KPMG

COVID-19 Beware of frauds & scams

March 2020

COVID-19 has created previously unthinkable consequences for our society. Organized 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 this 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 increase in scams associated with COVID-19, and it is expected that figures are starting to climb. Victims are typically targeted via phone, email and social media.

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

For the financial sector in particular there are great challenges. The industry has already begun to provide an unprecedented response, but is busy with their own business continuity issues. Demand is far outstripping supply as concerned customers inundate call centers, as fraud typologies change on an almost hourly basis.

Management's focus is on limiting the impact of Corona on the daily business routines. As a result, little to no time is allocated to monitor relevant key risks. This leads to blindness for weak spots in business processes. Over the last couple of days, large and smaller companies have instructed their employees to work from home. This creates a number of opportunities for increased fraud risks, such as:

- Deviation from checks and controls normally included in the process. Normal procedures and checks on possible breaches of regular control frameworks are interrupted. This becomes even more of a risk if there is an ongoing internal restructuring of processes or temporary capacity problems.
- Increased caution is required regarding the already proven effective methodology of "CEO fraud". More meetings and agreements will be handled by phone and email. This means that these can easily be manipulated, as we learnt from cases in the past.

Some COVID-19 related scams include:

- **Phishing scams:** Fraudsters posing as members of domestic and international health authorities, such as the United States Centre for Disease Control and Prevention (CDC) or the World Health Organization (WHO), targeting 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 yourself from exposure. Once opened, the computer may be infected with malware or expose sensitive personal information or credit card details saved online to a hacker.
- **COVID-19 fraudulent websites:** There has already been a significant rise in new fraud risk typologies, in particular related to the registration of large numbers of "COVID" internet domains.
- **Compromised business email:** The increase in remote working, accompanied with organization-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 their login to a faked company "COVID-19" portal. Once an employee has entered their credentials, the fraudster has unfettered access to the employee's company accounts and the organization's network.

- **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 sanitizer. After payment is made to "purchase" the goods, fraudsters pocket the money and never deliver the supplies.

- **Treatment scams:** Rising panic around contracting the novel coronavirus has created swaths of individuals looking for a way to prevent or cure COVID-19. Using social media and online forums, fraudsters promote bogus products that claim to prevent the virus and lure victims with the promise of vaccines, fake cures, and unproven treatment methods.

- **Provider scams:** Fraudsters are posing as doctors or hospital administrators, typically claiming to have successfully treated a known friend or relative for COVID-19 and demanding payment for said treatment.

- **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. 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.

- **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.

- **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.

There are many ways to help protect yourself, 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.

So what can you do to protect yourself?

- 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.

- 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.

- Be careful of fake online shops which use non-traditional payment methods, such as money orders, funds transfer, gift cards, or crypto-currency.

- Conduct background research 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 fund transfers or other unusual channels.

- Ensure that the anti-malware and anti-virus software installed on your devices is up-to-date.

- Stay informed of scams trends in relation to COVID-19.

Services

https://home.kpmg/ch/de/home/dienstleistungen/advisory/forensic.html
https://home.kpmg/ch/en/home/industries/financial-services-hub/regulatory-and-compliance.html

Contacts

KPMG AG
Räffelstrasse 28
Postfach
CH-8036 Zurich

kpmg.ch

Anne van Heerden
Partner,
Head of Forensic

+41 58 249 28 61
annevanheerden@kpmg.com

Philippe Fleury
Partner,
Financial Services

+41 58 249 37 53
pfleury@kpmg.com