COVID-19 frauds and scams: How to protect yourself

COVID-19 has created previously unthinkable consequences for our society. Organised crime has been quick to respond, mounting large scale orchestrated campaigns to defraud banking customers, preying on fear and anxiety related to COVID-19. In these uncertain and difficult times, fraudsters opportunistically prey on the fear and uncertainty created by a public health emergency, looking to profit from the public's desire to regain a sense of safety and security.

Across the world, we have seen an increasing rise in scams associated with COVID-19. Computer and phone hackers are trying their best to take advantage of the pandemic to lure potential victims to download infected files through suspicious links. Criminals are misusing high-volume searches and curiosity related to the virus on the internet. They have made malicious programmes which are hidden in files related to coronavirus.

Also, as governments prepare large stimulus packages in response to the pandemic and begin providing fiscal support to their citizens, the risk of being defrauded by COVID-19 related scams will likely continue to rise.

For a few sectors such as financial services, pharmaceuticals and life sciences and telecom, in particular, there are many challenges. These sectors have already begun to provide an unprecedented response and working through their own business continuity issues. Demand is far outstripping supply as concerned customers inundate call centres, as fraud typologies change on an almost hourly basis.

Some current and potential COVID-19 related scams include:

Technology-driven scams

Misrepresentation by sales channels

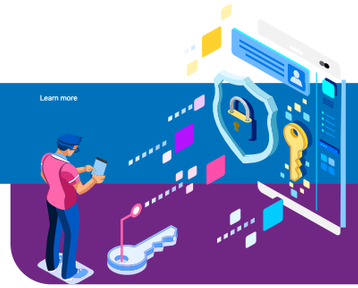
Investment and charity

What can you do to protect yourself?

Awareness

Preventive technology controls

Detective and investigative control



Some current and potential COVID-19 related scams include:

Technology-driven scams

01

Phishing scams: Imposters claiming to be members of reputed domestic and international health authorities, such as the US Centre for Disease Control and Prevention (CDC) or the World Health Organisation (WHO), target victims with emails including malicious attachments, links, or redirects to 'updates' regarding the spread of COVID-19, new containment measures, maps of the outbreak or ways to protect their victims from exposure. Once opened, such attachments or links infect the computer/phone device with malware or expose sensitive personal data, credit card, etc., and this can transmit the data to the hacker

02

COVID-19 fraudulent websites: There has already been a significant rise in new fraud risk typologies, particularly relating to the registration of large numbers of "COVID" internet domains. These fake websites look like genuine websites of the organisation but carry the malware to infect the computers/phone devices

03

Business email compromise: The increase in remote working, accompanied with organisation-wide updates regarding COVID-19, has opened the avenue for fraudsters to target businesses and their employees. Using emails disguised as COVID-19 updates, fraudsters attempt to trick employees to hand over their credentials by requesting they login to a fake company's "COVID-19" portal. Once an employee has entered their credentials, the fraudster can have unfettered access to the employee's organisation's business accounts and network

04

Ransomware attacks: Government institutions and commercial organisations are seeing a new spike in ransomware attacks. In this type of attack, the critical servers and end points are first compromised and then encrypted. Ransomware attack locks the operating system and end-user files rendering them un-accessible until some ransom is paid (usually through bitcoins) to the attacker. As remote access to computers is becoming a norm for "work from home" due to the government-imposed curfews/self-imposed lockdowns, we expect a spike in ransomware attacks to cripple the organisations' IT infrastructure to collect the ransom

05

Other mobile app scams: Fraudsters are developing or manipulating mobile phone applications which outwardly look as if they track the spread of COVID-19. However, once installed the application infects the user's device with malware which can be used to obtain personal information, sensitive data, or bank account/card details.

Some current and potential COVID-19 related scams include:

Misrepresentation by sales channels

01

Online education applications: As schools and higher educational institutions are closed, parents are increasingly subscribing to various online educational technology applications for self-learning, and fraudsters are also proactive in their activities. They connect with their victims, pretending to be a representative of known education applications, and offer substantial discounts for registering at the link messaged by them

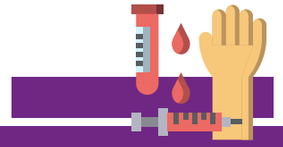
02

Supply scams: Taking advantage of current supply shortages and public desperation for resources, fraudsters have established fake online shops that sell medical supplies currently in demand, such as surgical masks and hand sanitisers. After payment is made to "purchase" the goods, fraudsters pocket the money and never deliver the supplies

03

Ounterfeit drugs: Due to the perceived difference between demand and supply of essential drugs, there is a high possibility of counterfeit drugs being stuffed in the supply chain in chemist/pharmacies and possibly even online marketplace. The general public usually cannot spot the difference between genuine and potentially fake products easily, hence the chances of them falling prey to such schemes are high

04



Covid-19 testing and treatment scams: Rising panic around contracting the coronavirus has created flocks of individuals looking for a way to prevent themselves from getting sick, get themselves tested without coming to government's notice (to avoid being subjected to government quarantine facilities, and staying away from family members, etc.) as well as to get treatment for COVID-19. Using social media and online forums, fraudsters may promote bogus testing kits, treatment products, etc. claiming to prevent and cure the infection. These include promise of vaccines, fake cures, and unproven treatment methods

05

Healthcare provider scams: Fraudsters may pose as doctors, nurses, paramedics, hospital administrators, etc. claiming to have successfully treated a known friend or relative from COVID-19 and luring their victim-patients in exchange of payment for the said treatment.

Some current and potential COVID-19 related scams include:

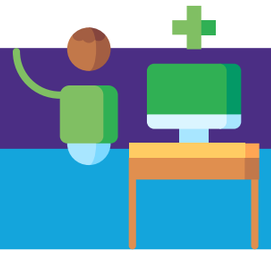
Investment and charity

01

Charity scams: In times of crisis, it is not uncommon for individuals to feel a personal sense of responsibility to help reduce the impact on the community and poor. Fraudsters prey on this desire, soliciting donations for non-existent charities claiming to help individuals, groups, or areas affected by the virus, or contribute towards the development of a vaccine to fight the virus

02

Investment scams: Keeping with the tradition of a classic investment scam, this scam has a twist, purporting to generate significant returns from investing in a company that has services or products that can prevent, detect or cure COVID-19



What can you do to protect yourself?

Awareness

There are many ways to help protect yourself, your loved ones, and your business from falling victim to COVID-19 scams. Paramount to reducing vulnerability is ensuring that people remain aware of how criminals are attempting to take advantage of the global health crisis.

01

Be wary of fraudulent emails claiming to be from experts who have vital information regarding the virus. Do not click links or open attachments from unknown or unverified senders and check email addresses from sources claiming to have information regarding COVID-19 for irregularities, such as spelling errors or miscellaneous symbols. Fraudsters often use addresses that only have a marginal difference to those belonging to the entities they are impersonating

02

Be careful of fake online shops which use non-traditional payment methods, such as money orders, funds transfer, gift cards, or cryptocurrency. Don't use any payment shortcuts given by a representative. Log in to official website to make any payment

03

Check the background before donating to any charities or crowd-funding campaigns. Be wary of any business, charity, or individual soliciting donations in cash, through the mail, via funds transfer or other unusual channels

04

Stay informed of investment scams and trends in relation to COVID-19 – e.g., schemes offering discount on products like online content streaming, companies who claim to have drugs curing COVID-19. Ensure that you buy drugs from authorised chemists or known sellers only. Even in such cases, it is imperative that you check product details including labels, packaging, ingredients, date of manufacture/expiry and location of manufacture

05

Avoid sharing pictures of home-desk/workstation on social media as you may inadvertently share confidential information. Always be mindful of what you share on social media.

What can you do to protect yourself?

Preventive technology controls

01

Protect and control remote access to critical IT infrastructure, restrict access on user-ids (internal/ external). Revoke all direct connects on your servers from outside office premises. Monitor server and network performance and set alerts

02

Limit and log the use of applications which give remote access, enforce forced password resets and build two factor authentications on critical IT assets

03

Ensure the anti-malware, anti-ransomware and anti-virus software installed on devices is up to date. Operating system patches are always updated. Avoid installation of freeware on IT systems as they may have hidden malware/trojans

04

Connect to internet using secure WiFi hotspots and broadband connections. It is highly recommended to connect to the internet using a virtual private network

05

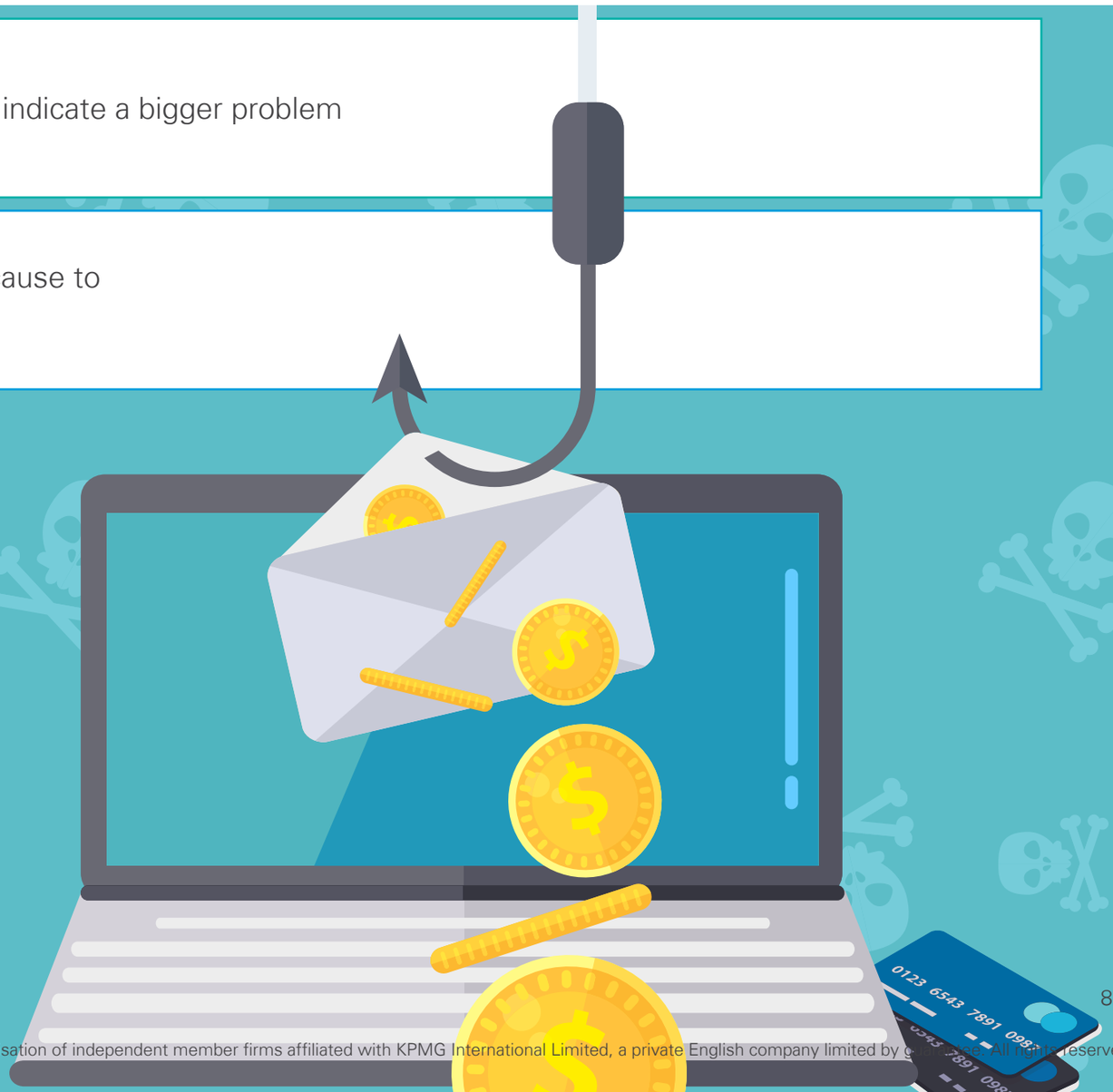
Avoid using public file sharing website unless authorised by your organisation’s policy.

What can you do to protect yourself?

Detective and investigative control

01 Do not dismiss any breaches or incidents as they may indicate a bigger problem

02 In case of a cyberattack, investigate the root cause to secure and prevent against further attacks.



KPMG in India contacts:

Vijay Chawla
Partner and Head
Risk Advisory
T: +91 80 6833 5509
E: vschawla@kpmg.com

Jagvinder S. Brar
Partner and Head Forensic Services
T: +91 124 336 9469
E: jsbrar@kpmg.com

Suveer Khanna
Partner
Forensic Services
T: +91 22 3090 2540
E: skhanna@kpmg.com

Manoj Khanna
Partner
Forensic Services
T: +91 80 6833 5519
E: manojkhanna@kpmg.com

Sudesh Anand Shetty
Partner
Forensic Services
T: +91 22 6134 9703
E: sashetty@kpmg.com

Mustafa Surka
Partner
Forensic Services
T: +91 22 6134 9313
E: mustafasurka@kpmg.com

Tanmay Bhargav
Partner
Forensic Services
T: +91 90040 18599
E: tanmayb@kpmg.com

Sidhartha Gautam
Partner
Forensic Services
T: +91 98991 83331
E: sidhartha@kpmg.com

home.kpmg.com/in

#KPMG josh

Follow us on:
home.kpmg.com/in/socialmedia