Expert commentary: COVID-19 pandemic poses privacy challenges to companies operating remotely

By Gabrielle Hermier at Surfshark | 승인 2020.03.21 03:18

Why businesses resort to VPNs during COVID-19 crisis

Source: Surfshark.com

COVID-19 pandemic poses privacy challenges to companies operating remotely. Surfshark is giving away six-month VPN protection plans for small businesses as more people resort to working from home.

Due to the rapid COVID-19 spread, many companies are experiencing a new challenge of remote work. For most, the situation comes as a stress-test of operating teams using only online tools and means of communication. As more countries tighten quarantine measures, privacy protection company Surfshark is giving away six-month subscriptions for small businesses seeking to ensure a safe environment for people working from home.

"Internal networks in office spaces are carefully set up, maintained, and protected by IT admins. It's much more difficult to ensure the safety of each remote employee's network," says Naomi Hodges, the Cybersecurity Advisor at Surfshark. "Demand for VPNs has surged significantly – we've received a high number of requests from businesses seeking to warrant that their employees have a safe and private workflow from home. Since Surfshark believes that privacy is an inherent human right, we will provide small businesses with our software for free, as part of our efforts to secure people who are working remotely against cyberattacks."

Although it is unsavory, crises such as the COVID-19 outbreak usually trigger a response in the criminal communities. Cybersecurity is unlikely to be an exception. Hackers will get access to too many easy targets and weak links to break.

When somebody works at the office, the internal network they connect to usually offers a good layer of security. The concept of working from home removes all these security measures which result in an increased risk of data breaches and leaks of confidential information. That is especially true if they opt to use a shared internet connection.

"People working from home are very appealing to cybercriminals," says Naomi Hodges. "It's difficult to ensure that they follow all the necessary security measures. For example, using 2FA and strong passwords, ignoring suspicious emails, always keeping a VPN on – especially if working on shared Wi-Fi. Criminals always look for the weakest link, and an unsuspecting employee is a perfect target."

VPN usage is highly recommended when working outside the office. If an employee connects to the internet via a VPN, they encrypt all the data that is being transmitted. That makes it extremely difficult for cyber attackers to intercept it and helps secure any sensitive information.

While working remotely without maintained security measures, an employee's device can also get infected by malware. Plus, there is always the oldest trick in the book – phishing: "As a form of social engineering, it's still one of the most reliable ways to gain access to a network – by merely tricking a person," says Naomi Hodges. "When employees are aware of the risks, they are in a much better position to confront this daily reality and assess any situation that may arise correctly."

By Gabrielle Hermier at Surfshark