REMOTE WORKING GUIDELINES FOR SMBs

Remote Access Security checklist for every IT admin

When societal disruption occurs, enabling a work-from-home option is essential for business continuity. But in the effort to keep workers productive and the business running, hastily extending a remote work option can leave your organization vulnerable in terms of security. If there's one thing we know about cybercriminals, it's that they don't hesitate to jump on opportunities. Use this step-by-step checklist to assist in protecting your workforce regardless of location.

☐ Button down your password policies

If you've been lax here, now's the time to strengthen your policies. Require long passwords (or better still, passphrases), mandate regular changes, and lock out accounts after a set number of failed logins. Explain to employees that they can't re-use their work passwords for any of their personal logins.

☐ Require multi-factor authentication (MFA)

Also known as two-factor authentication (2FA), this is absolutely your best defense against cybercrooks using coercive techniques, password-spraying or stolen credentials purchased on the dark web to masquerade as employees and infiltrate your network. If you use cloud-based email, productivity suites or other applications, turn the MFA on if it's available. If users need to access your internal network, put an MFA solution in place.

☐ Require a VPN for accessing your internal network

A VPN encrypts your corporate traffic as it traverses the public internet so it can't be read by eavesdroppers. As a plus, a VPN connection allows your IT team to extend more of your internal-network security measures to remote devices. If you already are using a VPN for some workers, make sure you have enough licenses and capacity to cover the new users. If employees will be accessing resources on your internal network, the combination of a VPN and MFA is a must.

☐ Use a virtual desktop interface solution if possible

With this type of solution, the employee accesses a virtual machine that is either in the cloud or your data center, and controls it remotely. It can be configured to look exactly like an office-based system. The advantage is that the sensitive data or files exist only on the virtual machine and are never resident on the employee's home system.

☐ Remind workers to be network-aware and Wi-Fi wary

One thing that's completely out of your control is their home network and other devices that connect to it. Tell them to turn off any file-sharing on the system they'll be using for work and to check their home router or Wi-Fi access point to be sure that WPA2 security is enabled. Remind them never to connect to an unsecured or open Wi-Fi access point that doesn't require a security key.

Invest in full-featured endpoint security for home workers

You can't trust that the antivirus that shipped with a home system or personal device is up to the job. A full-featured solution guards against all manner of threats with multiple layers of defense, including a personal firewall, protection from malicious websites, and guarding against malware on portable USB drives. The best option here is a business-class endpoint security suite that your IT department can administer remotely.

Require encryption if employees will work on sensitive files

If employees will be downloading corporate files to their personal devices, provide them with an encryption solution. Insist that they keep their personal files separate from the corporate documents, and save the corporate documents to an encrypted folder. Also, enforce a policy that they save revised documents to the corporate data store, so you don't have to worry about remote backup.

Instill the habit of logging out

When workers are taking their lunch break, are done for the day or anytime they're away from their device for more than a minute or two, they should log out from the corporate network. It's good practice anytime. It's a must if the computer is shared, or if others at home can access it.

Promote patches and updates

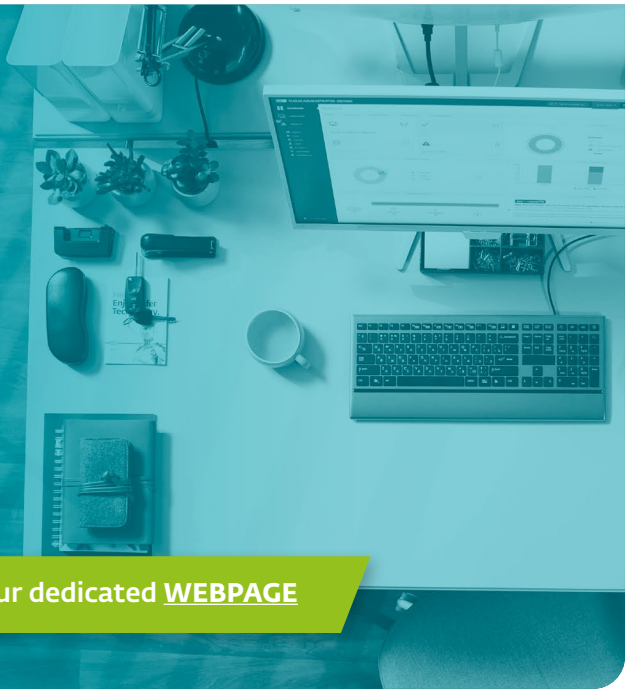
Tell your home-connected workers to enable automated updates on all of their systems, to make sure they're current with all security measures. Double-check whether your internal environment is up-to-date as well, especially security-critical items and systems that might remain unpatched because they run 24/7. Be extra careful of home-connected machines running Windows 7, which is no longer being updated. You might need to simply bar access until it's been upgraded to a supported version.

Provide cybersecurity training for employees

No matter how much technology you put in place, one other important piece of protection is between your employees' ears. Fake notices from work to confirm login credentials, visit business-related websites, handle requests from the boss to facilitate a payment or funds transfer, and other scams will be on the rise as cyberthieves try to cash in on home-connected workers. Knowledgeable, vigilant employees are less likely to fall for them. Especially when they're working remotely, a regular training program will keep their guard up.

Here's the good news

Cloud-based productivity suites, online collaboration through chat and conferencing, and other internet-connected and remote-access technologies can have home-based workers as productive as they are at the office – often even more productive. When they take their work home with them, make sure you send the right security measures along.



For more information on ESET security solutions, visit our dedicated WEBPAGE