5 Cybersecurity Tips for Work-from-Home Employees

Working from home is growing increasingly popular, but it poses issues for companies that have little to no control over the equipment and connections used in employees' homes, putting enterprise data in danger of security breaches.

If your firm has remote workers, make sure you have procedures in place to protect them as well as your entire network.

1) Update Systems on a Regular Basis

Keeping staff devices up to date is an excellent habit that can help your system become more secure. Updates for your devices or apps should be installed as soon as possible because they are designed to fix security holes and give additional protection against cybersecurity threats.

Instruct your personnel to pay attention to all notifications they receive on their cellphones and computers regarding changes. You can also create system policies to prevent users from connecting to the company network with outdated software or other systems.

2) Be on the Lookout for Phishing Scams

Scammers send out emails all the time, attempting to dupe users into downloading contaminated files or revealing sensitive information. When employees use corporate email systems, it is typically extremely simple for employers to reject suspicious correspondence. It is, however, considerably more difficult if they use their personal email. Therefore, it is critical to establish a policy prohibiting workers from using personal email for work-related purposes and to train them to recognize and avoid phishing attempts.

If an employee is a victim of a phishing scam on their personal computer, it can have a severe impact on your corporate systems if they login to your network using the same device.

3) Use Multi-Factor Authentication and Strong Passwords

Any computer system's first line of defense is a strong username and password. It doesn't matter if it's a personal or professional equipment. Setting passwords on all your devices is a good way to keep them safe. Requiring your staff to change their passwords to something more complex and safer is a big first step.

Another requirement while connecting from home is to use two-factor authentication. Hackers will not be able to connect to your system if an employee's ID and password are stolen since they will not have the unique code generated by text or other tools.

4) Separate your work and personal devices

While having your staff connect to work from their own devices can be easy and cost-effective, it does introduce certain additional security issues. Personal computers and mobile devices frequently lack the necessary security applications and software to keep data safe. You get a lot more control over the problem if you need employees to utilize a separate work device. Therefore, most firms would supply laptops to remote workers that are solely used for work-related tasks.

5) Make use of anti-virus and anti-malware software.

Employees should utilize established antivirus software provided by their IT department or a contract consultant to detect and remove viruses, spyware, ransomware, rootkits, trojans, and other sorts of malware. A decent antivirus program is required whether the employee uses a personal device or a company-provided computer.

Prioritizing Security

While there is no doubt that working remotely will continue to gain popularity in the next years, cybercriminals will attempt to take advantage of this trend. Any firm that allows workers to work from home must have a complete security policy in place to protect both employees and the company.


SECURITY BREACH
REPORT
CLOSE
SECURITY BREACH