COVID-19: A Breeding ground for Fraud?

May 18, 2020

Powered by SkX Protiviti
Fraud Risk Management: Sizakele Bophela
Risk Management: Wayne Poggenpoel

Introduction

The coronavirus outbreak is first and foremost a human tragedy, affecting hundreds of thousands of people. The World Health Organization declared this outbreak as a pandemic and a public health emergency. The warning bells are ringing!! From regulators, law enforcement agencies and consumer organisations around the globe, the message is clear: Fraudulent schemes related to the coronavirus have arrived and fraud is surely an inevitable symptom of the COVID-19 pandemic

> **Stay home. Wash your hands. Don't click that link. As the coronavirus pandemic continues to sweep across the globe, people have yet another thing to worry about: Fraudsters.**

Frauds and Scams in the wake of COVID-19

During a crisis, people and businesses tend to let their guard down on normal routines because they are worried about how to keep their doors open. The combination of financial and health threats make people more vulnerable and create opportunities for fraudsters to take advantage. Unfortunately, it seems that COVID-19 is a perfect storm for fraudsters because people are driven typically by greed and financial hardship and motivated by opportunity.

Below is a list of the current and potential COVID-19 related scams that are likely to affect individuals and businesses alike:

- **Phishing and Smishing Scams:** Due to COVID-19, phishing and smishing scams have increased whereby fraudsters are claiming to be members of reputed health organisations and financial relief organisations. They are targeting the public with e-mails and SMS messages which have malicious attachments/links regarding the spread of the virus, maps of the outbreak and ways to protect potential victims from exposure. As soon as the link has been accessed, such attachments or links can infect the mobile devices and computers with malware and transmit personal and confidential data to the hackers.

- **Investment Scams:** Investment scams claiming significant returns from investing in a company that is developing services or products that can prevent and cure COVID-19 are also likely to arise. These fraudulent companies may coerce investors to also consider investing in shares of companies that develop protective personal equipment, promising larger than normal returns.

- **COVID-19 Fraudulent Websites:** According to multiple reports, cyber criminals are now creating thousands of coronavirus-related websites daily. Thousands of new domains containing "COVID-19" have been registered and are being used maliciously. The main aim of these websites is to ask the public to donate towards certain charities and to also illegally acquire the personal banking information of donors.

- **Supply Chain Scams:** Taking advantage of the current supply shortage, fraudsters have established fake online shops that supply sanitisers, gloves, surgical masks and also non-existent COVID-19 equipment that claim to prevent and cure COVID-19. After the payment is made, the fraudsters pocket the money and never supply these commodities to the public. Also on the rise for companies, the need for emergency spend has risen and this has made procurement processes vulnerable to abuse. Furthermore, the procurement process has also become vulnerable to collusive behaviour between employees and suppliers.

- **False Charity:** In times of crisis, people feel a sense of responsibility to donate to the underprivileged. Fraudsters are now preying on this desire and have created fraudulent charities by claiming to help individuals who are affected by the virus.

- **Superannuation/Retirement Schemes Fraud:** Most of the expected COVID-19 related superannuation scams will involve an e-mail, SMS or phone call from someone impersonating a representative of an official organisation, such as a superannuation company, the Government or a financial institution, etc. These scams predominantly target the elderly and those close to retirement.

- **Employee Fraud:** In the current situation, every company is looking for savings and one of the immediate measures is to cut jobs or reduce payments to employees. As experience has shown, for some employees this may create an incentive to commit fraud. The employees who are working from home are also likely to spend a considerable amount of "work time" on non-employer related activities.

- **Misappropriation of Assets/Resources:** Coupled with employee fraud and the realisation of compromised/weakened controls, the assets of companies are subject to misappropriation and abuse. These include mobile devices and other resources allocated to allow employees to be accessible and to be able to do their jobs. Employers need to ensure that their asset registers are updated regularly.

There are useful government sites which provide updates on COVID-19 scams with methods changing and emerging daily. In Australia, one such site is the "Coronavirus (COVID-19) scams" on the Australian Competition & Consumer Commission (ACCC) website Scamwatch page. Another example of a global site, is the information updates from the U.S. Federal Bureau of Investigation (FBI).

How to Practice Good Fraud Hygiene? (And, please wash your hands)

Below are some of the best practices to assist you in ensuring that you do not become a victim:

• Never donate to charities via links in e-mails; instead, donate via the charity's website. Follow fundraising platforms' guidance on how to recognise and report fraudulent charities.

• Hover your mouse over a link to determine if it is genuine. Don't click it if it looks suspicious.

• Never respond to any e-mail that asks for personal or sensitive information.

• Be careful of any suspicious/phishing e-mail requesting policy renewals/premium payments.

• Be wary of e-mails from popular health organisations like the WHO. Visit their official website for the latest advice. The only call for donations the WHO has issued is the COVID-19 Solidarity Response Fund. Any other appeal for funding or donations that appears to be from the WHO is a scam.

• Don't panic in case of warning/threatening e-mails. Read carefully and then act.

• Use different passwords for different sites and don't provide personal information in pop-ups.

• Encrypt special files and data and avoid opening unexpected attachments.

• Keep your system updated with patches and antivirus software.

• Be aware of fake online shops which use non-traditional payment methods such as money orders, fund transfers, gift cards, etc. Don't use any shortcuts to make payments. If you need to make a payment, log onto official banking websites to make the payments.

• Stay informed of the scams and trends in relation to COVID-19, such as, investment scams, schemes offering discounts on products, companies who claim to provide drugs that prevent COVID-19, etc.

In times like this, it becomes easy for cyber criminals to entice and create panic amongst unsuspecting users by inviting them to click links and attachments via e-mails and messages. All you need is to be alert and vigilant when dealing with such e-mails to avoid cyber-attacks/fraud.

Cybersecurity and Privacy Considerations for the Remote Work Environment

As the coronavirus continues to spread, many companies have shifted to remote working practices to keep employees safe during the pandemic. As a consequence, this has placed unanticipated stress on remote networking technologies in addition to bandwidth and security concerns. The majority of organisations are not experienced with such a rapid culture shift, therefore, they should continually monitor access to prevent any potential security vulnerabilities.

Further to this, there is a need for organisations to consider the following risks before employees are given the option to work remotely:

• **Unsafe Wi-Fi Networks:** Employees may be connecting to a home wireless network or accessing corporate accounts using an unsecured public/personal Wi-Fi, thereby allowing the fraudsters nearby the ability to easily penetrate and monitor the connection and steal confidential information.

• **Personal Devices for Work:** There exists a reality of employees transferring files between work and personal computers when working from home. Therefore, IT departments need to be completely aware of issues that may arise whilst employees are using their personal devices for work-related matters. Additionally, not keeping the software up-to-date could allow security weaknesses within the IT environment.

• **Ignoring Physical Security:** Physical security is important when it comes to a company's sensitive information. As remote working provides for an increased risk of data leakage, a reminder must be provided to employees not to expose or allow business data to be compromised. Companies must also ensure that secure and appropriate IT controls are in place for data protection.

Best Practices for Remote Working

The coronavirus crisis has accelerated digitisation and has further reinforced the trend towards working from home. Below are some of the best practices when working from home during the COVID-19 pandemic:

• **Communication is the Key:** A standard communication schedule is very important to keep remote teams together despite being physically distanced. Regular team meetings provide an opportunity for team members to connect personally and share their experiences. Employees working remotely can use various communication mediums such as Microsoft Teams, Zoom or WebEx video conferencing platforms for better collaboration. They must also use common secure platforms to manage projects and documents with their co-workers and clients.

• **Close the Loop:** It is a best practice to follow up after every call with a summary of the information covered, decisions agreed upon in the call, and accountability and ownership for next steps. This helps to confirm that even in a dispersed work-from-home environment, everyone left the call with the same understanding.

• **Identify a Dedicated Workspace (and Time):** A dedicated workspace is a key aspect of working from home. You can replicate your office environment by keeping aside a dedicated area that feels like your

professional zone. You should also position your workspace in such a way that you can concentrate and have the resources you need. As organisations embrace remote working arrangements, the lines between personal and professional time can blur. It is very important to understand and respect the working hours of others while allowing for flexibility wherever needed.

• **Plan Ahead (As much as you can!):** It can become easy to fall into the trap of excessive short-term thinking during a crisis. Therefore, it's good to schedule some time with yourself to map out your week, month, and/or quarter ahead. What's coming up? While nobody knows just how long this COVID-19 situation will last, doing as much long-term planning as possible will indeed be beneficial.

While an unprecedented event like COVID-19, as a global pandemic, has made "work from home" the new normal, organisations should leverage trust, flexibility, focus, transparency, empathy and technology as the tools to enable effective remote collaboration. These practices and tips can be useful for setting up a successful work arrangement and together we can face the future with confidence.

How SkX Protiviti can help?

SkX Protiviti's Forensic consultants assist organisations in building a solid infrastructure for evaluating, mitigating, investigating, reporting and monitoring their risk of fraud, corruption and misconduct.

Understanding organisational vulnerabilities and establishing an appropriate framework to identify and respond to these fraud risks are essential factors in today's global marketplace. This is also perpetuated by the fact that regulators are demanding more active management and robust investigation for a wide range of risks, including financial crime, fraud and corruption.

Our Forensic professionals also assist organisations with building sustainable anti-corruption, investigative and fraud risk assessment processes as well as in the development of anti-fraud, anti-corruption and investigative programmes and controls to meet fiduciary and regulatory responsibilities. SkX Protiviti further supports organisations in their efforts to identify, triage/diagnose, investigate, report and monitor a wide array of other risks at every level — from the performance of risk assessments, programme design or remediation, risk governance, and employee training to audit anti-corruption, fraud, and investigation programmes and processes.

Our team's unique blend of anti-corruption, fraud risk management and investigative subject-matter expertise allows for a quick response to the identification of programme shortcomings and remediation of the critically important programmes. We also have extensive experience in undertaking investigations of suspected violations of those programmes by leveraging investigative, forensic accounting and technology disciplines across our global footprint to provide our clients with the experience and local resources necessary to gather the facts to make informed business decisions.

For more information contact:

Wayne Poggenpoel
Risk Management Lead

Sizakele Bophela
Fraud Risk Management Lead

Head Office-Gauteng
Building 1, 15 Forest Road
Waverley Office Park, Bramley
Tel: +27 (011) 797 6800

Kwazulu Natal
Suite 1A, 100 Armstrong Avenue
La Lucia Ridge, Durban, 4051
Tel: +27 (031) 562 1700