via the Internet and the company network. As teleworking or working from home continues during the coronavirus, VPNs are critical to ...

Aug. 11, 2020

As more tax professionals consider teleworking during COVID-19, the Internal Revenue Service and the Security Summit partners are urging practitioners to secure remote locations by using a virtual private network (VPN) to protect against cyber intruders.

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. As teleworking or working from home continues during the coronavirus, VPNs are critical to protecting and securing internet connections.

Using virtual private networks is the third in a five-part Security Summit series called

without. The risk is real. Taking steps now can protect your clients and protect your businesses."

Failure to use VPNs risks remote takeovers by cyberthieves, giving criminals access to the tax professional's entire office network simply by accessing an employee's remote internet.

Tax professionals should seek out cybersecurity experts if they can afford it. If not, practitioners can search for "Best VPNs" to find a legitimate vendor, or major technology sites often provide lists of top services. Remember, never click on a "pop-up" ad marketing security product. Those generally are scams.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) also encourages organizations to use VPNs. CISA also offers this advice:

- Update VPNs, network infrastructure devices and devices being used to remote into work environments with the latest software patches and security configurations.
- Alert employees to an expected increase in phishing attempts.
- Ensure information technology security personnel are prepared to ramp up these remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Implement multi-factor authentication on all VPN connections to increase security. If multi-factor is not implemented, require teleworkers to use strong passwords
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.

Technology