12 cybersecurity tips for the staff working remotely

Due to COVID19, companies have decided to opt for work-from-home policies asking their employees to self-isolate to prevent the spread of coronavirus. Technology has developed so much that people are convenient to work from the comforts of their home. But with this advantage, there is a chance that remote workers may lose their online security.

Here are some safety measures you can take to protect yourself from cybersecurity threats.

1. Use strong passwords

Make a strong password for your account. If you have multiple accounts, then don’t use the same password for each one. Ensure that your passwords have special characters and digits, characters comprising small and capital letters. Use a password manager like KeePass and LastPass to create, recall, and autofill the password for you.

2. Set up two-step verification

Make sure to use two-step verification (or two-factor authentication) for your accounts which include an additional step like biometric authentication, email, or text message confirmation to add one more layer of protection.

3. Use a Virtual Private Network

Using a VPN increases your online privacy. A VPN encrypts online traffic making it unreadable to anyone who tries to decrypt it. Make use of a VPN that is reliable and has a high speed.

4. Set up firewalls

Malicious programs can enter your device to leak confidential information. A firewall acts as a barrier between your device and the internet preventing your system from threats. Some of the best firewalls are SolarWinds Network Firewall Security, ZoneAlarm, TinyWall, and Glasswire.

5. Use an Antivirus Software

Use the best antivirus software to protect your system from malware. Even if malware enters the device then it detects it and removes it. Some of the best software are McAfee, Norton, Bitdefender, etc.

6. Take safety measures for your home router:

- Update your router with new firmware.
- Use a secure DNS service provider.
- The encryption should be changed from WPA2 to WPA3.
- Install firmware updates regularly.
- Use the highest level of network encryption and disable WPS.
- Choose a complex Wi-Fi password.

7. Install Updates regularly

Updates often include critical patches to security loopholes. Regularly update the device because it removes outdated features and improves the stability of the software. You can either set a reminder for updates or do it manually.

8. Regularly Back up data

Data from your device can be lost due to cyberattacks, physical damage, and human error. You can store your data in the cloud as it is convenient to use and also cost-effective. In cloud backup services, the user can customize the back-up schedule and storage options.

9. Check work from home scams

There is an increase in the work from home scams that targets economy workers. Many of the schemes demand your personal information or payments before you start to work. By the time you recognize them as a scam, the frauds might have already stolen your money.

Never share your personal information with a client without doing proper research and use only reputable and legitimate sites to work.

10. **Check for phishing emails and sites**

If you receive any mail from a company or website asking you to provide your personal information such as a password or social security number, then you can become their target. Delete it immediately and don’t download any attachments accompanying the mail.

For sites, check the validity of the web address.

Phishing sites lack the HTTPS padlock symbol. Check whether the URL starts with https:// or https://, the ‘S’ indicates that the website is encrypted with an SSL certificate. If not then don’t enter any information on it.

11. Use encrypted communications

You must use a secure way of communication while communicating with fellow workers. The messaging services of Whatsapp, Telegram, and Signal have end-to-end encryption. You can switch to specialized email providers such as Hushmail and SendInc to communicate via email.

12. Lock your device

Lock your device using a password to secure its contents until someone enters the password. Besides, you can use a full-disk encryption tool.

Use the above-listed tips to secure confidential information

and work safely from home.