Kingston Health Sciences Centre
Centre des sciences de la santé de Kingston

76 Stuart Street
Kingston, ON Canada K7L 2V7
Tel: 613.549.6666
www.kgh.on.ca www.hoteldieu.com

Disclaimer

Topic of Disclaimer:	Understanding safety risks of using Public Wifi
Date created:	**June 16, 2020**

As more businesses shift to services delivered over the internet like video consultations, consumers are increasingly turning to Free or Public Wi-Fi connections to limit the impact on home internet quotas and reduce overage charges on mobile phone plans. Public Wi-Fi can be accessed by many people and may not be as secure as your home or mobile phone connection.

Extra precautions should be taken to ensure that your data and devices remain private.

1. **PICK THE CORRECT CONNECTION**

   - **Stick to Wi-Fi or Hotspot connections you know.**

     Although your device will show all the available Wi-Fi networks and hotspots in range, you should only connect to those you know like your local Starbucks or Tim Hortons or public library. Avoid connecting to Wi-Fi or hotspots that you don't recognize.

   - **Look for secured Wi-Fi networks and avoid open networks.**

     Secured Wi-Fi requires a password to connect to and are generally safer than open networks that anyone can connect to. A secured WiFi network will display a lock icon near the network name. If you use an open network such as an airport or guest Wi-Fi that you visit a web page to access, be sure that it is being provided by a company you trust.

   - **Watch out for copy-cats.**

     Hackers and pranksters have been known to set up phony Wi-Fi that use similar names to trick people into connecting to them so they can eavesdrop on your internet activity or capture personal data. If you unsure which Wi-Fi network is the correct one to join, ask a staff member.

2. **PRACTICE SAFE SURFING**

   - **Make sure your device is up to date.**

     An older device that has not been patched with security updates is an easier target and less secure than one that is kept up to date.

   - **Make sure your device is secured.**

     If your device has a software firewall, make sure it is turned on.

- **Be careful what you share.**

  When using a public Wi-Fi or hotspot connection, limit or disable your device's file sharing settings.

  For Microsoft Windows based devices, disable File and Printer sharing on public networks.

  For Apple devices (iPhones and iPads), turn off sharing services like Airdrop.

  Avoid using websites or services that share your location.

- **Do not log into unsecured websites.**

  If you must log into a website or provide it with sensitive information, make sure the site is using encryption. Websites that are using encryption have an address that start with HTTPS:// (note the S in the address) as opposed to HTTP:// (no S).

Contact your internet or mobile phone provider and ask for help:

Many internet and mobile phone providers are offering COVID-19 relief in the form of reduced or waived internet quotas and overage charges.