

Risk Insights

Consider These Five Reasons to Offer a VPN to Remote Employees



With businesses sending employees to work from home in the wake of COVID-19, the cybersecurity of their home offices has become paramount.

One of the best ways to keep employee and business data protected is by having them connect via Virtual Private Network (VPN).

As a small business owner, it's important that you invest in the right protection to help safeguard your business in difficult times. If you're reluctant to take on the expense, you might be surprised at how little it costs. At TruShield, we offer flexible policies with tailored coverage you can rely on.

To learn more about our offerings and how we can help you grow your business, contact us today!

trushieldinsurance.ca | 1.833.692.4112

Here are five ways VPNs can keep remote employees secure:

01. BETTER NETWORK AND FIREWALL PROTECTION

By routing an employee's Internet traffic through your company network, you can provide the same firewalls and network-level protection that they'd have working at an office with robust cybersecurity defenses.

02. A VPN CAN ADD ANOTHER FACTOR OF AUTHENTICATION

Multi-factor authentication isn't perfect, but it does help add an extra layer of security to your network. Being able to create complex passwords for employees to access company data means less concern about being compromised by predictable and easily guessed logins and passwords.

03. YOU CAN RESTRICT ACCESS TO COMPANY DATA

Restricting access to a VPN to current employees means it's easier to spot a usage anomaly. If you're seeing 19 employees connected from Toronto, ON and one connected from Moscow, it's easier to spot a potential cyber event.

04. THEY CAN PROTECT YOUR DATA FROM THE OUTSIDE WORLD

Data leaks from unsecured servers are a regular occurrence, and the risk only grows from having more remote employees accessing them from multiple off-site locations. Putting your data behind a VPN and requiring authenticated access can prevent it from being discovered online.

05. PROTECTION FROM PUBLIC AND SHARED WI-FI

While many employees are staying quarantined at home, some don't have reliable or fast Internet access and need to rely on either public or shared Wi-Fi. A well-secured VPN connection means that employee data is encrypted and harder to intercept when being transmitted through a shared or suspect Internet connection.