4 Ways Your Remote Employees Can Protect Your Network

Do you or your employees often work remotely? You could be exposing your business to some network security risks in Anaheim.

Network security in Anaheim, and beyond, is important. This goes for both in-house employees and remote workers that may be tapping into your network. Working remotely is much easier today than it was even a decade ago. More and more companies are opting to allow employees to work from home to provide a more appropriate work-life balance and some companies are even going totally virtual to avoid paying hefty prices for real estate. But keeping your remote employees' devices and your network protected can be challenging when they're not under the same roof and working from insecure connections. Here are four ways your remote employees can help protect your network.

1. Knowledge.

The most powerful weapon for network security in Anaheim is education. Making sure you educate your employees on proper procedures and protocol is the first step in ensuring safety. Ensuring that your remote employees receive training that allows them to spot the possibility of cyber attacks and be prepared is crucial. They should receive the same IT training, and quite frankly more training, than your in-house employees.

You also need to train your employees to be aware of their surroundings more so than in casual settings. When remote employees are working from public places, your business's information can be more easily compromised. Say you have an employee using a company credit card to book travel or purchasing equipment for the business – a person with opportunity and a nefarious nature can easily watch keystrokes to obtain the necessary information to steal that credit card. Make sure employees know that they should, if at all possible, have their screens facing a wall behind them instead of an open layout or window.

2. Never use open WiFi.

Another thing remote employees can do to keep your business safer is to never use open WiFi. Oftentimes coffee shops and public spaces offer free WiFi though it is typically unsecured. Hackers can use open WiFi to see what peoples are doing on the network and use it as an opportunity for an attack. There are two common cyber attacks committed through open WiFi: MITM attack (man in the middle) and Evil Twin Hotspot. The MITM is the most common

and happens when a cybercriminal intercepts information that your employee is sending over the free WiFi. Your employee has no way of knowing if this type of attack has occurred because transmissions look totally normal.

The Evil Twin attack is a form of MITM and occurs when a hacker creates a fake hotspot that your employee can actually connect to. It looks almost identical to the “official” free WiFi being offered but allows hackers to gain access to everything that employee does.

3. Always use a VPN.

Another step in protecting network security in Anaheim is requiring all remote employees to use a virtual private network or VPN. This requires a secure connection between the internet and the device of their choosing. It hides all the activity your employee participates in on the internet from prying eyes and helps to better protect your business and its assets. Be sure to restrict access within the VPN to only the features a specific employee needs. Giving open access to every employee defeats the purpose.

4. Password procedures.

Make sure your employees – both remote and in-house – are always using appropriate password protocol. Everyone knows that passwords need to be much more difficult than they used to be but fewer people than you think realize that it’s more in-depth than that. Educate employees on the following:

1. **Don’t reuse passwords across multiple accounts.** While this is convenient, it’s dangerous. Different services have different security levels and it’s not safe to use the same password across a variety.
2. **Change passwords frequently.** Change them annually at the bare minimum but get in the better habit of changing them every 30 to 60 days.
3. **Don’t save them in a browser.** Frequently browsers ask if you want to have your password and username saved for a site you’ve signed into. Don’t allow it. Though it’s convenient, it can leave an entire list of credentials open to a hacker.

If you’re looking for a trusted partner to handle your network security in Anaheim, fill out a short form and let CMIT Solutions help. We have a nationwide network ready to support your business.

See Original Web Page