WORK FROM HOME SECURITY BEST PRACTICES

1 CHANGE YOUR ROUTER PASSWORD

Change your internet service provider (ISP) router admin password from the out of the box default settings to protect from drive by breaches. Here's how to do it.

2 SECURE YOUR WIFI

Secure your WiFi by using stronger encryption and a secure WPA password. Check out these 5 tips for a secure wireless network.

3 ADD ENDPOINT PROTECTION

Run an endpoint-protection software (anti-virus, malware, spyware, and adware protection). Some effective and reliable options are McAfee, Norton, Webroot, Sophos and Bitdefender.

4 USE A PASSWORD MANAGER

Use a password manager solution to maintain unique complex passwords. E.g. LastPass. Additionally, don't send passwords, credentials, and personal privacy information(SSN, DL, CC) via email.

5 USE MULTI-FACTOR AUTHENTICATION

Most Cloud apps will allow for multi-factor-authentication (MFA) to be enabled, requiring your phone or email to provide an additional code to login over and above your username and password.

6 ATTEND SECURITY AWARENESS TRAININGS

Attend regular security awareness trainings to better be aware of social engineer tactics to gain access to your data. Here is a good example.

7 USE VPN SERVICES

Use virtual private network (VPN) services when using an unsecured Wi-Fi Service to protect from man in the middle cyber attacks. NordVPN is a good option.

8 USE CLOUD SERVICES

Use cloud services like Microsoft 365 or G-Suite to provide an off-premise store of your data.

9 USE A CLOUD BACKUP SERVICE

Use cloud backup services like Carbonite and Backblaze to protect from losing critical data stored locally on your computer

10 USE ENCRYPTED SERVICES

Use encrypted services for giving remote access to your computer. Do not leave agents running with a simple password access. Some good examples are Gotomypc, and Teamviewer.

11 LOCK YOUR SCREEN

Remember to lock your screen when you walk away from your computer to avoid someone from having easy access to important data on your devices.

12 SHRED YOUR PAPERS

Shred important and confidential documents well especially if you do not have a shredder at home.

13 PROTECTION FROM PHYSICAL THEFT

Don't advertise thru your windows all the additional computers around the home. Keep curtains closed, lock doors and lock screens.

SPECIAL EDITION

14 ZOOM BOMBING PROTECTION

a PROTECT YOUR MEETING

Zoom bombing, which sees uninvited guests crashing your meeting or chat, relies on meetings not being password protected. People often post the Zoom meeting number online, and without any protection, bombers can simply enter and do their worst.

b USE WAITING ROOMS

Another way to stop Zoom bombers from entering your chat or meeting is the use of waiting rooms. This allows the host to screen everyone entering the meeting to ensure no one uninvited can get in.

c SHARE THE PASSWORD SECURELY

Remember to lock your screen when you walk away from your computer to avoid someone from having easy access to important data on your devices.

d KEEP SOFTWARE UP TO DATE

One of the important steps you can take is to make sure you keep any installed version of the Zoom mobile or desktop app up to date, says security researcher Sean Wright.

ECHO TECHNOLOGY SOLUTIONS