Personal Lines Insights

September 2021

Securing Your Devices

Every day, individuals of all ages spend a significant amount of time on tablets, laptops, and other smart devices. That being said, it's critical that this technology remains secure from cybercriminals and malware. After all, any device left unprotected could easily be targeted in a data breach, leading to compromised personal information and—in severe cases—identity theft.

To ensure your information isn't accessed and exploited by cybercriminals, consider these personal device security tips.

- **Protect your devices.** Use a passcode, PIN, fingerprint lock or facial identification to keep devices as secure as possible.
- **Don't forget to log out.** Always log out of mobile apps and websites when you're done using them. If you don't log out and someone gets access to your device, they could quickly locate and steal your login credentials or other personal information.
- **Use Wi-Fi cautiously.** Avoid connecting devices to public or unsecured (no password required) Wi-Fi networks. Use only legitimate, private networks—and never conduct financial business or access sensitive data while on public networks.
- **Keep a remote backup of critical data.** Back up any sensitive information to your computer or to a cloud-based service.
- **Use an antivirus program.** These programs provide enhanced security—safeguarding your apps, documents, and other important files from being infected with malware before you open them.

Technology will always be a target for viruses and cyberattacks. Nevertheless, following these tips for securing your devices will help keep you (and your information) safer.

Contact BeaconPath, Inc. for more cyber security/risk management guidance.

BeaconPath