Secure Your Data

as you

WORK FROM HOME

This is certainly a before and after moment in the history of the economy when the havoc caused worldwide due to COVID-19, has brought out a blessing in disguise, i.e. Digital Transformation. Everything about work has changed with employees working from home across locations. WFH brings great opportunities for organizations, but there lie risks on the other side. So, its important for businesses and employees to understand and recognize these risks and take necessary steps to protect themselves against these risks.

Citing this need, IPA organized a Webinar on SHIFT- Work From Home: Security and Digital Transformation on 30th April 2020 and invited two experts from this field to guide the IPA members and plumbing fraternity on this subject. Sandeep Sengupta, an Ethical Hacker, CISA & a Business Continuity Lead auditor and Col. Suhail Zaidi, Head -CII Centre for Digital Transformation were the two speakers during the Webinar. For those of you who were not able to attend the webinar, we bring to you a list of 25 To Do's that you must follow as you Work From Home.

Points to Ponder:

1. Before installing any app on the mobile, check the rating and read the reviews as there are many look-alike / duplicate apps available.
2. Install an app called LOOKOUT on the phone to check whether your phone has been compromised. This app can also trace your phone in case it is lost / stolen.
3. VOIP calls (Voice Over Internet Protocol) (i.e. calls made from a phone using a data network like JIO) can be spoofed by a hacker so that the calling number may show as that of your boss / friend and called number as your own. The caller may ask you to transfer money / share passwords etc. You should disconnect the VOIP call immediately and then call your boss / friend on a regular call from your mobile on the number listed in your contacts. It is prudent to inform all employees that in case they receive a VOIP call from you, then to immediately disconnect and call you on your mobile to reconfirm that it was actually the boss who had called.

4. In case any CCTV cameras have been installed, then to regularly change the password as otherwise a hacker can remotely monitor your office / home.

5. If you are using Gmail, then go to settings and change the password access to have a 2-factor authentication. i.e. give your mobile number as a secondary verification detail. In case of any doubt, Google will send you send an OTP (one time password) to verify that it is really you who is trying to access the Gmail account. Hence in case your password is known to the hacker, he will not be able to access the Gmail account without the OTP.

6. For office employees, have a 'hardening' policy. This means that you must inform employees in advance about which apps / programs that they can install on their office laptops / office mobiles. *All other software and apps should NOT be allowed to be downloaded on office laptops / mobiles as such software may have vulnerabilities that hackers can exploit. E.g.* - during the lock down, it has been noticed that there is a 40% increase in installing of apps for games. Many apps / programs are NOT secure and may compromise your device and even more important it may compromise the office data.

7. Do NOT give SMS access to any app on your mobile. Check the access that has been given to every app on your phone and disable SMS access to any app. In case there is access to the phone's SMS, then the app can have access to the OTPs that you get on your mobile and this can be used to empty your bank account or misuse your credit card.

8. For offices, the latest is to use 'Desktop in Cloud' concept. This is where all data is saved / accessed through the cloud. This can be configured so that any third party cannot access or download the files saved by you in your Cloud account. This protects your data even if the laptop is stolen / lost. No important data is saved on the laptop.

9. Be careful when taking selfies – ensure that laptop monitor with sensitive info is not part of the background.

10. Any credit card / debit card can be used on a foreign ecommerce site **WITHOUT the OPT**. Hence never allow anyone to photograph both sides of your debit / credit card.

11. **ZOOM**:

    a. The free version of Zoom stores all the data on a server in China.

    b. The paid version has an option where you can de-select the servers where you do NOT want the data to be saved – so you should de-select the Chinese server.

12. How do you decide which software is safe to use? Type the name of the software. followed by CVE – e.g. 'Zoom CVE' in the browser or go to www.cvedetails.com. This

will give all the data for any software that you want to install which includes list of vulnerabilities.

13. When using Zoom app, take care of the following parameters:

a. Have a unique password / username ID for each meeting. This is to prevent hackers from targeting meetings through a username which has been used before.

b. Enable 'Waiting Room' feature. This enables host to approve anyone who wants to join the meeting.

c. Disable 'Join before host'

d. Allow 'screen sharing by host only'

e. Disable 'Allow removed participants to re-join'

f. Restricting / disabling file transfer option (if required)

g. Locking a meeting

h. Switch off Alexa during official meetings

i. Put mike on mute

j. Put a tape on the webcam if you do not want to show yourself

k. Also do not allow participants to chat with one another

14. On laptops, many applications keep on running even when not in use.

a. Press Ctrl + Alt + Del

b. Go to Task Manager

c. Go to Details (arrow at bottom of screen)

d. Go to Start Tab and disable unused applications by right clicking

15. Never forward sites / links that you have not checked or are not sure of, as clicking on these links could help hackers to exploit device of others

16. Beware of fake e-commerce sites selling masks / sanitizers or whatever is in high demand at that time. These are all fake and you lose all the money that you have paid as advance.

17. Preferable to select 'cash on delivery' when ordering from such unknown sites.

18. Be very careful when making payments by clicking on links. E.g. the link pmcare@sbi.com is a fraud site. The correct site is pmcares@sbi.com .

19. Deactivate all debit and credit cards not in current use and re-activate them when you need to use them. This facility is available through net banking.

20. Use VERACRYPT to encrypt files and USB drives. So, in case you lose a CD with data or USB drive, then it gets very difficult to decrypt the data. This is a free service available on the net.

21. Never use Facebook password to access other applications. If Facebook gets hacked, then all your other applications can get hacked too.

22. Very often we receive links as Tinyurl (a shortened form of the actual link which is long). From the tinyurl we cannot make out any details about the actual site. You can use Google – 'unshorten tinyurl' or 'tinyurl expansion' to get the full version of the link.

23. Any site which is https// is OK. The 's' refers to it being a secure site

24. Dangerous and crazy things are happening on the internet. To find out check out 'www.thehiddenwiki.org', 'https://thehiddenwiki.com'. Do not use same device to play games, stream content from vague sites as what you use for financial transactions. This is to prevent your device from getting hacked through game apps or when you connect to vague sites.

25. Passwords can be cracked by a hacker using a technique called 'brute force hacking'. This software (available even from the net) will try each and every combination of possible passwords. Your modem can be accessible by others around your home / office. Hence it is advisable to change passwords every 2 months. Also have the habit of switching off the modem when not in use so that a hacker does not have unlimited access to your Wi-Fi signal.

Compiled By: Asit Adalja, IPA NEC Member