Internet Security Best Practices Overview

The following is a general overview of internet security best practices, and how to keep yourself safe online. Please note that this document is not comprehensive, and – due to the constantly evolving nature of threats on the internet – cannot provide any more than basic guidelines for protecting yourself online.

Educate yourself:

All of the advice below is excellent and will help protect you online, but nothing will protect you more than taking the time to learn about the various threats on the internet and how to mitigate them. Here are two good places to start:

- Microsoft's Online Safety Resources: https://www.microsoft.com/en-us/digital-skills/online-safety-resources
- GCFGlobal's Internet Safety course: https://edu.gcfglobal.org/en/internetsafety/

Also, keep an eye on the news for large-scale cybersecurity incidents. When a major company or service is hacked, it will be on the news, and if you are a customer you should contact them immediately to find out what steps need to be taken beyond changing passwords.

Do not give out personal information:

Never, ever give your data – personal, financial, or otherwise – to anyone online that you don't know. As Symantec says:

"In your daily life, you probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. It's important to exercise the same caution at work. Keep in mind that cybercriminals can create email addresses and websites that look legitimate. Scammers can fake caller ID information. Hackers can even take over company social media accounts and send seemingly legitimate messages."

It's important to consider carefully what you're sharing online. Be especially vigilant when sharing pictures, or sharing your screen during a video conference: consider what's in the background. Is there something there that you don't want other people to see, or that might allow someone else to violate your privacy?

Use strong password protection:

Strong, complex passwords can help stop cyberthieves from accessing your information. Simple passwords can make such access easy. Creating strong, complex passwords is essential.

Symantec says: "A strong password contains at least 10 characters and includes numbers, symbols, and capital and lowercase letters."

Also, don't reuse the same password for multiple sites, even if it's a good one. The more you reuse a password, the less secure it is.

Watch out for Phishing scams:

Phishing (loosely defined as "a scam by with an Internet user is duped into revealing personal or confidential information which the scammer can use illicitly") is the most common form of social engineering on the Internet today. It comes in a variety of forms, from email, to links and popup ads on websites.

Phishers prey on people in the hopes that they will fall for the scam and give the Phishers access to their computer, their network, and their private information. Phishing is one of the leading causes of ransomware attacks, and one of the leading sources of identity theft.

Be cautious. If you're unsure about the legitimacy of an email or other communication, don't open it.

Invest in anti-virus and/or anti-malware software:

Viruses and malware are everywhere on the internet. No matter how safe you think a website might be, even if you think you know who sent the email you just received, you are never completely safe from threats. Be sure you have strong anti-virus software running on your computer; do a little research and see which service is best rated at the moment. Even a free anti-virus solution (like Microsoft Defender, or Avast Free) can protect you.

Mac users: This goes for you too. The days of Macs being safe from viruses are over.

Connect to secure Wi-Fi, or use a VPN – Secure your own Wi-Fi:

If you're uncertain of the security of the Wi-Fi you're on – or are stuck using public open Wi-Fi, consider using a VPN service. There are many such services available online, of varying quality…do your research before signing up for a VPN service.

If you don't have access to a VPN, be incredibly careful about what you do online while connected to public Wi-Fi.

Make sure that your home Wi-Fi has, at the very least, a secure password on it so that it can't be easily accessed by anybody within range.

Install software updates:

Many Windows and macOS software updates are security patches. It's OK (and sometimes even a good idea) to wait a week after they're released before installing them, but don't put it off indefinitely – they're being released for a reason. Install them regularly to help keep your computer safe.

Many programs – like Microsoft Office – update on a regular basis as well. Make sure to check for and run those updates frequently, as many of them are security patches as well. This is especially important for web browsers (Chrome, Firefox, etc.) and email programs.

Back up your data:

Doing this simple step on a regular basis – both Windows 10 and the macOS have built-in automated backup solutions – will save you a lot of trouble in the event of a security breach or any kind of hardware or software failure.

Wipe data from old technology before disposing of it:

Data can be left behind if you don't completely wipe a computer, cell phone, or tablet.

Wiping a cell phone or tablet can be easily done by following the manufacturer's instructions. There are a wide variety of options for wiping computer hard drives…look for solutions that follow the standards set out by the Department of Defense. If you are in doubt, destroy the hard drive physically.