Using the Internet securely

COVID-19 has forced people to stay home and spend more time doing things virtually, so being able to use the Internet securely has become more and more important.

From grocery shopping to virtual schooling or to getting takeout from your favorite restaurant, our reliance on the Internet has increased dramatically. Unfortunately, the potential for hackers and scammers to take advantage of us has also increased. From fake COVID-19 emails to viruses and scam websites, we face a growing number of potential attacks on the Internet.

Tip:
Proper English is your friend. If you receive an email or text message that appears to be from a trusted source (like a bank, store or credit card company) but contains lots of spelling errors and/or poor grammar, it is likely to be a malicious message meant to trick you into clicking on a dangerous link or opening a malicious file.

The do's and don'ts of using the Internet safely

DO'S

Here are some ways to help you keep your Internet experience safe and secure.

- Do **make sure you're using strong passwords** on all Internet sites. Whenever possible, use different passwords for different sites. You don't want to have your Facebook password compromised and accidentally give an attacker access to your bank account. If you have difficulty remembering passwords, there are applications that will let you store them securely on your computer or smart phone.
- Do **use multi-factor authentication** (sending a code to your phone or email) for applications that store financial information such as online shopping (Amazon, Walmart, etc.) and online banking applications.
- Do **change your passwords periodically** (at least once a year), and change them immediately if one of your accounts is compromised.
- Do **make sure that you are using antivirus software,** and that it is updated regularly. There are free versions available if you don't want to invest in a commercial application. You can find some good recommendations for free antivirus software here: pcmag.com/picks/the-best-free-antivirus-protection

Tip:
This also includes mobile devices like your phone or tablet. With our increased use of mobile devices to access the Internet, there has been a corresponding increase in the number of attacks targeting those devices. Be sure to use antivirus on your mobile devices as well.

Learn more at pcmag.com/picks/the-best-android-antivirus-apps or techradar.com/best/best-iphone-antivirus-app

(There are not as many free options for the iPhone or iPad)

- Do **be careful what you share online and post on social media.** The Internet is forever, and things posted on social media can be spread incredibly fast. Make sure that you're comfortable with what you're posting being shared, and make sure you're only sharing it with the people it's intended for. Internet marketers, potential employers and hackers are looking for information about you based on your browsing history, search history, and what you share on social networks. Social media sites like Facebook, Twitter, Instagram, etc. have settings which allow you to control who can see your posts.
- Do make sure you **lock your mobile devices.** Mobile devices today come with a variety of solutions for locking – use them. Using PINs, patterns, fingerprints or facial recognition will help ensure your mobile device stays secure.
- Do make sure to **keep your system up to date.** Ensuring the latest operating system and Internet browser patches are applied regularly helps reduce the risk of your computer being compromised. This applies to computers and mobile devices.
- Do **be cautious about "free" services online.** Even reputable sites can be generating revenue by selling your information. A general rule of thumb is that if you're not paying with money, you're probably paying with your personal information.
- Do **be cautious of click bait ads and websites.** "Click bait" is a term for an online advertisement or "news" story that has sensational or lurid content meant to grab your attention and be clicked. These websites often have malicious content that can put your computer at risk.
- Do **make sure your Internet connections are secure.** A secure connection should show **"https"** (not just "http") before the website address. Also, be careful when using public Wi-Fi at places like coffee shops or airports. The connection may not be secure unless you're using a Virtual Private Network (VPN).

Tip:
Once upon a time, SPAM was just annoying, unsolicited email advertising designed to get you to click on a website. Now, it is being used to spread malicious software, including viruses and ransomware. Be sure to delete spam without opening any attachments or clicking on any links.

DON'TS

Here are some things that you should never do while using the Internet:

- **Don't click on links in emails or open attachments** without first making sure the sender is valid, that the links do not go to malicious websites, or the attachment is something you expected to receive.
- **Don't let your browser store your user IDs and passwords.** Browsers are one of the first things that hackers attack, specifically to harvest user accounts and passwords so they can access your accounts.
- **Don't click on any email you don't recognize.** Even if you recognize the sender's email address, if the email looks odd to you or contains a link or attachment, call, text or IM the sender. Verify the email was sent by that individual or organization. Email accounts can be hacked and email addresses can "spoofed" (made to look like they are coming from someone other than the actual sender).
- **Don't give anyone remote access to your computer.** There are many online scams that may seem like legitimate security warnings but are instead criminals impersonating technicians from major companies like Microsoft, Apple, Dell or even Geek Squad. If someone calls your phone and says they need remote access to your machine - hang up! Unless you are paying a reputable company for remote support, do not allow anyone to have remote access to your computer.
- **Don't click on the first search result in Google or other search engines** that include advertisements. Doing a search on a subject in many search engines can return paid advertisements that may have nothing to do with what you searched for, or even a fake advertisement that could lead you to a malicious website. Avoid the advertisements at the top of the page (especially if they say "Paid") and scroll down to find familiar, trusted websites.
- **Don't download pirated, bootleg or unknown software.** This includes movies or songs. While the temptation to download the "free" version of software is great, the risk that it includes malicious software is very high. Ensure all your downloads come from reputable sites. Be especially wary of sites that ask you to download or upgrade software to view the content. It could be legitimate, but most of the time it's a trick to get you to download malware. You may find that "free" software ends up costing you much more in the end, so be careful.

Additional resources

Here are some additional resources for helping ensure you have a safe and secure Internet experience:

General internet security

- Google Safety Center: safety.google/
- ConnectSafely: connectsafely.org/
- Securing your Wi-Fi: us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html / techradar.com/news/networking/wi-fi/five-tips-for-a-secure-wireless-network-1161225 / networkworld.com/article/3224539/5-ways-to-secure-wi-fi-networks.html
- Virtual Private Networks (VPN): pcmag.com/picks/the-best-vpn-services / cnet.com/news/best-vpn-service-of-2020-expressvpn-surfshark-nordvpn-more/

Family-related sites

- Google Safety Center (Families): safety.google/families/families-tips/
- ConnectSafely Internet Resources (Child-focused links): connectsafely.org/great-internet-safety-resources/

HopeTech provides educational life empowerment programs for adults.
The mission of Atos HopeTech is to provide a toolkit of resources that will comprise "TechASYST," enabling Atos employees to provide educational life empowerment programs through technology, with special focus on reaching communities that are underserved by technology currently (with focus on senior adults).

For More Information on HopeTech please email: nahopetech@atos.net