Working From Home? Here's What You Need for a Secure Setup

The current workplace reality is that, in response to the ongoing coronavirus (COVID-19) outbreak, many companies around the globe have rolled out work-from-home arrangements. As a result, there has been an influx of employees signing in remotely to corporate networks and using cloud-based applications. But this shift could also open doors to security risks and cyberthreats.

Security teams and home office users, however, can minimize the risks that come with remote-working setups. Below are some practical security measures that can be applied to this end:

- **Use a company laptop for remote work if possible**. Do not use your personal machine as it may have fewer security controls than your company-owned hardware. Work-issued laptops or machines should be for employee use only; other members of your household should not have access to your dedicated work equipment.

- **If use of personal equipment cannot be avoided and you have to use your own machine, keep it as close as possible to office security standards**. Use security software provided by your company, follow company data protection measures, and do not mix personal browsing and activities while working.

- **Use company-designated VPNs and avoid free, public Wi-Fi**. Use the dedicated enterprise VPN servers only on your work laptop or desktop to make the connection between your network and the office's secure. But be wary of phishing attacks that steal VPN-related account credentials. If VPN connectivity is not on the table, ensure that data communication is done via encrypted email or Pretty Good Privacy (PGP) encryption.

- **Remember to back up data**. Follow the 3-2-1 rule in backing up data: Create at least three copies of the data in two different storage formats, with at least one copy located off-site (e.g., provide external SSD or HD drives).

- **Set up your 2FA**. Many major websites and services are implementing two-factor authentication (2FA). Make sure to have logins set up to not rely on passwords alone (e.g., use authentication mobile apps or biometrics). Passwords have time and again been hacked, leaked, or stolen.

- **Split networks**. Use a guest network to isolate the company laptop or desktop. If you have a router or switch with a virtual local area network (VLAN) functionality, activate it and dedicate a VLAN for office work only.

- **Prepare a backup solution at home**. Having backup options (e.g., hardware such as USB hard drives) puts you in a better position when something goes wrong, such as connectivity loss or server failure. For macOS users, Time Machine can be activated to create backups.

- **Secure the gateway: your router**. The router is the gateway to all internet-connected devices in your home network. Attackers are known to compromise home routers with default credentials that users often neglect to change. It is good practice to regularly change the password for your router as it may have been previously shared with other users. Passwords that are not prone to dictionary attacks are recommended, i.e., those that have more than 12 characters, with a mix of letters, numbers, and special characters.

  Likewise, it is important to always update the firmware of your router to the latest version. Routers issued by internet services providers (ISPs) usually have automatic updates, but due diligence can be done through a router's web console, which is accessible using its IP address.

Since kids are also staying at home, likely having their online classes, and other members of the family may also be working remotely, home network security basics such as creating backups and employing a proxy service should be adopted. Create a safer digital environment by employing home network security that not only can block and filter sites, but can also protect your network and devices against hackers and web threats.

- **Protect data against ransomware and theft by enabling Folder Shield**. You can also consider employing router security that allows device management (e.g., disconnecting unwanted devices in the network), controls social media use, blocks inappropriate sites, and sets time limits for device usage.

- **Protect smartphones**. As with laptops and desktops, make sure phones are updated with their latest firmware versions. Download only legitimate apps from official stores and review the app permissions before installing them. Install a mobile security app to prevent malicious apps or codes from running on phones.

- **Save bandwidth**. As more users stay and work at home, bandwidth becomes a critical resource. Ensure seamless productivity by reducing consumption in streaming videos and other activities that throttle the bandwidth, especially during work hours.

- **Discuss the importance of online safety**. Help your family understand the public nature of the internet and its potential dangers. Remind them that they are responsible for ensuring that their online activities are safe and private by securing the way they set up and use their devices.

Setting up a secure remote-working environment is not an overnight job. It requires considerable effort from all people involved, especially in the case of those who are new to telecommuting. The measures laid out here should help companies and employees ease the burden and effectively protect work-from-home setups from cyberthreats.

COVID-19 Used in Malicious Campaigns

COVID-19 is being used in a variety of malicious campaigns including email spam, BEC, malware, ransomware, and malicious domains. As the number of those afflicted continue to surge by thousands, campaigns that use the disease as a lure likewise increase. The mention of current events for malicious attacks is nothing new for threat actors, who time and again use the timeliness of hot topics, occasions, and popular personalities in their social engineering strategies.

Email Spam

Many aspects of daily work, from meetings to presentations and collaborative tasks, have moved online because of quarantine restrictions affecting offices across the globe. As users adapt to new methods of working, they should be wary of cybercriminals using popular online tools, sharing software, and file attachments in their scams.

Many of the emails, purportedly from official organizations, contain updates and recommendations connected to the disease. Like most email spam attacks, they also include malicious attachments. One of the samples used the email subject “Corona Virus Latest Updates” and claimed to come from the Ministry of Health. It contained recommendations on how to prevent infection and came with an attachment that supposedly contains the latest updates on COVID-19 but actually carried malware.

Many of the spam emails were related to shipping transactions, either postponement due to the spread of the disease or one that provides a shipping update. One email informed about shipping postponement. The attachment, supposedly containing the details of the new shipping schedule, bears malware.

Malicious Websites

Cybercriminals are taking advantage of the public’s need for information, assistance, and supplies to victimize users. The US Department of Justice (DOJ) filed a temporary restraining order against a fraudulent website that is supposedly selling COVID-19 vaccine kits approved by WHO. However, there are no WHO-approved legitimate COVID-19 vaccines available in the market yet.

Malicious actors are also aware that many users across the globe are quarantined and spending more time looking for entertainment online. They use fake streaming sites, or sites offering entertainment promotions to appeal to users. As always, users should always be mindful of websites they regularly use, and to keep credentials to online accounts as private as possible.

Mobile Threats

A mobile ransomware named CovidLock comes from a malicious Android app that supposedly helps track cases of COVID-19. The ransomware locks the phones of victims, who are given 48 hours to pay US$100 in bitcoin to regain access to their phone. Threats include the deletion of data stored in the phone and the leak of social media account details. A look at their cryptocurrency wallet shows that some victims have already paid the ransom on March 20.

There are also reports of malicious Android apps offering safety masks to targets worried about COVID-19. Unfortunately the malicious app actually delivers an SMSTrojan that collects the victim's contact list and sends SMS messages to spread itself. So far, the app seems to be in the early stages of development and is simply trying to compromise as many users as possible.

Browser Apps

A new cyberattack has been found propagating a fake COVID-19 information app that is allegedly from the World Health Organization (WHO). Bleeping Computer reports that the campaign involves hacking routers’ Domain Name System (DNS) settings in D-Link or Linksys routers to prompt web browsers to display alerts from the said apps.

Users reported that their web browsers automatically open without prompting, only to display a message requesting them to click on a button to download a “COVID-19 Inform App.” Clicking on the button will download and install the Oski info stealer on the device. This malware variant can steal browser cookies, browser history, browser payment information, saved login credentials, cryptocurrency wallets, and more.

Protecting Yourself Against Scams

Unfortunately, scammers use current situations like the COVID-19 pandemic to prey on collective fear and misinformation for their fraudulent activities. There are measures you can take to avoid getting duped.

- Be wary of telltale signs of phishing scams: unknown senders, glaring grammatical errors, mismatched URLs, and outlandish stories.
- Do not provide your identifiable information such as personal details and bank account information. Check if a site is asking for more information than what’s logical. For example, signing up for a newsletter or notification list shouldn’t require you to share your email password.
- Cybercriminals might use “related” URLs (e.g., “paypalsupport-coronavirus”) to trick users into thinking legitimate organizations are using specialized websites for the pandemic. Users should also check such sites by looking at the company’s official sites or social media for any evidence that they have new domains up and running.
- A multilayered protection for your devices, such as computers and mobile phones, is also recommended for protecting all fronts and preventing users from encountering threats, such as spam and malware.

Note: You may also view this newsletter on www.score.org and www.trendmicro.com/ISSB