

Cybersecurity For All Aspects Of Daily Life

The internet is a big part of life in the 21st century. Going online was a mere novelty around 25 years ago, but now it has become a vital component of daily life.

According to the Digital 2019 report by HootSuite and We are Social, the average internet user spends more than a quarter of his or her life online. The same report states that consumers are on the internet an average of 6 hours and 42 minutes each day. The internet is used for work, school and recreation. In addition, as a consequence of the outbreak of the novel coronavirus COVID-19 in 2019-2020, social distancing measures have required people spend even more time online rather than in person.

While the internet has changed lives in many positive ways, the connectivity of the technology also opens individuals up to various dangers. These tips can help people be safe when spending time online.

- Think before you click. Malicious links can pop up everywhere, but particularly in phishing emails. Links may look like they come from reputable sources so it can be difficult to tell dangerous links from reputable ones. Hover the cursor over a link without clicking it to see where the link will lead. Do not click links from unrecognized sources or senders.

- Choose strong passwords. Passwords help protect personal information and data. Select strong passwords and do not share them. Do not use the same password for all accounts. Change your passwords frequently, especially if you believe your accounts have been hacked.

- Friend or foe? Some cyber criminals can create fake profiles to befriend you on social media. They may try to trick you into sharing confidential data with them.

- Maintain security updates. Software patches are issued when security flaws are discovered. Be sure to update software as indicated,

which can help you stay safer.

- Use private networks. Only connect to private networks when handling sensitive information. Security does not end with laptop, desktop or notebook computers. Securing mobile devices also is essential. Turn off Bluetooth and don't automatically connect to public Wi-Fi whenever possible.

- Lock up devices. Never leave your computer, phone or other tech device unlocked while you are away from it. That can make it easier for people to get into your system and steal information.

- Use two-factor authentication. Also known as a two-step verification, two-factor authentication is widely used to add extra security to online accounts. It's preferable on accounts that secure sensitive information, such as banking sites. This authentication uses different methods to trust devices, such as requiring users to type in a unique code that is emailed or texted in addition to entering their pass-

words.

- Be aware of ransomware. Heimdal Security, a cybersecurity company, says ransomware is a significant cyber threat. It encrypts all data and locks you out. It asks for a payment before a decryption key will be given. Frequent backups of computers and keeping data in multiple locations can help. Also, never access attachments from unknown senders.

It is important to learn about cybersecurity as the world spends more and more time online.



Keep Your Feet Warm

Inside and Out!

Moyer's SHOES
EST. 1952

Slippers & Boots
for the Entire Family

Acorn,
Haflinger
Red Wing,
Tundra,
Propét

2021
Readers'
Choice

Shoe Repairs Pick Up & Drop Off
for Towne Cobbler

316 W. Broad St. (Rt. 313), Quakertown
Mon-Fri 10am-6pm • Sat 10am-5pm
215-536-6378 • moyersshoes.com

Family Owned
for 68 Years