How to Survive the COVID Time Cyber Security Threats?
At a time when the world has transformed due to COVID, the cybercriminals found it as an opportunity for exploitation. In addition to the existing attacks, new types of frauds are now spotted in the cyber world.

Almost all the companies, educational institutions, and government functions have gone online today and have created a void of opportunities for such scams. Some firms with robust governance and related processes may be prepared to handle the new work conditions and their associated external security threats. But it is not same with others, who are still lagging in their maturity in information security controls. Millions of new users, including children and adults, who previously had no access to the Internet, have now entered into the field and potentially could be an easy target to these cyber-attacks and frauds.
So, What’s New?

Even if all forms of the scam are on the rise, the spam emails and other messages associated with “COVID” should be taken care of. Fraudsters send out false messages pretending as messages from governments or health centers. It is either intended to spread computer viruses, to collect personal or bank-related information, or to conduct financial fraud. Similarly, fraudulent emails that ask to donate to COVID patients and related organizations are rampant.

Experts have found that registration of domains using COVID-related names has increased tremendously. Fraudulent owners of such websites continue to attract victims to gather information from them and conduct financial fraud. There have been a lot of frauds associated with the sale of masks and sanitizer, COVID treatment, and donations etc.

Some of the more serious cyber crimes are now on the rise in the form of blackmailing. There has been an increase in these kinds of campaigns, in particular using fake profiles to carry out sextortion using recorded naked videos of victims.

The security threats to institutions have reached different levels during this period. Just as workers cannot avoid using company information and services at home, they also pose new security threats. "Phishing" email messages, information breaches, and cyberattacks can affect organizations’ security standing.

In the past, If the attackers used bulk email spam (SPAMS) messages to target any random victims more targeted attacks are seen in the recent past. The criminals leverage the information available in the cyber world, including social media. Today, cybercriminals are taking advantage of the victims through offers of banks and big companies, employers, and lotteries, etc. Scams involving recent events and news items have appeared as emails and posts on social media.
10 Common Sense Tips to Remember for protection!

1. Always handle cyber-related matters with caution and alertness.
2. If someone is forcing us to act or respond urgently and without giving any time to think, then always there is a chance of cheating or fraud. Be Smart!
3. Limit sharing of personal information with others, especially with strangers and on public forums.
4. Before accepting connection requests, study the profiles and posts to verify whether they are fake, fraudsters or antisocial ones.
5. Remember that nothing comes free. If someone reaches out to you with offers, that are too good to be true, be careful.
6. Ideally, we should try to find our weakness, where the attackers could be targeting. Necessary precautions around that will ensure that we don’t fail into the related traps.
7. Be very careful when clicking on any website links, downloading software or responding to emails.
8. Enable at least 2-factor authentication for online sites and applications.
9. Understand the privacy conditions and settings and action on it according to your requirements.
## How to Protect Your Mobile Devices?

<table>
<thead>
<tr>
<th>Right</th>
<th>Keep the phone updated to the latest Operating System version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review the privacy settings of the phone and the applications installed to limit the exposure of your personal data</td>
</tr>
<tr>
<td></td>
<td>Review and limit the automatic renewal of the subscriptions and other payment settings with credit card numbers on the phone.</td>
</tr>
<tr>
<td></td>
<td>Always ensure the camera, microphone and other accessory settings, so that your privacy is not compromised. Close/disable it, if not being used.</td>
</tr>
<tr>
<td></td>
<td>Review the settings of Whatsapp and other chat software, so that 2-factor authentication and other security features are enabled, to avoid hijacking it from other devices.</td>
</tr>
</tbody>
</table>

1. **Right**
   - Configure your devices with a screen lock - Facial Recognition, PIN code, pattern, or fingerprint.
   - Install the programs, with limited privileges on your devices and also understand its operation and access.
   - Ensure that adequate protection is enabled for your mobile device so that even if you lose it, the data does not fall into the wrong hands. If it is iPhone/iOS, you can enable find your phone, remote wiping etc.
   - Install security software to protect the device from malicious codes and applications.
   - When you are giving the phone for repair or donating it to others, ensure that the data is completely wiped off, after backing it up in your devices.
How to save your money in banks? Seven ways?

Securing money in a bank is one of the most pressing issues of the day. Cyber threats and criminal gangs have brought us to a point where we have to look for the security of our money and other information, even if the security threats are deliberate. Every day, there are many losses and miseries due to reasons that the banks have not taken appropriate steps to protect their technology environment.
Check your bank account regularly

Avoid sharing bank details to anyone

Use strong passwords for online banking accounts

Ensure to make written complaints

Ensure account is safe and secure

Keep printed statements as back-up

Avoid using public computers for banking activities

Banking with those banks who are generally found to be more serious on security and have demonstrated their commitments and efforts on safeguarding the customer information and investment

“Avoid using public computers for banking activities, as there could be many kinds of security vulnerabilities in those, where even your credentials can get stored in the system.”