



TECH TIPS FOR WORKING WIRELESSLY AND WISELY

Protect your network and data while taking advantage of the benefits of wireless computing

Wireless computing has changed the way we work. Freed from the need for cords and cables, any coffee shop or airport lobby is now a perfectly good place to work. And back at the office, wireless technology makes networking multiple computers and sharing resources simple and smart.

But wireless signals travel through the air, which makes them naturally easier to intercept. Fortunately, by taking a few basic precautions, you can drastically reduce risk. Follow these tips to keep your business protected.

Wireless protection out of the office

Using your laptop in a public Wi-Fi hotspot presents a whole new set of security risks and demands a few important precautions. You can avoid much of this by equipping your laptop with a USB internet stick. Ask your provider about affordable plans that give you secure wireless internet access in just about any location. Whichever way you choose to connect, consider these tips to increase security when working in public places.

Enable firewall and anti-virus software

A firewall acts as a barrier, blocking unwanted outside access to your computer. While it won't protect you from every threat, it's a good first line of defense. Be sure your firewall protection is enabled. Using a public network could expose you to viruses and spyware in addition to hackers. Make sure you keep your laptop's protective software up to date.

Protect your files

Make all the folders on your laptop private. You can also password-protect individual documents – especially sensitive documents and the ones you plan to use in a public location. For extremely sensitive documents, consider storing them off of your computer in a secure location such as a shared drive, and only accessing them when necessary. It's also a good idea to turn off file and printer sharing before entering a hotspot.

Use a Virtual Private Network (VPN)

A VPN is a secure connection through the internet to your company network. A VPN encrypts all the data coming and going from your computer, preventing exposure over a public Wi-Fi network. This is the safest and smartest solution for business users sending sensitive data while working in public hotspot locations.

Choose your connections carefully

Your laptop may pick up a signal from an unknown (and possibly untrustworthy) neighbouring network. Set your computer for manual network selection, and ensure that Wi-Fi ad hoc mode is disabled. Then, confirm that you only join legitimate networks run by businesses you trust.

Exercise caution when using wireless hot spots

If you're using your laptop in a Wi-Fi location but don't need to access the internet, disable your Wi-Fi connection to avoid unnecessary exposure. Use caution when sending email in a hotspot location, avoid entering private information such as credit card numbers and passwords, and stay away from sensitive online transactions such as banking or trading. And of course, keep a close eye on your laptop and never leave it unattended.

Wireless network security in your office

The latest wireless gateways combine a modem and router in one, offer lightning fast speeds and broad range, and let multiple users share internet access, printers and files. But to protect your business, it's important to take steps to keep outsiders from accessing your wireless network, and to keep your data private once it leaves the safety of your environment.

Change your default settings

When you first install your wireless router or gateway, you will need to log into an administration site to set up your network. Hackers are very familiar with the default manufacturer settings, so it's important to change these settings immediately, and always choose a password that is difficult to guess. Similarly, every router or gateway comes with a system ID, or Service Set Identifier (SSID). Once again, neglecting to change this from the default setting makes it easy for intruders to find and access your network.

Don't broadcast your network ID

Most wireless gateways and routers automatically broadcast your network ID at regular intervals, to make it easy for users to find a wireless network even if they don't know its name. Check your manual for instructions on how to disable this setting and make it more difficult to detect your network.

Turn on encryption

Encryption scrambles the information sent over your wireless network, making it very difficult for outsiders to decipher. While determined hackers have proven capable of cracking some encryption, for most businesses, encrypting your data will protect it sufficiently.

Enable Media Access Controller (MAC) address filtering

Every computer or device connected to your network has a unique number assigned to it, often referred to as its physical address or MAC address. When you set up MAC address filtering, you are instructing your wireless network to only allow connections from the devices it recognizes. While it is possible for hackers to set up fake MAC addresses, MAC address filtering is one more step you can take to make it more challenging to access your network. Consult your manual for instruction.

Install firewalls on every computer

While most routers and gateways come with built-in firewalls, enabling firewall protection on each computer adds another layer of protection. Ensure all firewall settings are enabled. It's also important to keep your anti-virus protection installed and up to date on every computer connected to your network.

Minimize signal leakage

A simple decision such as where to place your router or gateway can make a difference to your level of security. You can't eliminate signal leakage completely, but you may be able to help contain it by placing your equipment in the middle of your premises, away from windows and exterior walls. Consider turning your wireless network off completely when it's not in use for extended periods improves your security.

About Rogers

Rogers connects small businesses to customers, suppliers, partners and employees with fast and reliable wireless, telephone, internet and TV services. Over 1.5 million business customers rely on Rogers for proven tools and the know how to help keep them connected. Our affordable services run on our proven networks, backed by 24/7 technical support.

Looking for more articles to help your small business be more successful?
Visit the Business Resources Centre on www.easytomanage.ca.

