

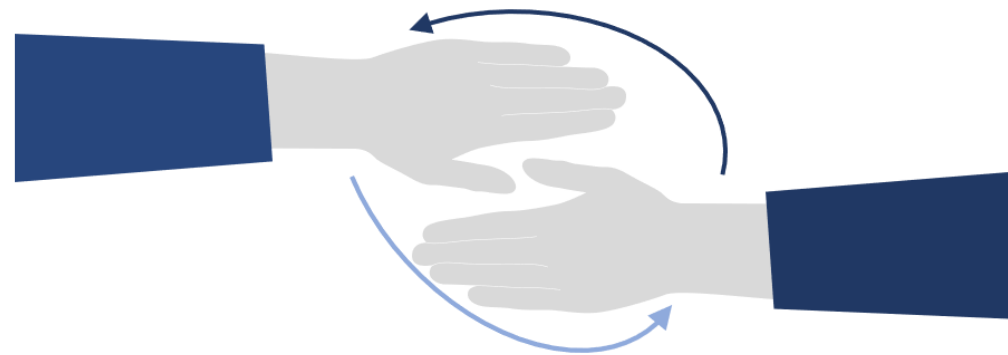


FINANCIAL INTELLIGENCE UNIT

COVID-19 and FRAUD



COVID-19 has greatly shifted the economic and social atmosphere of the world leaving unusual consequences for our nation. The negative social and economic impacts associated with the pandemic may lead to increased receptiveness of individuals, households, and businesses to donations and sudden windfalls. Fraudsters will try to use uncertainty to their advantage. Therefore, the Financial Intelligence Unit (FIU) would like to advise the general public to be aware of the increased risk of fraud during the current COVID-19 pandemic.



The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.

Pandemic Prevalent Frauds

Phishing Scam

Fraudsters pretend to be from financial institutions, utility companies, or government agencies that are providing information on COVID-19 via text messages and emails “phishing” for your information. These contain links and attachments designed to steal personal and financial information.

Online Shopping Scam

Fraudsters create fake online stores, claiming to sell products that do not exist, or pretend to be legitimate companies. In doing so, customers unknowingly grant fraudsters access to their personal and credit information which can result in loss of funds from unknown purchases conducted on the customers’ account.

Business-Targeted Scam

Fraudsters use COVID-19 as an opportunity to victimize businesses. They pretend to be a known business associate and submit fictitious invoices for payment. Payments are diverted to banks that are not the known banks of the business associate and instead go to the fraudsters.

The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.

Pandemic Prevalent Frauds

Mobile App

Fraudsters develop or manipulate mobile phone applications which seemingly appear as if they are tracking the spread of COVID-19.

However, once installed the applications infect the user's device with malware which can be used to obtain personal information, sensitive data, and bank account and credit card information.

Charity Scam

Fraudsters solicit donations for non-existent charities allegedly impacted by COVID-19. Some fraudsters also pretend to be representatives of legitimate charities. For example, Person A might receive a message from an individual via text, email or a private message on a social media application requesting donations be made to a personal account.

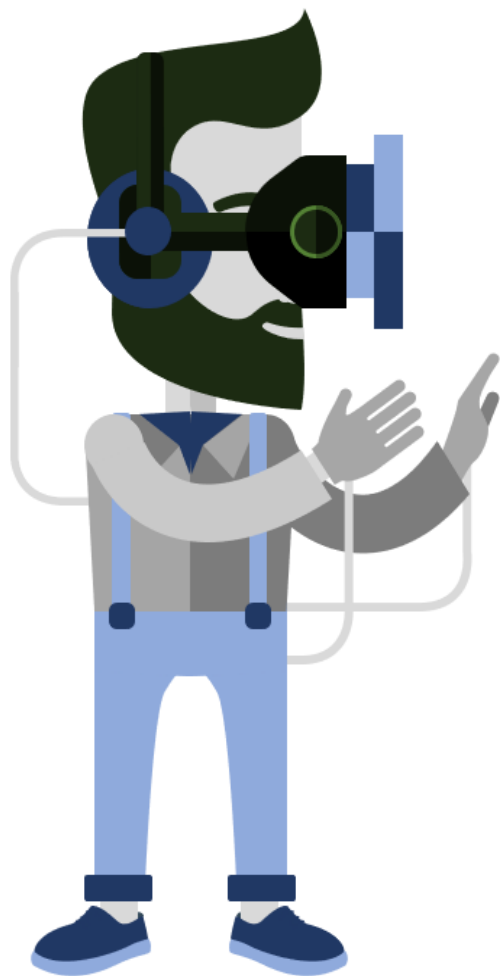
Ransomware Attack

As remote access to employers' networks is gradually becoming the new norm due to "work from home" orders this exposes networks to ransomware attacks that can cripple a workplace's IT infrastructure. These ransomware locks the operating systems and the workplace's files leaving them inaccessible until a ransom is paid.

The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.

Caution!

There are many ways to protect yourself and businesses from being victims of these COVID-19 scams. One way to reduce vulnerability is to remain alert of how criminals are attempting to take advantage of this pandemic.



Be wary of unsolicited emails.



Do not click on links or open attachments from unknown or unverified senders. Check email addresses from sources claiming to have information regarding COVID-19. Look for spelling errors or miscellaneous symbols in email addresses and in the body of the emails.



Be careful of fake online shops that use non-traditional payment methods, such as money orders, funds transfers, gift cards, or cryptocurrencies.

The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.



Caution!



Do background checks on entities or organizations before making charitable donations. Be wary of any business, charity, or individual who solicits donations in cash.



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



Secure e-mails and social media accounts with multi-factor authentication (for example, consider combining the use of password along with a security question).



Keep up to date with current advancements in finance, technology, and criminal activity. This will inform you of emerging security threats as well as measures to safeguard yourself.

Please report any transaction/activity involving fraud to the Financial Intelligence Unit.

The Financial Intelligence Unit (FIU) issues this Alert in accordance with section 7(1)(d) of the FIU Act, requiring the FIU to take such measures as may be necessary to counteract financial crimes.