Tips for Staying Safe Online

Presented by ICRMP's Technology Coordinator

With the changing landscape of the internet it is good to stay up to date with the best security practices. These tips should provide a good general framework for everyone on how to stay safe online at work and at home. And remember ICRMP has Cyber Liability included in your coverages.

1. **Stay up to date** – Having the latest updates for your operating system and web browser are generally the best defenses against viruses, malware, and other online threats. Many software programs and operating systems have some type of automatic update process, be sure to turn that on if it is an available option. It is also important to upgrade to the most current version of the operating system available for your hardware and move away from older unsupported versions like Windows Vista and XP.

2. **"When in doubt, throw it out"** – Emails with links to malicious websites or attachments are still the most common way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it! You can also contact the company or individual directly to verify legitimacy, just don't use any phone numbers or links from the suspect email. This also applies to warnings that may suddenly appear while web browsing. Close them if you can, if not, simply restart your computer.

3. **"Hover over Link" trick** – To check a suspect web link or email address, simply hover your mouse cursor over the link/address (without clicking on it) and it will show the actual address in the lower left corner of your web browser. Carefully read the address to help determine if it is legitimate. If you still aren't sure, follow the advice from #2 above.

4. **Be smart with passwords** – Do not use the same password in multiple places, especially for email accounts. For your password, try to shoot for 8-14 characters. The longer the better. Avoid using single dictionary words. Pass "phrases" of several words together are best as they are easier to remember and harder for hackers to guess. Mixed case letters, numbers and special characters are still ok to use in passwords and are still required by many services.

5. **Backup, Backup, Backup**! – It is critical to have a backup of your important files and documents. This will help you not only if an infection damages or deletes your files but also if you experience equipment failure. Either an external hard drive or an online backup service is a good option. You want to have all of your important files in at least two places.

6. **Anti-Virus Software:** - Have current Anti-Virus software installed and keep it up to date. While no Anti-Virus program is perfect, it does provide you with a good level of protection. Well known Anti-Virus vendors are generally the best: ESET, Kaspersky, BitDefender, Trend Micro, and Symantec.

7. **Use a modern Web Browser** – Google Chrome, Mozilla Firefox, and Microsoft Edge are more secure web browsers and provide more protection than Internet Explorer does. Internet Explorer is the least secure of all web browsers available.

8. **Protect your $$$** - When banking and shopping, check to be sure the site is security enabled. Look for the web addresses with a little padlock icon in the address bar or "https://", which means the site takes extra security measures to help secure your information. "Http://" does not provide a secure connection to a website.