protiviti®
Face the Future with Confidence

COVID-19: A breeding ground for fraud?

April 13, 2020

The coronavirus outbreak is first and foremost a human tragedy, affecting millions of people. The World Health Organisation has 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.

Frauds and scams in the wake of COVID-19

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

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

Below is a list of the current and potential COVID-19 scams:

- **Phishing scams:** Due to COVID-19, phishing scams have increased whereby fraudsters are claiming to be members of reputed health organisations and are targeting the public with emails including malicious attachments, links regarding the spread of the virus, maps of the outbreak and ways to protect the victims from the exposure. Once opened, such attachments or links can infect the computer with malware and transmit data to the hacker.
- **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 likely to arise.
- **COVID-19 fraudulent websites:** According to multiple reports, cybercriminals are now creating and sending out thousands of coronavirus-related websites on a daily basis. Thousands of new domains containing COVID-19 have been registered and are being used maliciously.
- **Supply 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.
- **False charity:** In times of crisis, people feel a sense of responsibility to donate to the underprivileged and fraudsters prey on this desire and may create fraudulent charities by claiming to help individuals who are affected by the virus, or contribute towards the development of a vaccine.
- **Superannuation fraud:** Most of the expected COVID-19 related superannuation scams will involve an email, 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 will predominately target the elderly and those close to retirement but also those who they have already obtained an identity (identity theft).

- **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.

There are useful government sites which provide updates on COVID-19 scams with methods changing and emerging daily. In Australia, one such site is currently the 'Coronavirus (COVID-19) scams' on the Australian Competition & Consumer Commission (ACCC) website scamwatch page.

An 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 prevent you from becoming an unsuspecting victim:

- Never donate to charities via links in emails; instead, give at 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 if it looks suspicious.
- Never respond to any email that asks for personal or sensitive information.
- Be careful of any suspicious/phishing email requesting policy renewals/premium payments.
- Be wary of emails from popular health organisations like WHO. Visit their official website for the latest advice. The only call for donations WHO has issued is the COVID-19 Solidarity Response Fund. Any other appeal for funding or donations that appears to be from WHO is a scam.
- Don't panic in case of warning/threatening emails. 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.
- 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 the payments. Log into official websites to make the payments.
- Stay informed of the investment scams and trends in elation to COVID-19, such as, schemes offering discounts on products, companies who claim to provide drugs that prevent COVID-19.

In times like this, it becomes easy for cyber criminals to entice and create panic among unsuspecting users by inviting them to click links and attachments via emails and messages. All you need is awareness and alertness while dealingwith such emails to avoid cyber-attacks/frauds.

Cybersecurity & privacy considerations for remote work environment

As the coronavirus spreads, most 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, 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 is a possibility of employees transferring files between work and personal computers when working from home. 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 provide 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. Daily 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 working hours of others while allowing for flexibility wherever needed.
- **Plan ahead (as much as you can!):** It can become easy for employees 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 Protiviti can help

Protiviti's Forensic consultants help organisations build 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 them are essential in today's global marketplace, as regulators are demanding more active management and investigation for a wide range of risks, including financial crime, fraud, and corruption.

Our Forensic professionals assist organisations with building sustainable anti-corruption, investigative and fraud risk assessment processes and developing anti-fraud, anti-corruption and investigative programs and controls to meet fiduciary and regulatory responsibilities. We support organisations in their efforts to identify, triage, investigate, report and monitor a wide array of risks at every level — from the performance of risk assessments, program design or remediation, risk governance, and employee training to audits of anti- corruption, fraud, and investigation programs and processes.

Our team's unique blend of anti-corruption, fraud risk management and investigative subject-matter expertise can quickly identify program shortcomings and remediate your critically important programs. We also have extensive experience in undertaking investigations of suspected violations of those programs 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.

Contacts

Anthony Hodgkinson
Director, Protiviti
+61.418.123.564
anthony.hodgkinson@protiviti.com.au

Adam Christou
Managing Director, Protiviti
+61.410.311.263
adam.christou@protiviti.com.au

protiviti®