ADVISORY ON CORONAVIRUS PANDEMIC CYBER FRAUDS

Attackers are using various methods to exploit the fear and need for information related to Coronavirus amongst people around the world. Some of the common methods used by threat actors to target people and carry out frauds are as follows:-

a) Sending Fake Malicious Documents (such as Health Advisories, COVID-19 Response Documents, e-books, etc.) in the name of reputable and trusted sources (like Government, World Health Organization, etc.).

b) Creating Fake Malicious Websites/Apps related to Coronavirus (such as Coronavirus Maps, Real-Time Coronavirus tracking apps, Corona Antivirus, etc.).

c) Running spam campaigns of selling masks, sanitizers, Coronavirus vaccines, etc. on online shopping portals exploiting the fear of Coronavirus among people.

d) Fake online Sales offering premium goods at unbelievable prices in the name of "Corona Special Offer".

e) Sending threatening emails and messages (such as extortion emails threatening to infect the family with Coronavirus) related to Coronavirus.

f) Various nation-state threat groups have also become active and carrying out spear-phishing campaigns targeting government officials.

g) Spreading of fake news related to Coronavirus to create panic amongst people. Such misinformation is being spread via platforms like WhatsApp, Telegram, etc.

SUGGESTIONS:-

1. Use only trusted sources, such as legitimate government websites for up-to-date, fact-based information about COVID-19.
2. Never respond to unsolicited requests for personal and/or financial information (even if conducted via phone or in person).
3. Download Mobile Apps only from the official App Store and avoid granting any unnecessary permissions.
4. Verify the authenticity of the charity campaigns related to COVID-19 prior to making any contributions.

5. Exercise extreme precaution before opening any email attachments or clicking any links received from unknown senders (especially in relation to Health Information or having the theme of Coronavirus). Be aware of phishing and take every possible precaution to avoid falling for scams.
6. Organizations should ensure that secure Access Technologies are in place and configured correctly, including the use of multifactor authentication, so that all employees can conduct their work securely from home.
7. Individuals should avoid using personal devices for work and ensure that personal devices have same level of security as a company-owned device. Also, take care of the Data Privace and Security of any sensitive information while doing Work from Homes.
8. Be cautious of the offers and discounts given in the name of Coronavirus and ensure that you are only ordering goods from authentic sources instead of going through the promotional links received in mails or messages.
9. Make sure that the devices have latest security updates installed and also have good antivirus or anti-malware solutions.

****