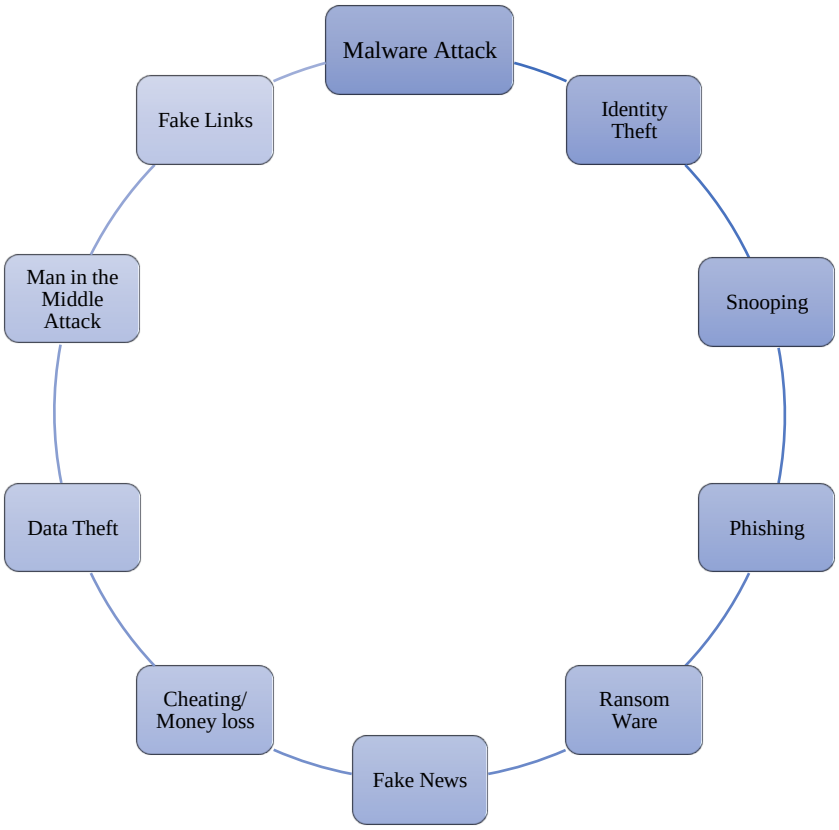
Cyber-CrimesDuringCovid 19 -Work from Home Scenario & Best Practices for Online Safety

By Dr. Karnika Seth, renownedCyberlaw Expert &Member, FICCI Homeland Security Committee.

Corona virus has impacted the world in an unprecedented manner putting health and safety of several people in great dangerduring past few months. This has led to several countries announcing a complete or partial lockdown whereby billions of people are advised to stay home and work from home. Cybercriminals have exploited this precarious situation and anxious mindset of people to commit social engineering attacks on them and phishing frauds. The Ministry of Home affairs, Govt of Indiahas reported a steep rise as high as 86% in cybercrimes over the past four weeks. The modus operandi of criminals predominantly has been to use trojans, keyloggers, other malware sent through infected links, attachments via mails or social media posts to commit phishing and ransomware attacks. Several fake posts selling testing kits, vaccines for Covid 19 and fake donation sites have been found floating on the social media platforms and Internet to dupe gullible people. With a view to educate society at large, FICCI conducted a Webinar delivered by the author herein on being vigilant about fake apps, sites, links, donation sites and adopt best practices for online safety in Work From Home scenario. Criminals are misusing the vulnerabilities and security loopholes in popular videoconference systems and news reports point out that applications such as Zoom are facing security issues.

Reliable sources have pointed out that in past few weeks registration of domain names using keyword ‘Covid’ has grown exponentially, out of which 50% registered are being operated for fraudulent purposes. This is not limited to fake websites.In one of the cases registered by Delhi Police, a fraudster created a fake UPI ID ‘pmcare@sbi’ for the PM Care Relief Fund while the correct ID is ‘pmcares@sbi’.Many phishing websites have been traced and blocked by concerned law enforcement authorities. Criminals are luring potential victims to download infected files through sending suspicious emails and links like 'Deadly Corona Virus Map' that is designed to steal a person’s critical information such as user names, passwords and credit card numbers. As a user tries to navigate through the map to learn the spread of Corona Virus, a malware identified as AZORult is activated which is an information stealer.



Rising cybercrimes during Covid times

Cyber terms – ready reckoner

Malware Attackis an attack where criminal uses a virus, worms or Trojans to send infected links or attachments to potential targets to damage a device or system or take control of an electronic device like computer, mobiles.

Identity Theft is stealing a person's identity by spoofing for fraudulent purposes.

Snooping attack is an unauthorized interception of a video or audio conference which is invasion of privacy and is criminal if done malafidely.

Phishing is a financial crime where the criminal sends fake email or messages to a person to authenticate an accountinformation and thereby extracts the password details or sensitive financial data to cause unauthorized debits to one's account.

Ransomware attack is a kind of extortion attack which prevents a device user from opening the files or applications on the attacked device.

Data Theft or Hacking means dishonestly or fraudulently accessing a person's data or system to steal data, introduce a virus, destroy a computer system etc.

Man in the Middle Attack is where the attacker spoofs a genuine email address and manages to defraud recipient of mail to pay moneys into a fake bank account instead of genuine email address holder's account.

The currentIndian Cyberlawsframework& cybercrimes

Although the Personal data Protection bill,2018 is not yet enacted, the Information Technology Act,2000 has several provisions that deal with cybercrimes and prescribes punishments therefor. For example, unauthorised access, downloading or extraction of data is punishable under Section 66 of IT Act and provides punishment of upto three years and fine or both. If a cybercriminal garbs a fake identity and steals financial data of a person through social engineering /phishing mails, the person could be guilty of Section 66C r/w 66D, and Section 420 of IPC.A person who hacks a system or device or video conference would be guilty of crime committed under Section 66 of IT Act,2000.

Section 66C prescribes similar term of punishment for identity theft and Section 66D of IT Act,2000 provides punishment for cheating by personation. The fake donation sites will attract this provision along with Section 420 of IPC for cheating.

Further, the Indian Penal code,1860 provides punishment for committing acts that create disharmony, public unrest, and provoking riots, hurting religious sentiments of a community under Section 153A, 295A of IPC punishable with imprisonment of upto three years and fine. Spreading of fake news that may invoke riots or create public disharmony or hurt religious sentiments of a community would also attract this Section.

It is pertinent to point out that the National portal https://cybercrime.gov.in/provides facility to register FIR online.Also, National Emergency helpline is 121 to report any emergency including cybercrimes.

Best Practices for Online safety in WFH times

The importance of keeping safe digitallyapart fromone's physical health cannot be understated especially in Covid times. In order to be digitally secure, it is essential for businesses to adopt the following best practices in WFH scenario-

- Prepareation of a work from home policy/ IT policy
- Use secure Wifi using WPA2/WPA3 technology
- Turn off WiFiand Bluetooth when not using it
- Use VPN for office work as far as possible
- Use Data loss Prevention Software, if possible
- Use strong antivirus and antispyware
- Update OS Software
- Use digital signatures to sign e-contracts and send emails

- Regularly backup the important data
- Impart security awareness trainings to employees
- Use only authentic applications after checking source
- Beware of the fake news/fake links/apps/ads
- Download AarogyaSetuapp and visit the official news handles to check the news such and updates on Covid 19 as PIB, news portals, news paper websites
- For Advisories check the Ministry websites for the Ministry of Home Affairs, Ministry of Health and Family welfare, Ministry of Information Technology. Read the advisories issued by CERT-In for cyber security measures here.
- Use secure and paid videoconference platforms.
- Read the terms and conditions and check source before you subscribe to a service.
- Use two factor authentications for accessing a service
- Donot share personal financial information with anyone over phone/mail/sms
- Use a reliable password manager service.
- Pay only on https websites
- DSCI has also issued best practices for Work from Home to secure the network while allowing remote access to employees.
- You can register a criminal complaint online at cybercrime.gov.in
- National helpline no. is 121.
- Type the address of a bank in URL address bar to access netbanking
- In case of phishing fraud-Preserve screenshots of evidence, report it to Bank immediately if account/ plastic card data gets compromised
- Block credit cards /debit cards and lodge police complaint in acse of any unauthorised debits.

It is important to stay home and stay safe in Covidtimes,and one's digital safety is equally necessary Cybercriminals are misusing the heightened anxiety levels among people to operate phishing rackets and make illegal gains. Adoption of online safety practices will be instrumental in not only curbing the rising cybercrimes but will aid in stoppingfake news. Businesses, their crucial data and employees will be safeguarded from unauthorized intrusions and data loss by maintaining digital hygiene. Crucial data of organizations and people will be protected from hacking/phishing/malware attacks. Adopting little prudence and best practices to online safety will go a long way in averting prevalent threats and risks

and support business resilience and continuity plans of any given organisation. Stay Home, Stay Safe and happy Surfing & WFH!

For any queries, you may write to karnika@sethassociates.com

About the author-

Dr. Karnika Seth is an internationally renowned Cyberlawyer, IP & Media Laws expert, practicing in the Supreme Court of India and High Court of Delhi. She is an accomplished Author, Policymaker, and Educator on Cyberlaws. Dr. Seth is the Founder of Seth Associates, an established law firm based in Delhi, that renders legal services to both domestic and global clients for more than two decades.