8 Safest Computing Strategies for Remote Employees

TechRounder PDF Edition

Live article: https://www.techrounder.com/technology/8-safest-computing-strategies-for-remote-employees/

By Vipin PG | Published February 4, 2021 | Updated January 4, 2026 | Format: Article | 5 min read

In brief

Are you still working from home even when the scourge of pandemic has subsidized?

Are you still working from home even when the scourge of pandemic has subsidized?

Is your organization on the verge of adopting the remote working scenario for a select set of employees for an indefinite period?

Lastly, are you finding it hard to adjust to the new normal that advocates the WFH culture?

If the answer to each of these questions is in the affirmative, keep reading on as we enlist 8 of the most crucial computing strategies that remote-working employees can follow. These 8 computing ways are targeted towards maintaining the perfect cybersecurity posture, which is one of the primary concerns for organizations in the post-pandemic era, especially for the remote workforce.

Analyze the Importance of Corporate Cybersecurity

As an employee, you must realize your role as the first line of defense that an enterprise has against cyber attackers. Although each work module that you send across goes through the IT administrators, you should be responsible for following computing approaches that are safe and non-invasive.

Based on the 2020 breach report released by Verizon, almost 30 percent of breaches and threats actually involved intrinsic factors, like misappropriate device usage on the part of the employee or something similar.

The results show that employees need to ascertain their roles in the corporate cybersecurity realm and must help the enterprise bridge the glaring void between productivity and middling IT security standards.

Refrain from Shadow IT Devices

While this approach holds true even for the on-premise employees, it makes more sense for the remote workers. The concept of shadow IT has gained precedence in the post-covid era where an employee working from home continued to use the same wireless networking for connecting each of their many smart devices.

For instance, a person using a streaming device on the home-bound television unwittingly connects the work laptop to the same Wi-Fi network, thereby exposing the corporate system to the Fake IT or Shadow IT threats. While your corporate device might be secured, the unsecured app store and IoT premise of the streaming device might allow the attackers to penetrate the organizational line of defense.

While a good way to avoid the same is to use separate networks for work and leisure, it is also important to side-load not only the best but safe apps onto the streaming device. Although using multiple IoT or wireless devices at home is common, threats show up when devices like the Fire TV Stick are stacked with applications having unscrupulous identities.

Even though using a streaming device with pre-loaded apps still makes sense, Shadow IT becomes a cause for concern if you jailbreak the device and use relevant yet shady third-party applications on the same. Therefore, the idea is to be discrete, get a VPN for the job to manage anonymity, and even keep learning about the best and safe applications that go well with the streaming device.

Or else, you can ditch the home network completely for managing corporate tasks!

Check Extensively for Phishing Emails

A report released by Tessian reveals at least 25 percent of the corporate employees end up clicking on phishing emails. Complementing this finding is a study from PhishMe, stating that an employee who responds to a phishing email just by clicking is 67% more prone to future attempts.

While phishing might sound like a basic attack via a fake email or message, it can easily expose the employee credentials and allow hackers to access the corporate systems. While the Verizon report categorizes phishing as one of the more prominent reasons for data breaches, precisely with a 22 percent exposure, lately attackers have been clubbing the same with social engineering or a more manipulative form of unauthorized system penetration.

A good approach to keep these threats at bay is by learning more about the anti-phishing practices whilst coordinating extensively with IT administrators.

Opt for Stronger Passwords

As a remote-working employee, you need to be mindful of the system access passwords. A good way to approach this computing strategy is by avoiding password reuse. Apart from that, you can always talk to the IT administrators to get hold of an IAM or MFA module for your system.

Not just that, password sharing, regardless of who asks for the same, is strictly prohibited! Besides, it is crucial to ideate long, intuitive, and simple passwords, while writing the same down for improved access.

Avoid Office Gadgets for Personal Indulgences

While you might feel shopping for a new product from the office laptop wouldn’t do any harm, it can certainly open a new can of worms for your organization. A company sends over periodic security patches to the home-bound workforce, thinking that the hardware isn’t open to commercial or personal usage.

Downloading a movie or even something as basic as opening a personal tab on the corporate device can interfere with the internet or networking policies of the employer, which might put the gadget and even your sanctity at risk. A good way to steer clear of these threats is to avoid high-risk websites and installing any unwarranted software solution on the concerning gadget.

USB Devices are Threats

Most laptops provided by companies are often USB locked. However, if you are forced to use a home-bound machine, it is necessary to stop using portable devices that offer ready storage support. Even if you plan on transferring something from one point to the other, opt for USB devices that are personal and not provided by some third-party sources.

While USB-centric threats might feel inconsequential, rogue devices can be extremely harmful and sabotage the existing information sets, if left unattended. A good way to combat the issue is by reaching out to the IT administrator, precisely to get the USB scanned and authorized for professional usage.

Social Media should not be about Work

You are mistaken if you feel that being associated with a reputed firm gives you bragging rights. While you can always flaunt your achievements, you should never resort to social media interactions that require you to reveal the nature of your work. Besides, every company has a specific set of social media policies that employees need to adhere to. However, even if the organization doesn't restrict your free will, consider this as a proactive approach to strengthen the cybersecurity posture.

Public Wi-Fi is a Bane

While public Wi-Fi is a boom for the millennial population, corporate entities must stay away from the same for obvious reasons. In most cases, a public Wi-Fi setup, in absence of a reliable and paid VPN, works as a traffic sniffer or honeypot. However, if you are bound to use some form of internet connectivity while being on the move, rely on the mobile hotspot and that too if the device is encrypted categorically by an enterprise-grade Virtual Private Network solution.

Each of the mentioned strategies requires you to be vigilant regarding work. Moreover, you must understand that work from home has already transformed into a more permanent operational pattern for most organizations, which in turn makes these safer computing strategies even more relevant.

References

1. enterprise.verizon.com - resources / reports - https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/

2. firesticktricks.com - amazon-fire-stick-apps.html - https://www.firesticktricks.com/amazon-fire-stick-apps.html