– 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 Saf lv eu't

Revised: 7/28/2020

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, 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.