8 RULES TO ENSURE CYBER SECURITY WHEN YOU WORK FROM .

Just as the lockdown started, most of the people seamlessly began working from home. As nobody was prepared for this, none were given adequate training or guidance about the basic security measures to protect their own digital security. As a result, criminals have found this as an easy surface to attack.

Here are 8 tips on keeping your digital activities secure while you work from home.

1. BEWARE OF PHISHING

- Always double check the e-mail sender's address. Even if you know the name of the person, verify if it is the correct e-mail address.
- Do not click on any link provided on the emails (or download files) from unknown people.
- If you have to open pdfs/docs/Excel-sheets from unknown senders, it is much better to upload them to a cloud service like Google Drive, and open via Web tools.
- If there is any known Web address in the e-mail, instead of clicking them, type them in the browser and open the site. Remember, criminals can easily fool you by faking URLs.
- If you receive any e-mail asking to check or renew your credentials even if it seems to have come from a trusted source, before responding try to verify the authenticity of the request through other means.
- Be particularly careful with any emails referencing the corona virus, as these may be phishing attempts or scams.

2. SECURE VIDEO CALLS

- For video chatting, it is always better to use Web clients inside of your browser. If you have to download and install any software, make sure that you are downloading from a legitimate website. Criminals often spoof websites and stack them with malware, which may spy into your

work or may be ransomware.

- Note that many of the well-known video-chatting services are not end-to-end encrypted. Do not share any password or authentication details over it. There is a chance that attackers can access that information.
- Don't share virtual meeting URLs, or screenshots from your video calls on the social media. You may accidentally be leaking information (meeting ID or other confidential information).
- Remember to close all software that are not required during the meeting.
- Connect to the internet via secure networks. Avoid open/free networks. Most Wi-Fi systems at home these days are correctly secured, but some older installations might not be.

3. DO NOT INSTALL ANY UNVERIFIED SOFTWARE

Do not download and install pirated software or anything else from random sites off the Internet. Many of them are malware ridden. Remember, since you are working from home, it may be difficult to get help in case of a cyber attack.

4. LOCK THE COMPUTER WHEN YOU ARE NOT USING IT

Even if you are inside the house, make sure to lock the computer screen when you get up. This is because someone in the house, maybe children, may click on the system and that could mean trouble.

5. REMEMBER TO ENABLE A FIREWALL

All operating systems come with default firewall systems and you should not disable them. They are essential to defending against many known attacks.

6. UPDATE YOUR SYSTEM DAILY

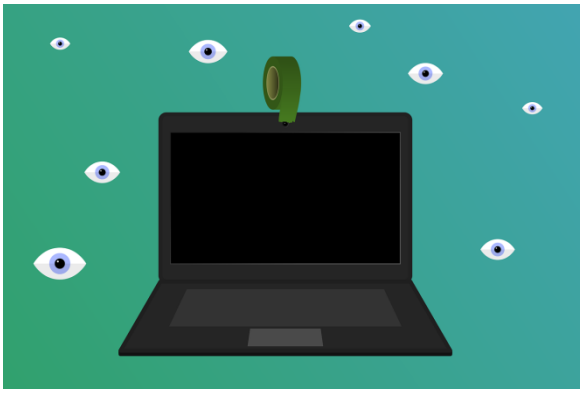
As and when companies find bugs in their software and OS, they are also fixing them by releasing regular updates. Make sure that every day, you find time to update your system. Just having the latest version will save you from many threats.

7. DO NOT USE A REMOTE DESKTOP (OR VNC) SERVICE UNLESS ABSOLUTELY NECESSARY

You may be required to remotely grant access to a computer from inside your company's infrastructure. But, if that is not required, make sure that those services are always off by default in your systems. Remote desktop/VNC services have been well-known attack vectors for many years, and a number of breaches happen through this route.

8. TAPE UP THE WEBCAM AND MUTE THE MICROPHONE BY DEFAULT

If you are not in a meeting, make sure that your webcam is either taped or blocked. The microphone should always be on mute. There will be times when private topics may be discussed, and having the microphone on mute will help prevent any leaks or unnecessary sharing of embarrassing information.



REF: https://m.economictimes.com/magazines/panache/tape-the-webcam-enable-firewall-11-rules-to-ensure-cyber-security-when-you-work-from-home/amp_articleshow/75005471.cms

https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home