Protecting Your Network Connections

Piggybacking, or when unauthorized users connect to your network, is an all-too-common occurrence. If you don't have proper protection in place, hackers can break into your network and access classified information or even engage in criminal activity under your network, leaving you accountable for the crimes committed.

Even "friendly" neighbors can cause harm when piggybacking on your network by raising your internet bill and slowing down the speed. Follow these precautions to keep your network access available to only those who are meant to be using it.

Keep Your Network Access Limited

Wireless network access should be restricted to authorized devices only. You can solve this by **manually entering the Media Access Control (MAC) addresses** of each of your specific devices to keep unapproved parties out of your network. It's important to note that this method is not foolproof, however, as some hackers have discovered ways to imitate MAC addresses.

Change Admin Defaults

It's important to **change your wireless network name (SSID), router names, and passwords** from their default settings. Hackers can access a public database, or rainbow tables, of commonly used default logins, making it easy for them to guess their way into your network if you leave them as is. Your admin password will need to be strong and specific. Utilize both upper and lowercase letters, as well as numbers and other special characters to make it more difficult to guess.

Stay Anonymous

Only visit the administrative interface via private browsing to prevent URLs from being saved in your browser history. Utilize **a virtual private network (VPN)** to hide your location.

Encrypt Your Network

By mixing up your data into indecipherable codes, you stop hackers from being able to use your information. You'll want to **manually turn on your router's encryption feature**, as most routers have them turned off by default.

Verify Your Router is Up To Date

Update your router as new software comes out to ensure you're not operating under system versions with bugs that hackers can take advantage of. You'll also want to **confirm your system provides WPA2**, which older wireless routers may not be capable of, to protect against all the different hacking programs. Anything other than WPA2 is outdated and leaves you at high risk for being hacked.

Protecting your network connections is essential to keep your sensitive data safe from harm's way. To make sure your network is always functioning, you'll also want to connect it to a UPS in case of power outages and anomalies.

Talk to the experts at PowerIT today to find out how to protect your wireless network from any problems that may arise, so you don't fall victim to costly downtime.