Online Best Practices

Almost everything you do from a computer these days can be accessed via a web browser. Because web browsing is such a big part of the online world, it's important to be safe when perusing. Following these tips will increase your protection:

- **Padlock icon and https://**. If you are entering sensitive data, such as your credit card number or bank account information, into a browser form, make sure the site is secure before doing it. Look for a lock icon somewhere on the browser (usually located in the upper left corner) and/or an "https://" in front of the address. If it isn't there, don't put in your information - regardless of how legitimate the web site looks.
- **Anti-malware.** Make sure anti-malware is installed and kept updated on all devices. Enable the software to automatically update when one is available.
- **Use a firewall.** Most operating systems these days have some type of basic firewall protection. Make sure it's enabled.
- **Don't click on suspicious links or pop-ups.** Links can take you to a different website than their labels indicate. Typing an address in your browser instead of clicking a link in an email is a safer alternative. Additionally, your browser has a pop-up blocker; make sure it is enabled. If one gets through, make sure to pay attention to the message and choose appropriately.
- **Don't reply to spam emails.** If your email service allows you to report messages as spam, take advantage of it. This helps cut down on spam overall.
- **Learn how to identify phishing.** Phishing is a way hackers try to steal information. To prevent it means paying attention to where a link is taking you and if it doesn't make sense, don't go there. Phishing attempts come in email messages and also can be found by just visiting a website. Hover over the ad or link, and if the URL doesn't make sense, don't go to it.
- **Passwords.** Maintain strong passwords. Even though it's very convenient don't let your browser store passwords, especially for any site that has private information such as your financial data.
- **Public computers and WiFi.** Avoid using public computers or public WiFi, especially for connecting to sites that have confidential data about you such as your financial information or healthcare data. If whatever you need to do cannot wait till you get to a secure location, disable WiFi and use the data capabilities on your smartphone.
- **Sign Out or Log Off.** Always "sign out" or "log off" of web sites when you are finished. Simply closing the browser *may not* end your session.
- **Teaching Children.** Exposure to web browsing and the Internet starts very young. Teach children safe browsing habits right away and everyone will stay safer.

Get the lastest information from our website. Scan the QR Code to go directly to this page.