Carebridge CORPORATION

A Carebridge Quick Tip

Keeping Your Personal Data Safe

Staying safe in today's world requires that you understand how your personal privacy can be jeopardized by the use of electronic devices and how to limit your risk of exposure. The US Department of Homeland Security provides the following tips:

Any piece of electronic equipment that uses computerized components is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the internet or a network that an attacker may be able to access. Remember that a wireless connection also introduces these risks. The outside connection provides a way for an attacker to send information to or extract information from your device.

How can you protect yourself?

- **Remember physical security** - Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas.
- **Keep software up-to-date** - If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- **Use strong passwords** - Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. (Do not choose options that allow your computer to remember your passwords.)
- **Disable remote connectivity** - Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.
- **Encrypt files** - If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. When you use encryption, it is important to remember your passwords and pass phrases; if you forget or lose them, you may lose your data.
- **Be cautious of public Wi-Fi networks** - Before you connect to any public wireless hotspot – like in an airport, hotel, train/bus station or café:
    - Be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
    - Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.

For additional information and resources on this topic visit US Homeland Security https://www.us-cert.gov/ncas/tips/ST05-017 or Canada Get Cyber Safe, https://www.getcybersafe.gc.ca/index-en.aspx.

Carebridge is available to assist with additional resources by calling 1-800-437-0911 or visiting www.myliferesource.com.