Cyber Crime Education: Prevention is Better than Cure

Summarised by
Prof. Arun C Mehta

Is no one spare?

In the present day, with lots of new technologies coming every day, do not think that anyone using a mobile phone/computer has any option but to avoid the untoward situation and loss by taking basic preventive measures. Though the cybercrime and nature of the crime that is taking place in society have affected most senior citizens, non-tech-savvy people must be extra cautious.

Loss of Personal Information may cost heavily

A careless attitude may result in loss of information which can be misused by criminals who always look for the opportunity to attack. Once a person is trapped may lose his personal information, money, and reputation in society, extortion through blackmail, and even become a part of the cyber-crime.

Once the criminal has access to vital information, s/he can even influence an individual to do something wrong and indulge in a crime, often even without knowing. In the process, many times, not only was the victim at a loss, but many times his friends and family members were also affected and met loss. There are instances where individuals' personal and business data are stolen and shared with competitors, resulting in heavy business loss.

Given the above, it seems that a small amount of carelessness may affect an individual and his/her family members heavily and cause loss.

Who is vulnerable?

In the prevention process, it is essential to know what is vulnerable. Practically everything that an individual is indulged in day-to-day life may be his mobile number, FaceBook and Instagram accounts, photos that he/she shares through social media including Whatsapp, chat, messages, email, online bank account, using online payments (Paytm), internet browsing, internet calling and even a call on mobile phone, etc. nothing is invulnerable.

This gives us the feeling that old paper-pencil days were more secure. The present-day full of advanced technologies can also be secure but with a small additional caution and prevention.

Can cybercrime be prevented?

Yes, taking a few preventive measures ensures that cybercrime/attack can be prevented, but one has to be vigilant at all or most of the time. Mobile phone plays a vital role through which most cyber crimes take place. Can we stop using mobile phones? No, these days, it is not possible.

Then what is the solution? How can we safeguard our data? It is in our own hands; we need to change our habits and be extra cautious on mobile and the internet.

Where do cyber-criminal get data?

From where do cybercriminals get data? Who provides the personal data? The answer is simple; we only provide data through irresponsible and casual behavior. Cybercriminals apply different tactics to different people to access personal data. Some people get phishing emails, and others get lucrative offers and freebies. Mind it; nothing is accessible for free on the internet; even a free Mobile App is not free, which also collects individual personal data and sells it for profit. So be extra cautious when downloading a new Mobile App or when next you get lucrative offers through email.

Never do?

- Never click a link/URL from an unknown source or receive it through email, as phishing is one of the most preferred methods of cyber attacks.
    - Better to avoid purchasing data packages from different sources, which may allow cybercriminals to get access to personal data accidentally.
    - Do not download Mobile apps from little-known or unknown platforms.
    - Never note down passwords in a diary or notepad.
    - Take extra caution in using private internet networks.
    - Never share passwords/patterns with technicians; if shared, they must be changed quickly.
    - Extra care must be taken in choosing passwords, do not set 'guessable passwords' (like name, date of birth, 12345, etc.). Always use special characters, such as @, #, and $ %, in the password, which is difficult to crake, but nothing is impossible for hackers. Make the password lengthy, which even you can not remember.
    - Avoid or minimize sharing pictures/photos on social media. Make it a habit not to post pictures on social media.
    - Avoid sharing information more than required as it can lead to cybercrime. It is advisable to minimize personal data on social media platforms.

Always do

- Delete recorded conversations on the mobile device at regular intervals so that personal information is not shared with unknown persons or stolen.
- Sofar possible, do not leave your mobile phone at the repair shop; it is still better to wait then and there.
- So far as possible, never leave your Hard Disk Drive at the repair shop to prevent untoward situations that may cause money loss.
- Always avoid opening and installing a private mobile application.

- Never entertain a call from an unknown person on a Mobile number dedicated to online banking and other financial purposes. If affordable, better to use a separate mobile instrument for both mobile numbers.
- Keep WiFi off when not in use. Do not forget to change the password of the WiFi Router once in three months.
- Do not share Internet/WiFi passwords with anyone. Note down the time and date you have given internet access to someone.
- Keep location sharing/GPS off on each application you use on Android or iOS phones.
- So far as possible, do not save passwords on mobile or laptop/computer; better to save all passwords in a password-protected Pendrive
- Clean the computer now and then, and delete browser history, cookies, and site data often.
- With the help of a Computer Expert, encrypt any data you store on the hard disk, as it can prevent lost or stolen data.
- Banks and platforms like Google have a provision for two-factor authentication, which can minimize lost or stolen data.
- Make it a habit to share data offline through Pen Drives.
- Use good anti-virus software for both mobile and desktop/laptop computers.
- If one can afford it, keep two mobile SIMs, one exclusively for internet banking and another for the rest of use. The second Mobile number can be used for applications like Paytm. Like Mobile SIM, keep an alternative email Id also.
- So far as possible, use the internet browsers in incognito mode; none of your browsing history, cookies and site data, or information entered in forms are saved on the device or to a Google Account you're not signed into.
- Make it a habit to clean your computer by deleting old files which have not been used for long.
- Always do not opt for data storage on the cloud, especially when you first configure a new device.
- Always keep the Bluetooth off when not in use.
- Always keep your computer and mobile device up to date, which can prevent malware from infecting your system/device.
- In case you have lost your phone or it is stolen, immediately contact your bank customer care and stop all services linked to the stolen phone number
- For the Aadhaar-enabled Payment/Debit System that allows the merchant to accept payment from a bank customer by authenticating the customer's biometrics, lock AeDS by visiting the official website of the Unique Identification Authority of India.

***Never forget that nothing is free available on the internet. Do not be access greedy*.**

Have a pleasant surfing, and be safe.

In case of a Cyberattack, Call the helpline number 1930