FRAUDS AND SCAMS IN THE ERA OF COVID-19

A scam is a confidence game, swindle or other fraudulent scheme, especially for making a quick profit, while fraud is an intentional deception made to secure unfair or unlawful gain or to damage another person (Canada.ca, 2019).

Fraudsters have adapted to the conditions of COVID-19 and recognized areas of need created by the pandemic that they can exploit to scam vulnerable seniors. This blog post will go through some of the common frauds and scams that are happening with COVID-19, namely online shopping, phishing email, and investment scams, as well as what you can do to protect yourself.

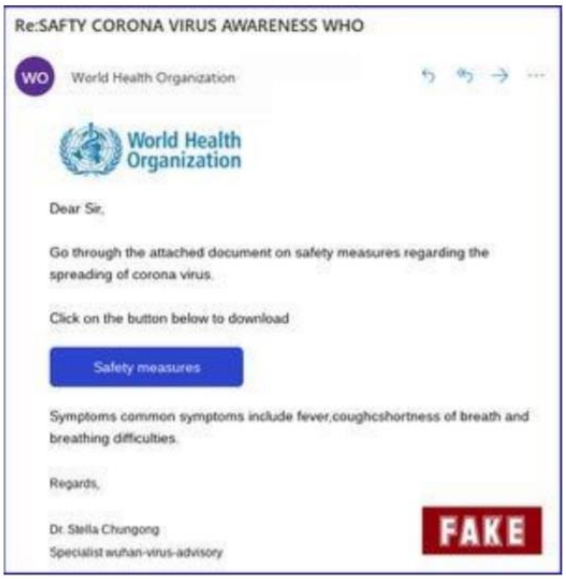
Online Shopping Scams

With the increase in online shopping, fraudsters have created false advertisements and posts on online marketplaces for personal protective equipment such as masks and gloves, as well as gym equipment, toys, and pets. These ads are also likely to mark goods at greatly reduced prices to attract online shoppers. Once a connection is made with the sellers, they may ask for payments and personal information but will never send you the promised goods, which are known as non-delivery scams. When you are online shopping or browsing through marketplaces, watch out for spelling mistakes, lack of customer reviews, and "too good to be true" deals that might indicate a non-delivery scam. It helps to have some knowledge of the market price of the item you are buying, which can be referenced with a quick Google search.

Phishing Emails

Another common type of scam is phishing emails, which are scams under the guise of employment opportunities, well-known charities asking for donations or offering free items like masks or hand sanitizers, health agencies alerting you to COVID-19 exposure and wanting your personal healthcare information, and many more. Below is an example of a phishing email that was made to appear like it is from a health agency. This email seems to be from the World Health Organization and requests the receiver to download safety instructions. At first sight, it

may seem authentic due to the sender information and World Health Organization logo, but a closer look reveals some suspicious errors, such as the misspelling of “safety” in the email subject line and other grammatical errors in the email body.



Despite the various types of phishing emails, they all have the goal of obtaining your personal and financial information. Therefore, **ask yourself first if the email you have received is familiar or expected prior to opening it, and if you open it and see that it has urgent, coercive or threatening messages, do NOT trust it or follow any links contained in the email.** For charities, the Canadian Revenue Agency has a list of registered charities and agencies with which you may verify any requests or claims you come across. It is always recommended to directly enter websites on your own using the search bar, rather than following links in emails that may have illegitimate origins.

Investment Scams

Investment scams are another type that will try to obtain your information, with common themes of investment scams being questionable investment opportunities, stock offers, and “get rich quick” opportunities. These types of scams may reach you through unsolicited emails or phone calls. For emails, they often start as spam emails promoting a risky investment with little information provided. Callers may present an investment opportunity and use high-pressure tactics such as repeated calls or limited-time offers to coerce you into making the transaction. Fraudsters may also try to gain your trust to reveal some information about yourself, and then target your insecurities to pressure you into making a deal. If you find yourself in this type of situation, know that you should never feel pressured to make a decision; if you do feel this way, it is likely a shady company or representative that you should no longer speak to. For

investments in general, you should always have plenty of time and information to come to your own well-informed decisions.

Protecting Yourself

So, with so many different types of scams out there, how do you protect yourself from fraudsters? Some rules of thumb to follow include:

- Not opening any unfamiliar or unsolicited emails and attachments
- Not following links included in unknown or suspicious emails
- Not giving out your personal and financial information
- When online shopping, verify your seller and look for customer reviews
- For calls, ask tough questions that fraudsters would not be able to answer
- If you received concerning notifications from companies or government agencies about your accounts, directly log into your accounts on your own to verify and do NOT follow any links provided from unverified or untrusted sources

For a more complete list of the types of frauds and scams as well as instructions on how to protect yourself, see our Seniors First article: Frauds and Scams Resource List. Links are provided to resource agencies and news articles. Additionally, images of real scam attempts are shown to better equip you to recognize scams.

REFERENCE LINKS:

Types of Fraud

Canadian Anti-Fraud Centre Bulletin: Non-Delivery Scams

Protect Yourself From COVID-19 Related Phishing Scams

Extortion Frauds

List of Charities and Other Qualified Donees

Investment Frauds

Protect Your Money: Avoiding Frauds and Scams

CONTRIBUTOR

Thank you to our volunteer Shu Min Yu for writing this blog!