GUIDE

REMOTE WORKERS AND IT SECURITY

Five things to do today to keep your organization's network and data secure

Remote employee security checklist

- Hover over links and review the URL.
- Avoid clicking on links from unknown sources.
- Always use a Virtual private network (VPN) connection.
- Change your home router password.
- Regularly install program and firmware updates.

When circumstances require you to close down offices and buildings, it is important to ensure your employees still have access to online tools and systems to remain productive. A shift to remote working means a potential increase in the number of vulnerable devices accessing your network. This can have an impact on your data security.

Here are five things you can do right now to make sure your organization is protected:

Share data security best practices with remote workers.
Remote workers have caused a security breach in 20 percent of organizations.[1] Keep data security best practices top-of-mind with employees. Now is a good time to remind them about remote work policies and have employees retake your cybersecurity training course.

Educate employees on common and evolving phishing threats.
Phishing is one of the top cybersecurity threats. The sophistication of cybercriminals means they are creating relevant and timely new phishing scams to bait employees to click on email links that allow the cybercriminals to penetrate your organization's network. In a recent study from Cisco — 2021 Cyber security threat trends: phishing, crypto top the list — 86% of organizations reported having at least one user connect to a phishing site.[2] This means your organization may be just a click away from considerable risk. Remind employees to hover over links and review the URL. They should avoid clicking on links from unknown sources.

Recommend employees disconnect or secure vulnerable devices (old printers, etc.) on home networks.
Many people leave their home networks vulnerable. They don't frequently change their router password or regularly install program and firmware updates. These software and firmware updates often include patches for security vulnerabilities. Encourage employees to regularly check for updates, update passwords or disconnect vulnerable devices from their home networks.

Make sure employees know how to report a cyberattack.
65 percent of cyber threats go undetected by today's organizations.[3] When an employee suspects a cyberattack, you want to know right away. Make sure employees know your organization's preferred way to report a cyberattack.

Require working in your organization's secure environment.
Many employees will be connecting to their home wireless networks or using public WiFi to access their work email and tools. This can make it easy for cybercriminals to steal data and proprietary information. Remind employees they should always use a VPN connection, which encrypts internet traffic, especially when using unfamiliar WiFi networks.

It's a whole different business world with distributed workforces becoming the new normal. By implementing these fives tips you can increase the likelihood that your data will stay protected and employees productive while working remotely.

Spectrum Enterprise makes it easier to protect your network by designing, configuring and managing your internet security. A remote access solution is made possible through either our reliable, dedicated and scalable Fiber Internet Access (FIA) or our Spectrum Business Internet services, coupled with our Fortinet-based Enterprise Network Edge solution with security. This enables remote workers to securely connect to the network via encrypted VPNs. All of this is provided with no additional licenses to buy and with support for up to 50,000 users.

Spectrum Enterprise can help your organization improve security and safeguard your network.

Learn more

1. "Statistics Of Cyber Security Risks When Working from Home." Databasix, October 4, 2021.
2. "5 cybersecurity threats for businesses in 2021-and 3 tips to combat them." Security, Joe Banks, September 22, 2021.
3. "Cyber Threats: 65 Percent Go Undetected by Today's Organizations." Government Technology Insider, Jackie Davis, June 3, 2020.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Spectrum ENTERPRISE