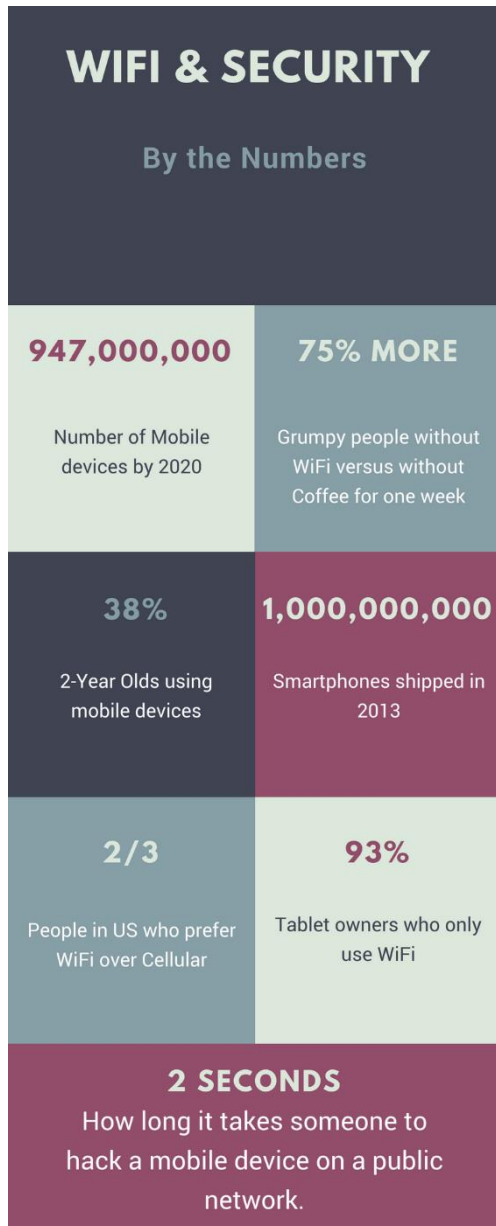




Sometimes (Free) WiFi Can Be Costly

There is no doubt that technical gadgets are quickly becoming extensions of our bodies. As such, keeping these digital appendages healthy and safe should always be at the forefront of our minds. However, with the constant temptation to take a few shortcuts and to save a few dollars, we can quickly find these devices either riddled with diseases (malware) or hijacked by a stranger. Below are some simple steps that can be taken to ensure the security and privacy of your data if you choose to use Public WiFi.



Before You Connect:

- Either turn off WiFi on your mobile device when not in use or turn off the ability to automatically make a connection.
- Double-check the WiFi name and password with the public provider before making a connection.
- Secure Your Mobile device by installing a Virtual Private Network (VPN) application*, ensuring software is up-to-date and turn on browser capabilities to be notified of fraudulent websites that you may visit.

While Connected:

- Immediately login to a Virtual Private Network (VPN) once your WiFi connection is made.
- Constantly look for “https” or a key-lock symbol for websites that require you to login to access your account.
- Logout of any account as soon as you leave that website or application.
- Avoid using websites that hold sensitive data such as banking information, student records, etc.

When You Disconnect:

- Choose to “Forget the Network” from your device’s WiFi list.

*Contact your IT Department for VPN and Connection Information.

