Internet Security

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:

Periodically, you may receive fraudulent email messages appearing to come from a valid source. These emails are generally referred to as SPAM or 'Phishing' messages.

To protect yourself and your family from phishing scams:

- **Be suspicious of any unsolicited emails asking for personal information.** You should always be very suspicious when asked for personal information, especially when asked by companies or organizations that should already have such information. If you need to update your information call 1.800.746.4726 to speak to a Customer Service Representative.
- **Always report fraudulent or suspicious email.** Reporting such instances will help get these "bad guys" tracked down. You can report any suspicious emails like these via the Spam button within webmail. Simply use the Spam button within webmail, mark the item as spam, and delete the email.
- **Make sure you have an updated anti-virus program and a firewall.** A firewall can help prevent a "bad guy" from attacking your computer. Anti-virus software will protect your computer if you do accidentally open one of these fraudulent emails that contains a virus. RCN offers McAfee PC Security Suite and Total Protection software. If you are interested in this software, call 1.800.746.4726 to speak to a Customer Service Representative.

For more information about Internet fraud and tips for identifying fraudulent emails and web sites, please visit http://www.fbi.gov/scams-safety/e-scams.

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

4 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.