The Hidden Dangers of Public Wi-Fi and Remote Work

Remote work has become the new normal for many businesses, giving employees the flexibility to work from home, coffee shops, airports, and anywhere in between. While this flexibility boosts productivity, it also opens the door to serious cybersecurity risks.

One of the biggest threats? Public Wi-Fi.

Why Public Wi-Fi Is Risky

Public Wi-Fi networks, like those found in hotels, cafés, or airports, are convenient—but they're also prime hunting grounds for cybercriminals.

Here's why:

- **Unencrypted Connections:** Many public networks don't encrypt traffic, meaning your data travels in plain text.
- **Man-in-the-Middle Attacks:** Hackers can intercept communications between your device and the internet, stealing passwords, emails, or financial details.
- **Rogue Hotspots:** Cybercriminals can set up fake "Free Wi-Fi" networks that look legitimate but are designed to harvest your data.
- **Malware Injection:** Infected networks can spread malware directly to connected devices.

Company-Wide Remote Work Security Tips

- Provide employees with company-approved VPNs and remote access tools.
- Implement endpoint security solutions to monitor and protect devices.
- Offer cybersecurity training focused on remote work risks.
- Create clear policies for remote work and device usage.

The Remote Work Factor

When employees work outside the office, they may:

- Access company files and systems through insecure networks.
- Use personal devices that lack strong security.
- Store sensitive data without proper safeguards.

This makes remote workers a prime target for cyberattacks.

Best Practices for Secure Remote Work

1. **Use a VPN (Virtual Private Network)**
   A VPN encrypts internet traffic, protecting sensitive business data from eavesdroppers.
2. **Enable Multi-Factor Authentication (MFA)**
   Even if a password is stolen, MFA ensures accounts remain secure.
3. **Keep Devices Updated**
   Apply the latest security patches and updates to operating systems, browsers, and applications.
4. **Avoid Public File Sharing**
   Turn off file sharing and AirDrop when connected to public networks.
5. **Use Secure Connections Only (HTTPS)**
   Always look for the lock symbol in your browser before entering credentials.
6. **Separate Work and Personal Devices**
   Limit business activities to company-managed devices whenever possible.
7. **Encrypt Sensitive Files**
   Protect stored files with encryption in case of theft or device compromise.

Remote work isn't going away—but neither are cybercriminals. The convenience of public Wi-Fi can come with hidden dangers if the right precautions aren't taken.

At Teleco, we help businesses build secure remote work environments with VPN solutions, endpoint security, and employee training—so your team can work from anywhere with confidence.

teleco.ca

✉ **sales@teleco.ca**

One Partner. One Call. Work securely with Teleco.

☎ **1-800-465-3933**