Internet Fraud 1: “How to spot phishing scams arising from COVID-19”

1. This is an example of phishing.
2. The scams work by, scammers making emails look authentic from organizations such as, The World Health Organization, and asking for donations, or tricking the users into sending their personal information, or sending malicious links in these emails.
3. There are many ways to stop/prevent the fraud. Some of them are:

* **Be Vigilant** about the individual(s) that are sending you these emails
* **Be Skeptical**
* **Check the “from” Address** when you receive these emails
* **Never click on suspicious links or attachments**
* **Protect your devices**.

1. If you have been scammed, then the best things to do are the following: if you accidentally sent financial information to the scammer then inform your financial institution of the mishap that occurred, notify the police of what happened and give them a detailed explanation of everything that occurred between you and the scammer, as well as keeping an accurate record of everything that occurred.

Internet Fraud 2: “Protecting yourself from cheque fraud”

1. This is an example of, cheque fraud.
2. The scams can work in different ways. Some of the most common techniques that criminals employ are stealing cheques, creating fraudulent cheques, changing the name(s) of the cheque, and changing the amount that the cheque contains.
3. Some things that can be done to stop/prevent this type of fraud are:

* **keep your cheque in a secure location**
* **review your monthly bank statement to ensure that there is nothing that looks out-of-the-ordinary**
* **if you close your account ensure that you shred any unused cheques**
* **consider electronic payments as they are more secure than cheques**.

1. If you have been scammed, then the best things to do are the following: contact your financial institution as soon as possible, contact the police with evidence, and contact the organization that the cheque was issued from.

Internet Fraud 3: “Does this email look phishy? Check out examples of the latest scam emails”

1. This is an example of, a phishing scam, or more specifically, email fraud.
2. These scams work by, criminals attempting to fool individuals by sending them email messages that point at fake websites. Often, the emails that are sent to the victim look legitimate. However, when the user enters sensitive information such as their name, their address, and financial information, that data is given over to the criminals.
3. Some things that can be done to stop/prevent this type of fraud are: **be skeptical** (if you THINK that a bank has sent you an email that requires you to enter important financial information, then it is always good to communicate with a representative from a bank, to ensure that you are not getting scammed),

* **never enter important financial or personal information through email**
* **always enter your bank’s website through the URL that you know is correct**,
* **check the domain name** that the sender enters in the email to see if it matches up with the organization that they claim to be a part o. If it happens to be different, then block the user, delete the email, and report this activity to the police.
* **Make sure that your computer is protected**. There are advanced anti-malware, anti-spam, and anti-virus software. Therefore, always ensure that your computer is protected by buying or installing some of these popular software products.

1. If you have been scammed, then some things that you can do are: contact your financial institution if you entered your bank information, and report this activity to the police as well. In order to have a piece of evidence, save the email or screenshot it as evidence that you have been scammed.

Internet Fraud 4: “Threats and intimidation to pay your tax bill? How to spot the tax season scam”

1. This scam is known as a tax season scam, or a “CRA scam”.
2. The CRA scam is, when scammers dupe you into believing they are representatives of the Canada Revenue Agency. This type of scam has many different kinds of form including but not limited to: phone, email, and text messages.
3. Although, the emails, phone calls, and text messages can often look legitimate, there are red flags that make a CRA scam apparent. Therefore, some things that can be done to prevent this kind of scam are:

* **Does the call or voicemail make threats that you owe money to the CRA**
* **Does the email, call, or text message contain a sense of urgency that you owe money to the CRA, or a warning that they will contact the police**
* **Does the email or text ask you to click a link and make you enter personal information, so you can receive a refund or benefit payment**

1. If you have been the victim of a CRA scam, then some things that you can do are: contact the police and let them know your situation by providing sufficient evidence of the encounter that you had with the scammers, through whatever methods they scammed you. After that, contact your financial institution, if financial information was disclosed to the scammers, and ensure that there is enough evidence provided to support your claim.

Internet Fraud 5: “Learn how to protect yourself from credit card fraud”

1. This scam is known as a, credit card scam.
2. This kind of scam/fraud can work in several ways, with some of the most common ways being: your card could be lost or stolen, a criminal could obtain your card number and expiry date, or criminals could tamper with payment terminals at retailers to obtain your card information so they can create a counterfeit credit card.
3. In order to stop or prevent this type of fraud, there are many things that banks have been doing in their part which includes:

* **Having highly sophisticated security systems and teams of fraud experts in place** to monitor transaction, protect customers and to prevent or detect any type of credit card fraud.
* **Customers are protected when using credit cards that are issued by banks**, and are not responsible for any fraudulent transactions that are made on their cards.

At the same time, there are many things that credit card users can do to prevent this type of scam, and some of those things are:

* **Report a lost or stolen card as soon as you notice it is gone**
* **Never lend your card or give your PIN number to anyone**
* **Choose a PIN that can not be easily detected**, do not use your birth date or address
* **Make sure that you check your online account regularly**, and if you notice something that looks out of order then report it to your bank

1. If you have been scammed, then you should contact your credit card issuer (bank or financial institution) immediately using the number that they provide on the bank of your credit card. By doing so, the credit card issuer will take the appropriate steps to prevent you from fraud.