Quick Tips to Protect Yourself from Cybersecurity Threats

- No “it will not happen to me” thoughts: No hackers limit their operation just to the secret or crucial information. Certain data which the general user does not consider to be that crucial might catch the eye of a hacker. To tackle this threat, it is essential that every individual considers their device to have crucial data and keep it secure.

- Password management: Even though longer passwords are a bit difficult to remember, their complexity and length make the task of cracking these passwords a lot more difficult. As it is known to all, hacking the password of any account gives the hacker complete control over the account. There are a few guidelines related to setting up passwords which we are going to discuss. It is always considered safe to have a password of length varying between 15 and 20 characters. It is advisable that the password must contain a unique alphanumeric combination of upper case and lower-case letters along with special characters. It is advisable that no two accounts over the Internet should have same or even similar passwords. It is also a wise practice to change the passwords of all the accounts including the ones of the personal devices periodically and take care that the passwords are not repeated.

- Leaving devices unlocked: Leaving your mobile device or computer unattended is yet another common mistake which most end users end up committing unintentionally. Whether you are at a friend’s place or a cafe, whether you need to attend an important call, or you need to go to the washroom quick, the first thing you need to do before leaving your device is locking it.

- Always use secure network connection: Avoid doing crucial transactions over a public network. Any network other than your home or work network is an insecure network. Even though the data over your device is encrypted, it is not necessary that the connected network transfers the data in an encrypted format. Moreover, there is a constant risk that the public network you connect with may be tapped thereby proving a risk to the data being exchanged over the network. Before using any connection other than trusted networks, always make sure that you secure the connection using appropriate VPN settings.

- Beware of phishing websites and use internet cautiously: Always be aware of identity theft. Not always will hacker approach you or your system to get crucial data from you. Many times, it is just your personal information which they are interested in. This information then comes in handy while creating alias accounts and identities which are then utilized for hacking. Apart from identity theft, yet another thing which is sought after and can be stolen without your notice is the IP address of your web devices. This cannot just be used to track your location but can also be used as an alternate device ID when the hackers invade other crucial systems. The major part of the solution set to this problem includes steering clear from websites and pop-ups which demand your personal information. Also, avoid clicking links to the phishing websites which can be identified by their general randomness. Identity theft, not just limited to the Internet. The end users must also be aware of the unexpected and unknown phone calls relating themselves to different lotteries and contests and thereby gather crucial personal information from you.

- No pirated and cracked software: Avoid usage of pirated and cracked software. Although these software’s are meant to be used unrestricted without the need to purchase the software from the manufacturer, they come with their own set of issues. No hacker would develop a crack for any software unless there is any hidden intention and gain behind it. The cracked versions of software’s do contain some malware in them and this malware may either affect the performance of your device or even leak out crucial device information such as your IP address. The malware also possesses a risk of affecting the system files of your device thereby corrupting your device data. Moreover, using a pirated software for professional purposes also poses a risk of legal actions over your firm and thereby cost you much higher than the software license itself.

- Always keep your devices protected with antivirus: An antivirus gives you optimum protection against potential malware and bugs. Even though antivirus programs claim they provide optimum malware protection, it is imperative to keep the virus database regularly updated for it to function efficiently. Just like other paid software's, there are cracked versions of antivirus as well. As discussed earlier in the article, you must steer clear from such free wares. Always remember to not click on the pop-ups claiming a virus attack on your PC while browsing. That is not how your antivirus program operates, and such click pages are certain links to phishing websites.

- Always keep your software bundle updated: Updating antivirus database is not just the key to a healthy system. It is essential to keep the operating system as well as the third-party software's well updated. The system and software updates not just contain performance optimizations but also a few security related updates which not just protect the software but also the user data related to the application as well as related antivirus patches.

- Always keep your firewall active: Every computer is protected by a firewall. This firewall controls the flow of data over any network. It is the preliminary protection offered by any operating system. Though firewall is the most secure feature in data protection is used, it is a bit cumbersome process to use a firewall. Many times, a few applications are denied access through the firewall, and hence, it cannot be used all time. With the development in the field of information and technology, many loopholes in the firewall have developed. Hence, these days third-party firewalls provided mainly by the antivirus developing companies are used. The firewalls not only provide optimum data transfer security but also give the users a high level of customization for ease of use.

- Keep your sensitive data stored away from any device in a secure storage: Even though your device has an antivirus, is password protected, is connected to a secure data connection or protected by a firewall, it is always a wise move to keep your critical device data secure. The best practice to secure sensitive data is to securely remove the data from the device and store it over a protected external storage device. It is advisable that the storage device is not just password protected but is also protected by encryption layers. Along with encryption of external storage, it is also advisable to encrypt the device data and make sure it is duly encrypted during transfer.