Personal

It’s second nature for us to access the internet throughout the day. Our smartphones, laptops and desktops have essentially become an extension of ourselves. Just like a seatbelt in a car or a helmet on a bike, we all need some type of internet security to protect ourselves from potential hazards. Here are a few internet security tips to ensure you’re safety online.

1 **Shop Safely:**

   **Check for the padlock:** It’s important when shopping online to make sure the site you’re on uses an SSL (secure sockets layer) certificate encryption. You can easily identify a site that uses this certificate by finding an image of a padlock in one of two places: either the status bar or the bottom of your web browser. This encryption ensures your credit card information, email or other personal information is protected from hackers.

2 **Phishing Protection:**

   **Turn on anti-phishing protection:** Several browsers have an anti-phishing feature you can switch on to protect your computer from phishing scams. Turn on:
   - Smart Screen in Internet Explorer
   - “Block reported Web Forgeries” in Firefox
   - “Enable phishing and malware protection” in Chrome (it may already be turned on)

3 **Social Sharing & Passwords:**

   To minimize the risk of your personal information getting into the wrong hands, it’s best to share sparingly on social media and create unique and hard to decipher passwords.

   Many social networks allow you to share a wide range of information including everything from your high school alma mater to your pet’s name. A completely filled out profile could actually supply the answers to security questions that are used to retrieve your passwords. Even if you privatize your profile, it takes just one security oversight to open access to identity thieves. The key here is to be selective about the amount of information you choose to provide in your profile.

   It’s important to not only use a unique password but also differentiate your passwords across all of your accounts. If you use the same password across all platforms and an identity thief accurately guesses your password, they now have access to all of your accounts. Here are a few quick tips to build a strong password:
   - Substitute some of the letters for numbers
   - Try spelling a word backwards
   - Use special characters
   - Or use credible online password generators
Remove Malware:

Learn how to remove Malware: The first step to removing malware is simply recognizing the signs that something is wrong with your PC. Signs include unusually slow performance, warnings from security programs you didn’t install, browser pop-ups when no browser is actually open, and much more. If you recognize any of these warning signs follow one or all of these options to remove malware.

Update Anti-virus software: New viruses are created daily. Your antivirus software is aware of this and updates frequently to accommodate these viruses. Simply check to see if you are using the most up-to-date version of your software to combat the latest malware.

Revert to safe mode: This will allow you to boot up Windows without letting the malware to spread. In safe mode, start removing temporary files. To do this, go to the Start menu and then type Disk Cleanup. From here you’ll see what you can safely delete. You want to delete temp files because harmful malware could possibly hide here.

Turn off your Internet: If you suspect that someone has remotely accessed your internet, be sure to turn off your internet and Wi-Fi immediately to cease all access.
Family

The internet has greatly influenced the way children interact and build connections with the world around them today. In order to insure each interaction is safe and fosters great internet habits there are a few things you can do to integrate internet security in your home.

1 Social Networking:

There are a variety of social networks available plus more being created each day. It is a good measure to be aware of these new networks, functionality and privacy settings. Have your child walk you through how they use each tool so you better understand information they’re publishing online.

2 Devices & Location:

Know the spectrum of available devices. Internet technology is not limited to your family computer, it can also be mobile. Be sure to also monitor gaming devices, cell phones, and laptops for social networking apps or other methods of publishing content.

Place the family computer in a high-traffic area. It’s harder for your child to view unsafe content or to communicate with unknown people if the computer screen is in a common area, completely visible to everybody in the house.

3 Sharing Personal Info:

Very often web pages will ask children for their personal information in order to provide personalized content to them. It’s best to establish with your younger children what types of information are appropriate to provide and not provide.

With teenagers, teach them how to be selective when publishing photos and other content online. Once content is published online you no longer have control over who sees it. While you may be able to remove an image from a photo album, the photo essentially never goes away.

4 Monitoring Usage:

Content Filtering: Know the types of Parental Control Tools available. With this type of filter you will be able to apply content filters such as the ability to block access to websites matching unwanted categories.

Access Scheduling: These types of applications will allow you to set a weekly schedule for Internet access, some control computer use in general, and some offer both as choices. A daily or weekly cap on Internet usage can also be handy.

Social Media Tracking: With this option you will be able to limit your view to just general post and interactions that contain certain words you may deem inappropriate. You also have the option to completely see everything their child does on social networking sites. With both options the child’s password is needed for access.