[COVID-19] 10 Tips to Stay Safe from Cyber Threats While Working from Home

Devolutions

BUSINESSES MUST ADAPT AS FAST AS POSSIBLE TO SURVIVE THIS UNSTABLE AND VOLATILE PERIOD

In the past, remote workers — who were typically called teleworkers or telecommuters — were the rare exception, and the envy of folks who had to endure a miserable commute, or slog away from 9-5 in a tiny windowless cubicle.

The situation is radically different today due to the COVID-19 pandemic. Businesses must adapt as fast as possible to survive this unstable and volatile period. Now, remote workers are no longer just a piece of the workforce puzzle, they have become the centerpiece.

While companies are doing everything they can to get through it, hackers take advantage of the situation to steal data. As a result, both organizations and remote workers need to play an active role in closing security gaps and reducing the size of the threat surface. **Here are 10 tips that help keep remote workers safe and hackers at a distance.**

1. Use Mobile Data Hotspots and/or VPNs

Remote workers love public Wi-Fi access, because it's available virtually everywhere these days —doctors' offices, airports, restaurants, and the list goes on. Unfortunately, hackers love public Wi-Fi as well, because they can snoop, phish and spoof with remarkable ease.

One option to address this risk is to provide remote workers with mobile data hotspots. If this is not cost-effective, then at least remote workers should use a good virtual private network (VPN). While VPNs are not 100% bulletproof, they are massively more secure than ordinary public Wi-Fi access. To learn more, read the article "Should You Use a VPN?"

2. Segment Home Networks

Many remote workers mistakenly believe their home network is secure, when in fact it can be just as vulnerable as a public Wi-Fi network. While using a VPN (as noted above) helps reduce the risk, remote workers should go a step further and segment their home network and isolate it behind a business-grade firewall.

3. Use Two-Factor Authentication (2FA)

2FA is an extra layer of security that requires remote workers to verify their identity by providing their login credential, along with another piece of information that could be:

- Something they know, such as the answer to a secret question, a PIN or a password.
- Something they have, such as a smartphone, a token or a credit card.
- Something they are, such as their fingerprint, voice recognition or an eye scan.

The basic idea is that even if a remote worker's login credentials are stolen, it's unlikely (albeit not impossible) that hackers will be able to supply the additional information and access a device, application, network or system. We also recommend using Devolutions Authenticator, which supports texting, push notifications and email.

4. Use a Robust Password Manager

To strengthen security, remote workers (along with in-house workers) should use a robust password manager like Devolutions Password Server or Devolutions Password Hub that offers features such as password rotation, a strong password generator, automatic checks against passwords that have been exposed during hacks ("pwned"), and real-time email alerts in the event of unauthorized access attempts. Remember: the vast majority of data breaches are caused by stolen or weak credentials.

5. Install Endpoint Security

Endpoint security is a critical line of defense to keep hackers from launching attacks against devices, and ultimately shifting their attack to networks and integral systems. Key endpoint security tools include:

- Network firewalls (both on endpoints and home networks)
- Anti-virus software
- Software updaters (more below)

While it may be fine for some organizations to let their remote-working IT pros decide when to update their software, for general business users the best practice is to put remote devices on a standard image and activate automatic updates for all apps and programs — especially security software.

6. Use a USB Data Blocker

If remote workers need to charge their device and the only option is a public USB charging station, they should always use a USB data blocker. This allows the power leads to connect (and the charge to occur), but it does not expose data pins inside the device, thereby preventing data exchange and protecting against malware.

7. Use a secure remote access solution

In remote work, IT professionals must always have secure access to business critical assets. Whether they need to update machines in the computer network or to assist users remotely, the ideal is to use a complete remote access solution that is quick and easy to deploy. Wayk Now is one of those affordable solutions, as it offers a free edition for personal and commercial use.

If the organization is looking for advanced features, such as unattended access, concurrent sessions, remote execution and session recording, the Enterprise edition meets their needs. It is subscription-based and offered at a competitive price.

IT professionals can also acquire Wayk Den, a free self-hosted server, to manage all the machines in the IT infrastructure. They can check the centralized dashboard to find out which machines are connected, view audit trails for compliance, and more.

Due to COVID-19, an unlimited number of Wayk Now Enterprise subscriptions are included with any private Wayk Den deployment for the next six months.

Different remote access solutions exist, so here is an overview of what is on the market.

8. Provide Ongoing Cybersecurity Training

All employees need ongoing cybersecurity training, but especially remote workers who can sometimes let their guard down since they're not constantly being reminded to follow best practices (or to put things more bluntly, they aren't too worried about facing the wrath of IT because they're located elsewhere). Cybersecurity training should include aspects like:

- How to recognize and avoid online scams
- How to choose strong passwords or passphrases
- How to protect data at home

In addition, remote workers should be cautioned against over-sharing on social media — such as checking-in to apps when they arrive at hotels, airports and so on — since such activity can draw the attention of hackers, who can use the information to hunt down victims. Remote workers should also keep their devices with them, and never leave them unattended for even a few seconds. When leaving home, devices should always be securely locked away vs. left out in the open for burglars to easily and quickly grab.

9. Switch to Cloud-Based Storage

Storing data in the cloud isn't just more convenient for remote workers, but it also enhances protection from threats like ransomware. Plus, if a device is stolen, then access to cloud-based data can be controlled by changing passwords or locking it down. To learn more, read the article: "Robust IT Security Comes to the Cloud".

10. Use Screen Protectors

It may be very low tech compared to some of the other tools on this list, but screen protectors are a highly effective way to keep "shoulder surfers" from snooping and stealing data. Every remote worker should have one.