Cabin fever? *Now that businesses are starting to open, keep cyber safety in mind when out and about.*

Looking for a return to normalcy?

After five months of being homebound due to COVID-19, states are beginning to allow shops and restaurants to open their doors again. But as we enter these public spaces again, remember that coffee shops, eateries, libraries, and other shared spaces are not secure locations for working remotely, even if they offer "free" Wi-Fi.

Free, public Wi-Fi "hotspots" are so common that people frequently connect without a second thought, but using this option can carry a steep security price tag if not careful.

- **Don't connect to unknown Wi-Fi.** Use the personal hotspot on your mobile device instead.
- **Use a wall outlet.** To charge your personal devices**,** use a wall outlet or a portable charger.
- **Avoid public charging stations.** Cybercriminals sometimes install malicious software in these stations.
- **Safeguard your PII.** Avoid logging into accounts that require sensitive data, such as bank or credit card information.
- **Say goodbye.** Users should always log out of accounts when finished.

Also, remember that it is important to keep your devices close and don't leave them unsecured or unattended anywhere.

***