Scammers: Be Aware

Knowledge is the Best Safety

Top 5 Scams:

1. **Tech Support Scams:** “pop-ups” that appear on your computer screen and look like legitimate offers for computer service or help. In addition, criminals could get your telephone number and call to claim they are representing a reputable company such as Microsoft.
2. **Tax Scams:** The CRA will NEVER reach you by email or nor they call demanding payment.
3. **Ransomware:** Use up-to-date antivirus system. Also, never open spam emails from unknown senders, do not download attachments from spam or suspicious emails, and avoid clicking on links in suspicious emails to help avoid these types of scams.
4. **False debt collectors:** they come as official-looking documents and the tone of the emails is threatening and urgent.
5. **Sweepstakes scams:** a sweepstakes scam often will want you to pay to receive your prize.

PHISHING

PHISHING SCAMS are messages of phone calls made to look and sound like they're from people or companies your familiar with. In some cases, a cybercriminal may already know something about you to make the message or phone call sound more legitimate.

PHISHING

Phishing scams are messages or phone calls made to look and sound like they're from people or companies you're familiar with. In some cases, a cybercriminal may already know something about you to make the message or phone call sound more legitimate.

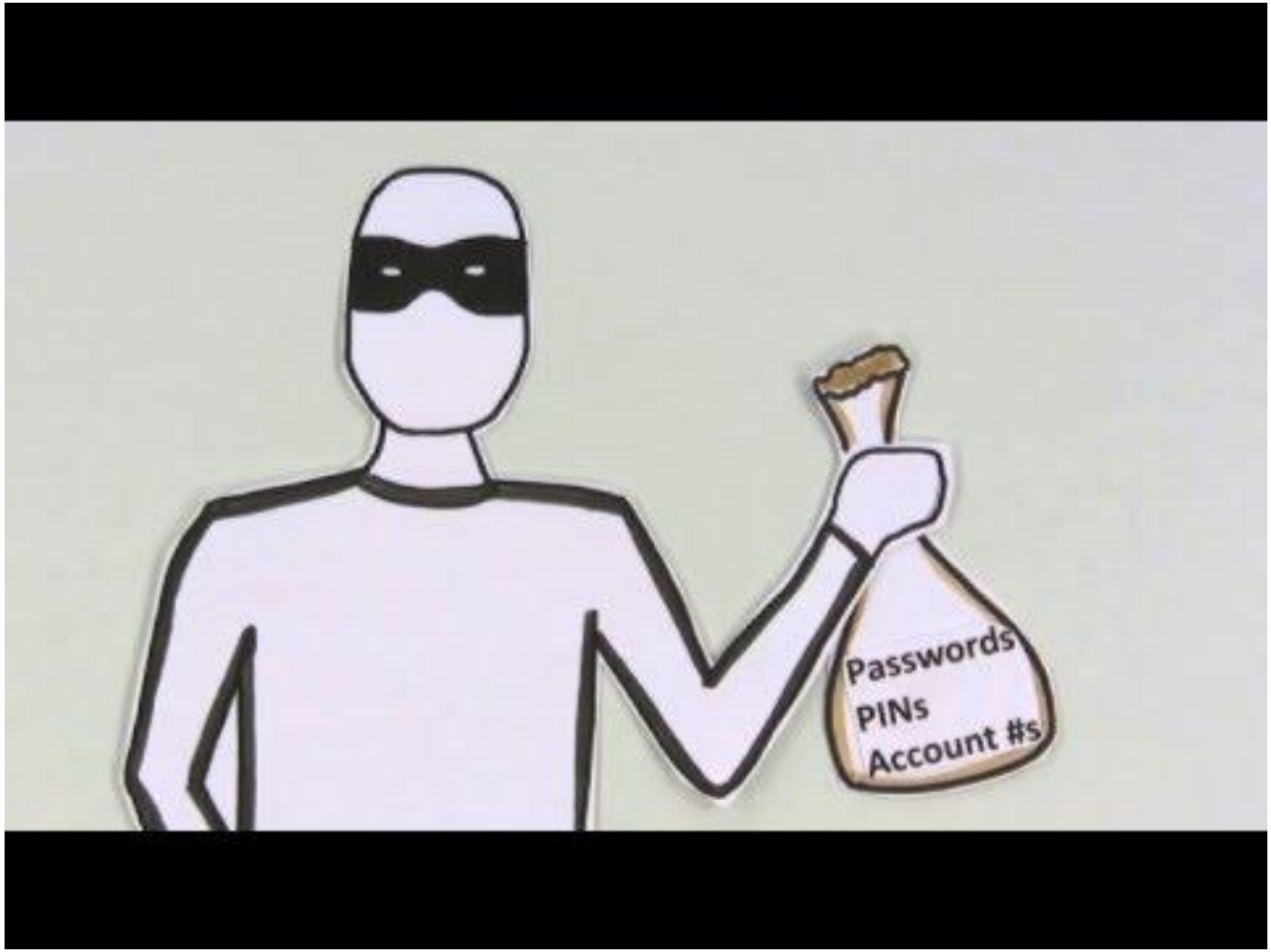
IF YOU RECEIVE A SUSPICIOUS EMAIL, PHONE CALL OR TEXT (EVEN IF IT SEEMS LIKE IT'S FROM A FAMILIAR COMPANY OR A FRIEND) HERE'S WHAT TO DO:

BREATHE. Phishing messages often pressure or threaten you to respond quickly. If an email needs you to "act now", it's probably a scam.

DON'T OPEN ANY LINKS OR ATTACHMENTS you're unsure of. Reach out to the sender in a different way, like by phone, to confirm.

CONSIDER YOUR INTERNET HISTORY. Unless you requested it, any message asking you to reset your password or update your account info is likely fake.

DELETE ANY MESSAGES THAT SEEM TOO GOOD TO BE TRUE, like winning a contest you didn't enter.


Passwords
PINs
Account #s

Look out for these scams: be aware

Covid-19 Online Scams:

- Fake health organizations
- Websites that sell fake products
  - Masks, hand sanitizer, disinfectant wipes, use know retailers
- Bogus government sources
- Fraudulent financial offers
- Fake nonprofit donation requests

Look out for these scams: be aware

Disaster Relief Scams:

- Scammers hide behind relief organizations
- Scammers will use tragedy or natural disasters to con you
- Thinking your helping your giving your financial informations to these frauds
- Use established and well known charities
- See **GuideStar** or **Charity Navigator**

Look out for these scams: be aware

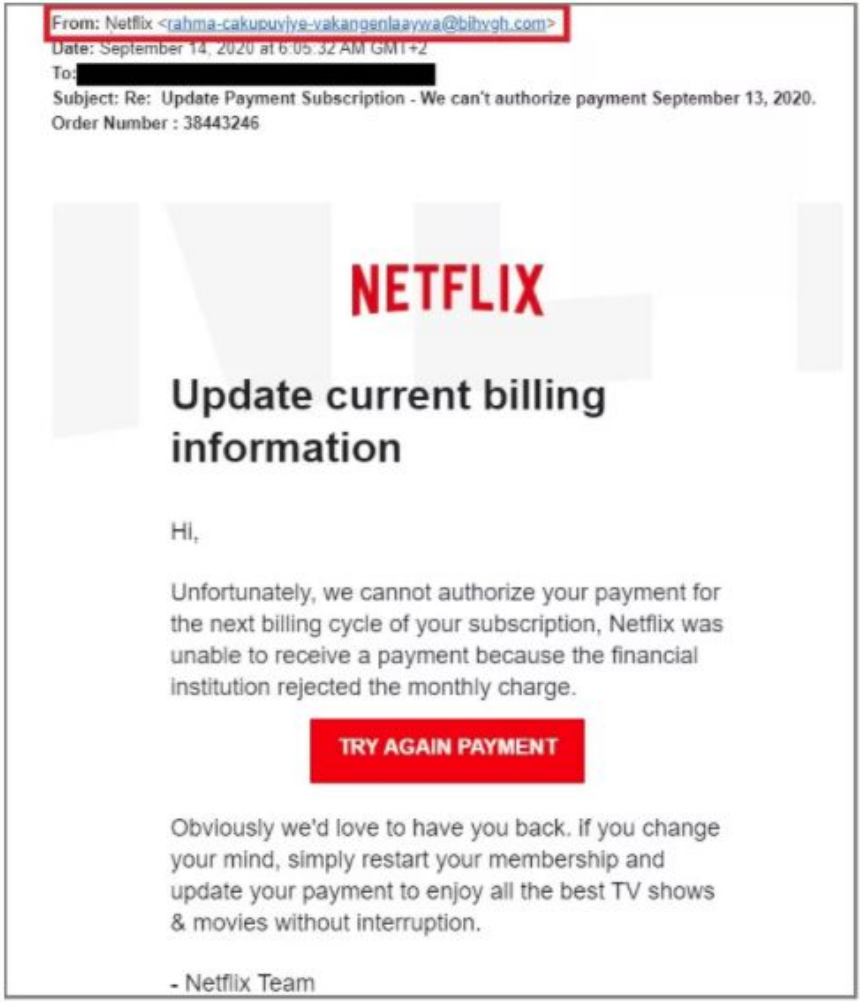
Phishing Scams:

- According to the FBI more that 114,700 people fell victim to phishing ($57.8 million)
- Never click the links provided in emails
- This makes you vulnerable to viruses and malware
- No reputable institution will ask for your passwords or other key information online
- Phishing emails will often contain typos or grammatical errors, and the sender's email address often looks suspicious
    - This is intentional to “weed out” people who would be unlikely to fall for a scam

Look out for these scams: be aware

Phishing Scams: Examples:

- Say they've noticed suspicious activity or log-in attempts on your account
- Claim there's a problem with your account or payment information
- Include a fake invoice
- Ask you to click on a link to make a payment
- Claim you're eligible to sign up for a government refund
- Offer a coupon for free goods or services



From: Netflix <rahma-cakupuvlye-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [redacted]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

Update current billing information

Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

TRY AGAIN PAYMENT

Obviously we'd love to have you back. If you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

- Netflix Team

Look out for these scams: be aware

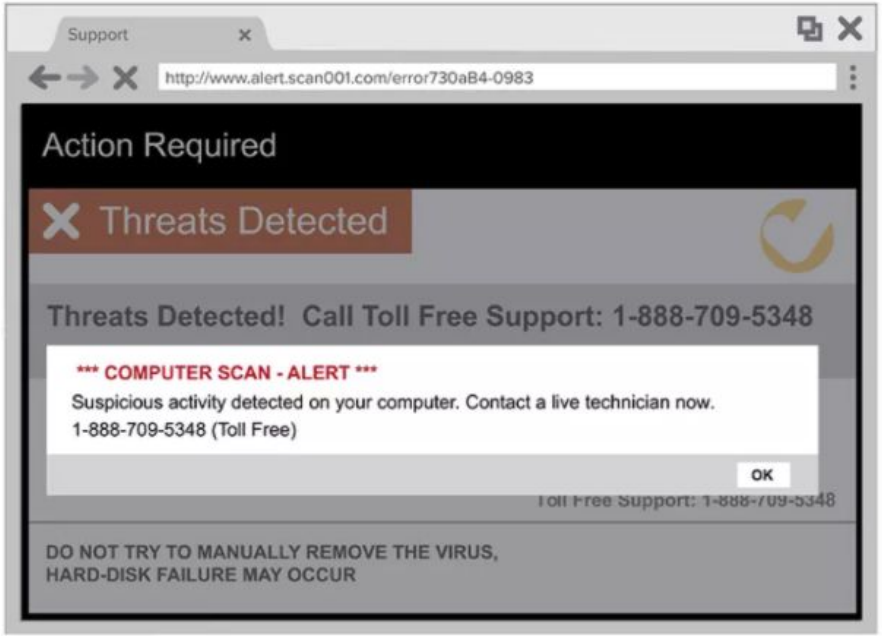
Fake Shopping Websites and Formjacking

- Use URL's similar to websites the are mimicking
  - Ie. "AmazOn.net
- Formjacking is another retail scam
  - A legitimate retail website is hacked
  - Customers are redirected to a fraudulent payment page
  - Your information then becomes available
  - Check that the payment page address is the sake as the website page

Look out for these scams: be aware

Tech Support Scams:

- You receive a contact stating your computer is infected
- They prompt you to:
  - Prompts you to download an application that allows them to control your computer
  - Downloads a virus to make you believe that there is something wrong
  - Tells you they can fix it for a fee



Look out for these scams: be aware

Other types of Scams:

- Travel Scams
- Grandparent Scams
- 419 Fraud -- Advance Fee Scam (Nigerian letter scam)
- Pre-Approved Notice
- Debt-Relief and Credit-Repair Scams
- Lottery Scam
- Fake Check or Money Transfer
- The Bottom Line