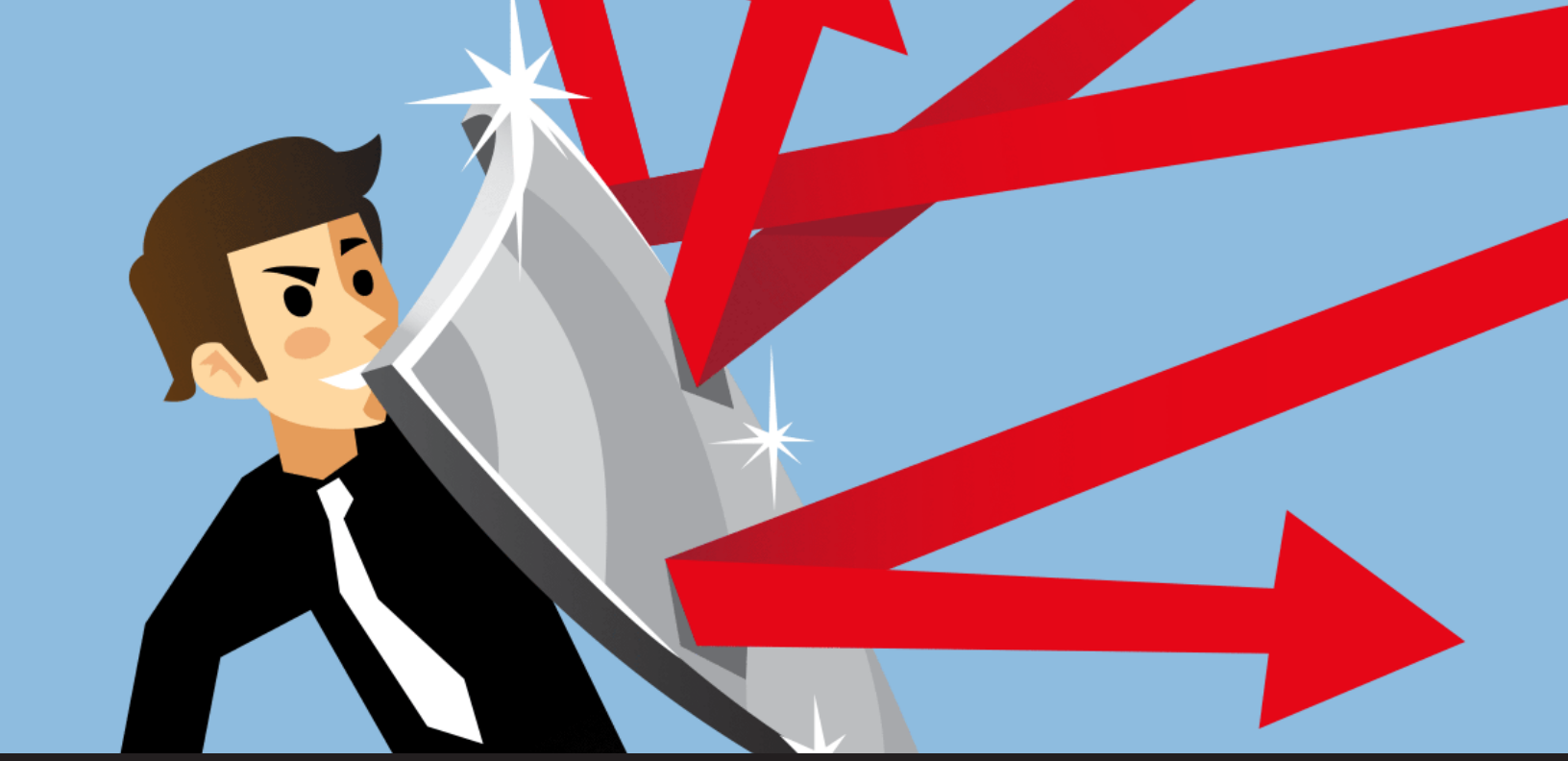

10 Tips to Keep Remote Workers Safe from Cyber Threats

Devolutions

REMOTE WORKERS AREN'T JUST A MAJOR PART OF THE WORKFORCE PUZZLE, THEY'VE BECOME THE BIGGEST PIECE.

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.

But these days, the situation is dramatically different. Remote workers aren't just a major part of the workforce puzzle, they've become the biggest piece. Here are the eye-popping statistics:

- 55% of employees currently work remotely on a full-time basis. (Source: AND CO)
- 70% of employees currently work remotely at least one day a week. (Source: International Workplace Group)
- By the year 2020, 72% of the workforce will work remotely either part-time or full-time. (Source: IDC)
- 90% of remote workers plan on working remotely for the rest of their careers. (Source: Buffer)

And it's not just remote workers who are reaping the rewards. Organizations that equip and enable remote workers are enjoying key benefits as well, including:

- Saving an average of $2,000 in real estate costs for each remote worker. (Source: Stanford University)
- Generating a 25% lower turnover rate vs. organizations that don't offer remote working. (Source: Owl Labs)
- Getting, on average, more productivity from their remote workers than in-office workers. (Source: Polycom Inc. & Future Workplace)

Despite this good news for both employees and employers, there is an uninvited and unwelcome guest lurking around every corner, trying to crash the remote working party: hackers. 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. For a comparison of popular 2FA tools, **click here**.

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
- Anti-malware 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. Aim for COPE, Settle for CYOD, and Avoid BYOD

When it comes to remote device security, the gold standard policy is Corporately-Owned, Personally-Enabled (COPE). But although IT teams love COPE, it is costly for the organization and restrictive for end users — which leads to complaints and, in some cases, circumvention. As such, if COPE isn't affordable or practical, the next best policy is Choose Your Own Device (CYOD), which supports streamlined support and procurement standards. Yet again, however, this can be costly and end users can fight back against limitations.

The last option on the list is Bring Your Own Device (BYOD). While this is certainly more affordable and more end-user-friendly than COPE and CYOD, it poses significant security risks. To mitigate the inherent risks of relying on BYOD, organizations should have a comprehensive and up-to-date mobile policy and security enforcement in place, and they should augment these with ongoing training (see below).

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.