How the Shift To Remote Work Has Impacted Business Security

By Erika Fitzgerald for publication under Jeff Shiner's byline
--

As we emerge from pandemic-induced shutdowns, many businesses are settling into new ways of working. But, as with anything new, there's a learning curve. That's why we're here with a how-to on maintaining business security in an evolving environment.

While COVID-19 initiated a massive turn to WFH, remote work was already trending upward. According to a recent analysis, remote work in the United States grew 44% over the last five years and 91% over the last ten years.

However, the rapid rise of remote work opens new security risks. Stay ahead of evolving security threats associated with a more distributed workforce.

There's no reward without risk

With 68% of workers preferring to work from home in some capacity, one thing is true: remote work is here to stay. Flexible work arrangements present many opportunities for increased growth, productivity, happiness, and well-being.

Yet, remote workers can unknowingly overlook security risks. After all, not every employee is an IT pro – and that's okay. Nevertheless, companies can reduce risk by ensuring employees have the tools and know-how to work securely from anywhere.

These common security gaps can help you and your workforce block entry points for bad actors.

- **Insecure passwords.** Simple passwords are easy to crack. Hackers can access multiple accounts if employees use the same password. We found that 26% of people still use their first-ever password for an online account. And 51% of parents working from home admit their child has accessed their work accounts. The more someone uses a password, the weaker it becomes.

- **Less secure Wi-Fi networks.** At the office, IT controls Wi-Fi security. However, networks have fewer security protocols at home, such as WEP instead of WPA2. Even worse, if an employee works from an unsecured public network, such as a cafe or airport, their device is a free pass for attackers.

- **Phishing attacks.** Lately, we've seen a rise in malicious emails – or "phishing scams" – preying on COVID-19 fears. These emails trick users into opening malicious links and attachments to gain remote access to the entire system, including passwords and files.

Ultimately, the sudden shift to remote work has created some blind spots for IT. For example, IT can't remotely monitor devices with the same level of scrutiny. As a result, hackers can seize opportunities to attack vulnerable employees and networks.

Respondents to one survey reported increased security breaches during shelter-in-place orders. 23.8% paid extra expenses to address a cybersecurity breach or malware attack. And 19.8% dealt with a remote worker.

Those who adapt will prevail

Today, most employees cite flexible working as a priority. And companies that embrace remote work security will emerge stronger in the end. To stay ahead, issue secure company devices and empower employees with these protocols:

- **Deploy a password manager.** Businesses need to invest in enhanced security measures. 1Password Business makes it easy to generate secure passwords and share them with remote workers.

- **Take advantage of multi-factor authentication.** Multi-factor authentication – such as two-factor authentication and Duo – adds an extra layer of security to your Secure Remote Password. Think of it as a second barrier to entry against unwanted visitors.

- **Connect through a VPN.** Strong passwords combined with multi-factor authentication on a VPN are the holy grail of security. The VPN allows users to connect their devices to any Wi-Fi via an encrypted tunnel that safeguards against security threats.

Building a secure "work from anywhere" system requires some IT investment upfront. But, the cost of ignoring security? It's insurmountable.

1Password started as a remote-first company 14 years ago, and we've been working remotely ever since. So, we have experience maintaining security across a distributed workforce. And we're here to support organizations like yours in the future of remote work.