other disasters. Just as Gary tells students in his self-defence and street-proofing classes, our purpose here isn't to make you paranoid, but to arm you with information and techniques to make you safer.

1. I'm not using Windows so I'm safe: Not exactly. While MS Windows has a reputation of being more vulnerable no operating system is 100% safe. Apple's Mac-OS and iOS as well as Android and Linux have been getting a lot more attention from the purveyors of malware, ransomware, spyware and other nasty things that can compromise your computer or other connected device. Besides having your operating system targeted you should be concerned about "operating system agnostic" security threats which exploit weaknesses via a web browser, without regard to the operating system.
2. Updates: Operating system and software security updates and patches are usually issued after a vulnerability has been identified and they certainly aren't unique to the Windows "ecosystem." Once an update or patch is issued anyone looking to exploit vulnerabilities who didn't know about it before becomes aware of it. The longer you delay in installing available updates and patches, the more vulnerable you become.
3. Passwords: Your password is supposed to protect you and your system. Weak passwords and passwords written on sticky notes stuck to monitors or keyboards are like leaving the front door key in the lock. A strong password contains a mix of upper and lower case letters, numbers and non-alphanumeric characters and is not an easily recognizable word, name or a birthday (especially if that birthday is exposed on social media). Of course there is a bit of a balancing act between choosing a strong password and one you can remember without writing it down and leaving in a plainly visible location. It's also worth noting that using the same password (or PIN for that matter) for multiple accounts means that if it does get cracked or stolen one time everything becomes wide open. And if you have so many passwords that you can't remember them all, consider a "password safe" program or at least an encrypted and password protected document or PDF file rather than a text or document file with a name like passwords.docx. Also consider two factor authentication where it's available.
4. Protective software: While MS Windows has a reputation of being more vulnerable, and therefore more in need of software designed to protect you from the wide range of malware threats, **no operating system is 100% safe**. Anti-malware software and browser plug-ins, while not infallible, are definitely advisable. Never spend more on protective software than your data or personal identity is worth to you. There are good free and open source options out there, but many of the free versions, especially for Microsoft, Apple or Android systems, have paid versions that are even better.
5. Don't click "OK": Well, okay, go ahead and click it, but not without first reading the alert or other message. And if you're asked to authorize the installation or execution of something you didn't specifically intend to install or run CANCEL the operation immediately. One of the things that makes most Linux based systems more resistant to vulnerabilities is that, any operation that wants to install, update or otherwise make changes to your system requires authentication by entering an admin-level password.

6. Hover before you click: Chances are very good that your bank, or eBay or PayPal will never send you an email containing a link to your account. The link that looks like it points to www.paypal.com may be actually going to a completely different domain with a fake log in page intended to steal your user id and password. When it comes to browsing the same can be true. If you hover your mouse over a link and the URL displayed points to a different domain than the displayed link purports to represent don't click it!
7. Backup, backup, BACKUP! Anything that's worth saving on your computer (or phone or tablet) is worth backing up. Not convinced? Reformat your hard drive to find out what you could be missing after a ransomware attack or a system crash. Well don't really format your hard drive, but think about what you could lose if you did. And what about all those photos you have on your phone if it gets lost, stolen, dropped down a storm sewer or run over by a garbage truck?
8. Portable devices: Whether it's a laptop, tablet, smartphone or any other connected device, it probably contains data, stored passwords or any of a number of other things which could make your life miserable in the wrong hands. Never leave it unattended even for a minute. A client of ours left her laptop long enough to get a refill at a coffee shop. It wasn't stolen, but during the time it was out of her sight someone apparently connected a USB key and copied her My Documents folder, which contained, among other things, a document entitled Banking. We'll leave the rest to your imagination. But even if you never leave your device unattended, you can still be vulnerable. We recommend against doing any on-line transaction which might expose sensitive data (including passwords) over unencrypted public Wi-Fi connections. Even if you're working over a secure (https:) browser connection it is possible for someone with (admittedly illicit or at least unethical) software intended for such things to intercept a Wi-Fi data stream, save it to a hard drive and the analyse it at their leisure (again, illicit tools are required) to decrypt and extract passwords, etc.
9. Consider using a VPN: Many people think of a VPN as nothing more than a way to circumvent geo-restricted content, but a VPN can be just as important for safe computing as your anti-malware software. This is especially important if you often connect a laptop or other mobile device via public wi-fi. If you don't know why, take a look at https://www.forbes.com/sites/leemathews/2017/01/27/what-is-a-vpn-and-why-should-you-use-one/#4be73ed14b8f. Our current recommendation is ProtonVPN, with the "plus" subscription.
10. Be careful with what you store in the cloud: On-line or cloud storage can be great, but you should always remember that whenever you store data there you're trusting someone else to protect it, so we would advise against cloud storage for anything you wouldn't ask a stranger to keep an eye on for you while you go get another cup of coffee.
11. Privacy and security go hand in hand: **Think before you post**. It may be obvious that telling Facebook that you're looking forward to 2 weeks in a tropical paradise when your home address is posted somewhere on-line is like advertising on www.TargetsForBreakins.com, but there are lots of other ways in which an ill-considered post or information you divulge in an on-line survey (do you really know who might be one the other end of that clever "tool" to tell you what kind of cat you most resemble?) can compromise not only your privacy, but also your security.

All things considered, the greatest threats to safe computing are **complacency, smugness and ignorance**, but we've barely scratched the surface here. We haven't even mentioned firewalls and other ways of securing your network or stand-alone computer from incursions from the Internet, spam filters, tracking cookies, lock screens or shoulder surfers. Find out more about safe computing practices by exploring the links at https://duckduckgo.com/?q=safe+computing+guidelines, bearing in mind that this link will send you to the Internet-in-the-wild and GEConsult can't vouch for the accuracy of any information you might find there.