Cyber Security Tips and Advice for Remote Workers

COVID-19 is rapidly changing how we work, communicate, and interact with one another. Some private companies, public institutions, and government departments are mandating that all employees who can, must work from home.

For many users this is the first time they have worked from home. Not only is there the stress of the uncertainties around COVID-19 but also an adjustment period for people transitioning their work habits to home. This also applies for students that have been asked to take their classes online, from home. The tips and best practices listed below are intended for this clientele as well.

As a security leader, you know how challenging it can be for people to remain cyber secure in an office environment where cyber security is part of the culture. Now with employees working remotely, it is extra challenging to ensure that people maintain their cyber secure best practices and habits.

To help support security leaders and employees during this transitional period, we have created a special kit dedicated to cyber security for remote workers. This blog is part of the Working From Home Cyber Safely Kit and is focused on giving you and your employees actionable tips and habits that can keep everyone cyber secure when working remotely, using mobile devices, and traveling.

And because there is a rise in COVID-19 phishing and social media scams, we've included a section on how to identify cyber threats.

How to Stay Cyber Secure When Working Remotely

Security awareness is very much top-of-mind when people are working in an office environment. However, when people change their work routines, their cyber security habits can also change.

To stay cyber secure when working remotely, employees can do the following:

- Use a secure connection to connect to the company network. Ensure the company VPN is configured to use multi-factor authentication.
- Only work from home and do not connect to the company network with any unsecured public Wi-Fi.
- Do not share work data and information with the home computer or personal devices. There is a risk that personal computers and mobile devices do not have the latest security updates for the operating systems and browsers.
- Make sure your computer has the latest applications, operating systems, network tools, and internal software installed. Have the IT/support team install malware protection and anti-spam software on laptops and computers.
- Create new and strong passwords for your laptop, corporate mobile device, and email.
- Use only approved cloud applications for sharing and storing data.
- Avoid storing or printing paper documents with sensitive information at their home.

The organization should continue to promote security awareness best practices and leverage, newsletters micro- and nano-learnings, and other campaign awareness tools. This keeps security awareness top-of-mind and helps reinforce the lessons learned from training and simulations.

How to Keep Your Home Computer Cyber Secure

Remind employees of these keys to home computer cyber security:

- **Keep all software up to date.**

  Ensure the latest operating systems, browsers, and apps are installed on computers and devices that connect to the Internet.

- **Install a home firewall and use a secure Wi-Fi connection.**

  These measures protect company assets and yourself from cyber-attacks.

- **Use antivirus software.**

  Use antivirus software to automatically scan websites, downloaded files, email attachments, and content stored on external hard drives, memory cards, and USB sticks.

- **Create strong passwords.**

  Strong passwords are just as important on the home computer and devices as they are on work computers and devices. Stop using names, favorite colors, or reusing same passwords for home and work devices.

- **Stay click aware.**

  It is easy to forget cyber security best practices when away from the office. The best strategy is to remain vigilant and skeptical of all unsolicited emails, text messages, social media chats, and attachments. When in doubt – don’t click.

Remind employees that they are the first line of defense against cyber-attacks. Reinforce to employees that you want them to doubt the legitimacy of emails, text messages, and social media chats – the best approach is to be extra cautious.

6 Tips on Mobile Device Cyber Security

Cybercriminals target victims however and whenever they can. And this means that mobile device cyber-attacks are on the rise.

Always follow these 6 tips on mobile device cyber security :

1. Disable Bluetooth audio discovery.

   Cybercriminals are on the lookout for Bluetooth signals that they can hack and use to connect to mobile devices.

2. Turn off auto-connect.

   Never connect to an open or public Wi-Fi network automatically. In fact, the best practice is to never connect to public Wi-Fi that is not password protected.

3. Use fingerprint security and visual authentication.

   Enable the highest level of security and authentication possible on your mobile devices. Make sure all mobile devices are protected by a password that is unique to them.

4. Latest versions of all apps and operating systems.

   Install all updates, these are typically released to fix known security weaknesses and to protect your device from cyber threats.

5. Be text message aware.

   Do not respond to text messages from people you do not know. Do not respond to unsolicited text messages from companies or organizations.

6. Be aware of data leakage.

   Do not authorize unlimited app permissions and access. Only give apps the minimum access required.

Remember the basics of cyber security best practices – never leave your devices unattended, lock your devices after use, and do not let a stranger use your mobile device.

COVID-19 Phishing and Social Media Scams

In recent weeks the frequency of COVID-19 phishing and social media scams has increased.

Cybercriminals are using convincing emails and social media posts disguised as coming from legitimate health authorities and government departments to prey on fears and unanswered questions about novel coronavirus.

Follow these cyber security awareness habits to stay protected from phishing and other cyber threats:

- If you don't recognize the email sender, don't open the email.
- Pay attention to the spelling of email addresses, subject lines, and email content.
- Be wary of emails that use urgent language and ask you to help out by transferring funds or sharing confidential information.
- Do not click on links from unsolicited emails.
- Never send confidential information in an email.
- When shopping online, always inspect the address bar and verify that the URL contains "https" or the lock icon.
- Do not accept social media followers or friends from accounts that you do not recognize. If an account that you do not trust follows or friends you, block the account.

If you're at all uncertain about the validity of an email or other message, do not respond. If you receive a strange email from a colleague or boss – talk to the person and ask them about the email.

Remind employees that security awareness and cyber security best practices apply everywhere – in the office, at home, riding the bus, in the airport, at the coffee shop, and wherever they are connecting to the Internet.

TERRANOVA
SECURITY