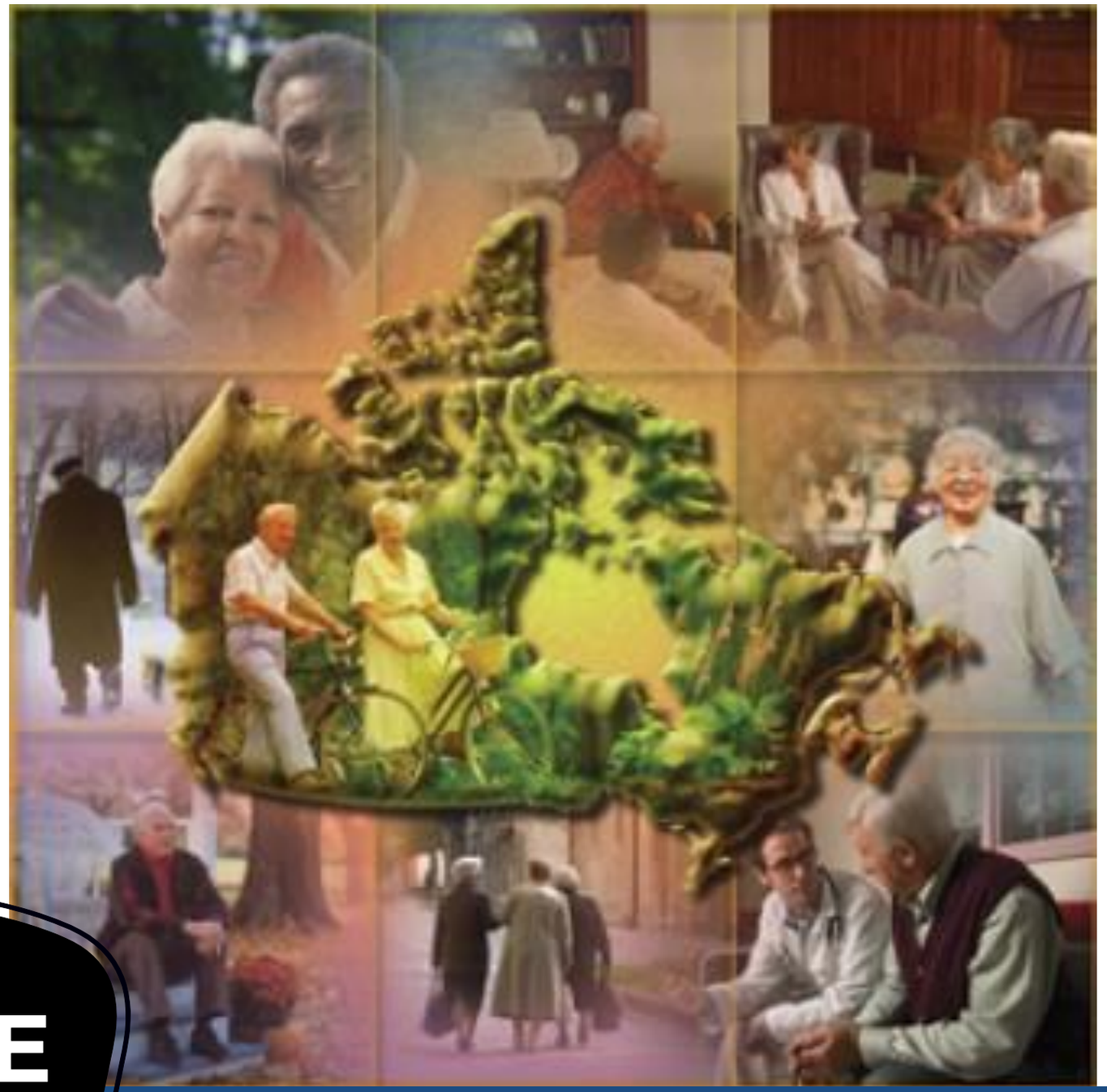


BARRIE POLICE

FRAUDS AND SCAMS

Detective Constable Kris Nicholson #7817 – Fraud Unit

Constable Julie Reynolds #6058 - Community Services Unit

PRESENTATION OVERVIEW

- ➤ Introduction
- ➤ Most common scams
- ➤ How to identify scams
- ➤ How to protect yourself
- ➤ Most recent cases in Barrie
- ➤ Questions?

FRAUDS AND SCAMS

"it is one of the ugliest forms of fraud and its on the rise in Canada"

- Statistics from the Canadian Anti-Fraud Centre show that con artists most often target 60-69 year olds, but are increasingly targeting younger populations
- On average, seniors lose 33% more money than younger victims
- Canadian losses to fraud:
  - 2020 - $106M
  - 2021 - $383M
  - 2022 (as of Oct. 31) - $420M

- Criminals target Canadians as we are a wealthy country

FRAUDS AND SCAMS

- It is estimated that only 5% of victims report their frauds to police or the CAFC
- Frauds are extremely difficult to investigate with today's sophisticated technology…**once the money is gone, it is usually gone for good!**
- Education and awareness is the most effective way to tackle this crime

WHAT CAN YOU DO TO HELP?

If you do fall victim to a scam, use your experience to alert others and combat these frauds.

After this presentation, please help us to spread the word…

Share your knowledge with friends and family!

CANADIAN ANTI-FRAUD CENTRE

A central agency in Canada that collects information and criminal intelligence on frauds

Primary Goals:

- PREVENTION through education and awareness
- DISRUPTION of criminal activities
- INTELLIGENCE dissemination
- SUPPORT to law enforcement
- PARTNERSHIPS between the private and public agencies
- VICTIM support

Toll Free: 1-888-495-8501

Website: www.antifraudcentre.ca

FRAUDS AND SCAMS TARGETING SENIORS

LOTTERY SCAMS

TELEMARKETING/SALESPERSON SCAMS

PHISHING SCAMS/IDENTITY THEFT

COVID SCAMS

GRANDPARENT SCAMS

INVESTMENT SCHEMES

RENOVATION AND DOOR-TO-DOOR SCAMS

MORTGAGE SCAMS

ONLINE SHOPPING SCAMS

LETTER FRAUD SCAMS

INTERNET FIX SCAM

BANK OR CREDIT CARD INVESTIGATION SCAMS

RENTAL SCAMS

CRA and BANK SCAMS

ROMANCE SCAMS

IDENTITY THEFT AND FRAUD

- **Identity Theft** – refers to acquiring and collecting someone else's personal information for criminal purposes.
- **Identity Fraud** – is the actual deceptive use of the acquired information of another person in connection with various frauds.
- **IMPACT ON YOU** – Damage to credit history – refusal of credit – assumed identity
- What does the fraudster want? All your personal information!
- How do they use it? Open bank accounts, transfer funds, take out loans
- protect yourself – wipe your device, be cautious when clicking on embedded links, scrutinize emails for legitimacy and manage passwords
- Be on the lookout for PHISHING schemes

INTERNET PHISHING SCAMS

What is Phishing?

- Fraudster sends message through text messaging, email, instant messaging such as snapchat or fraudulent links on TikTok or other social media platforms
- messages are designed to trick the victim into thinking they are dealing with a reputable company (i.e. financial institution, service provider, government)
- phishing messages will direct you to click a link for various reason, such as updating your account information, unlocking your account, or accepting a refund
- Fraudster's goal is to capture personal and/or financial information, which can be used for identity fraud

In some cases a hacker can take control of your computer, access personal data, gain access to sensitive information, logins, passwords, bank accounts and so much more.

INTERNET PHISHING SCAMS

Can you find the 11 signs that this is a fake email?

From: Helpdesk <helpdesk-infotech@gmail.com>

To:

Subject: Fraud Alert!

Attachment: Password Reset Details.exe

Dear Info-Tech user,

We have recently detected a login to your online account that was not performed by you. In order to rectify this situation please go to InfoTech website here to change your password to ensure your account is secure. The documnt attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details and I will verify your account for you. If you fail to do so by next week will result in your acount being deleted.

Sincerely,

Info Tech

INFO~TECH
RESEARCH GROUP

INTERNET PHISHING SCAM

From: Helpdesk <helpdesk-infotech@gmail.com> 1

To:

Subject: Fraud Alert! 2

Attachment: Password Reset Details.exe 3

Dear Info-Tech user, 4

We have recently detected a login 5 our online account that was not 6 rmed by you. In order to rectify this situation please go to InfoTech website here to change your password to ensure your account is secure. The 7 document attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details 8 I will verify your account for you. If you fail to c 9 by next week will result in your acount being deleted.

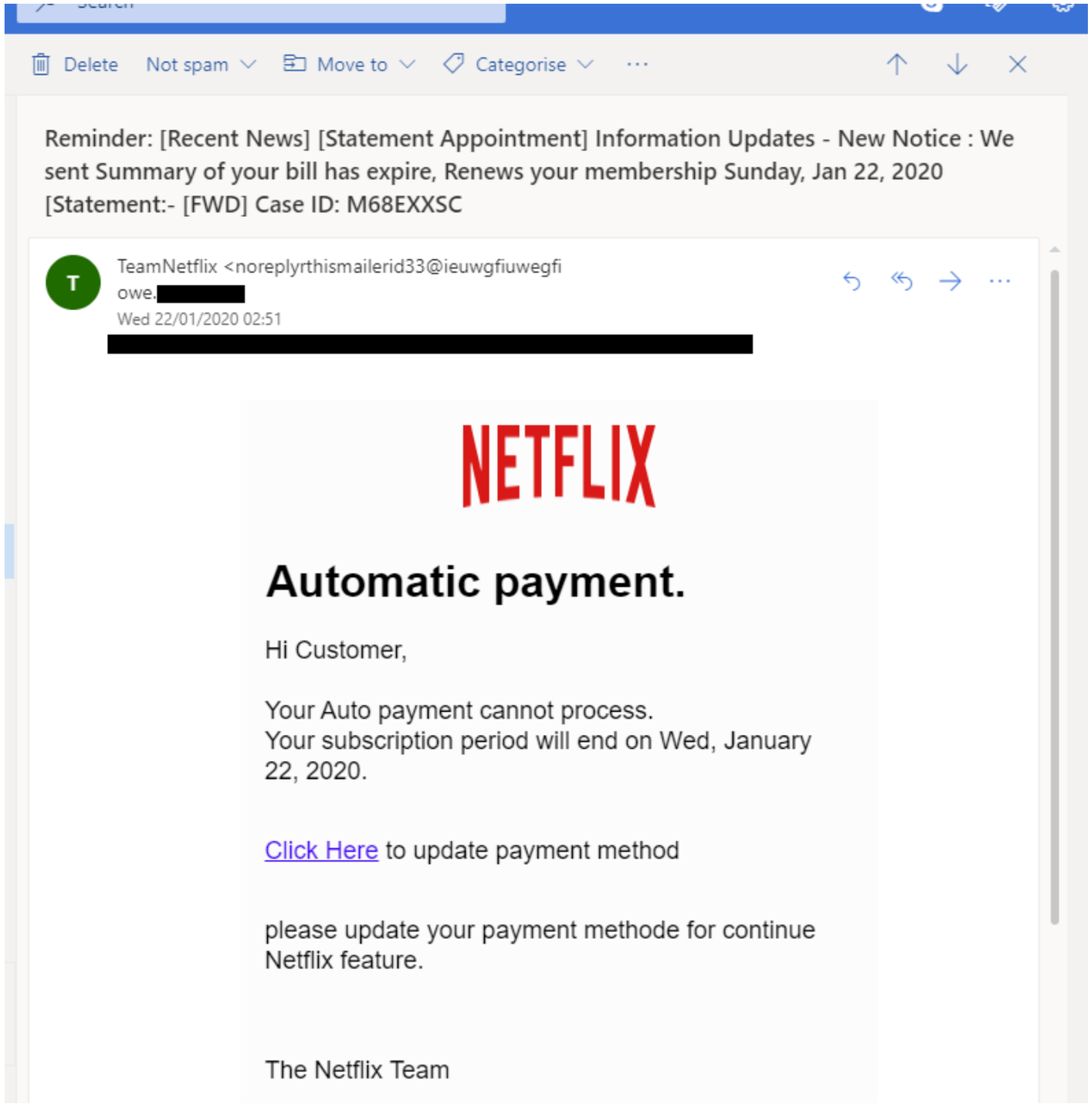
10

Sincerely,

Info Tech 11

INFO~TECH
RESEARCH GROUP

INTERNET PHISHING SCAM



GRANDPARENT SCAMS

- Senior receive a phone call – usually male voice
- Caller may start call saying hello grandma or grandpa, do you know who this is?
- Senior responds by saying “is that you Johnny?” or saying name of grandchild.
- Fraudster uses information they are able to pull out of victim to gain victim’s trust
- Presents story about urgently needing money, usually to be bailed out of jail, or as a result of a car accident or for medical bills
- Sometimes hands phone over to “lawyer” or “officer”
- CREATES URGENCY AND SECRECY
- Success of fraudsters is due to playing on victim’s emotions, thereby preventing them to think clearly

GRANDPARENT SCAMS

Take Time to verify the story. Scammers are counting on you wanting to quickly help your loved one in an emergency.

Call the child's parents or friends or other family members to find out about their whereabouts.

Ask Questions to the person on the phone that only your loved one would be able to answer and verify their identity before taking steps to help.

Never Send Money to anyone you don't know and trust.

Never Give Out Personal Information to the caller and be cautious of them asking questions which may reveal information they can use to scam you further.

BITCOIN AND INVESTMENT SCHEMES

Always be suspicious of:

- Unsolicited investment opportunities (even from friends or family)
- Promises of higher than normal returns
- High pressure tactics
- Requests for Cryptocurrency payments

BITCOIN AND INVESTMENT SCHEMES

BANK OR CREDIT CARD INVESTIGATION SCAMS

- Imposter from cards security company will contact you about a suspicious transaction on your account.

- Ask you to verify your account information including card number and the security numbers on the back of the card.

- This is an attempt to get your information to steal your identity and make duplicate cards.

- Banks will never ask for this information over the phone or by e-mail. They will have you come to the bank, or will simply provide you with information and ask you to confirm

CANADA REVENUE AGENCY AND BANK SCAMS

- Many different variations – email/telephone/text message
- May ask for personal information
- Send you a link to a website resembling the CRA's or the bank's, and then asks you to verify your personal and/or account information
- Ask for banking information in order to deposit a refund
- Fraudsters are aware that Canadians often let their guard down when offered money from the CRA or bank

Questions to ask yourself:

1 - Does this sound too good to be true?

2 - Am I expecting more money from the CRA?

3 - Is the requester asking for information I know the CRA already has on file for me?

ALWAYS TAKE THE TIME TO VERIFY CALLER IS WHO THEY SAY THEY ARE!!

Canada Revenue Agency | Agence du revenu du Canada

Canada Revenue Agency
www.cra.gc.ca

Dear Tax Payer,

You are entitled to your tax refund now. The tax refund is $241.34. You are required to follow t
login to our secure Epass site with your Social Insurance number and complete the required info
for your refund to be processed.

http://www.cra-arc.gc.ca/gol-ged/gov/confirmtaxrefund?REF128328-Jh28877a

Yours sincerely,

Gilles Dompierre, Department of Revenue, Canada

BMO Bank of Montreal : Notification of Irregular Account Activity. — Inbox

From: **BMO Bank of Montreal <customer-service@bmo.com>** Hide
Subject: BMO Bank of Montreal : Notification of Irregular Account Activity.
Date: 23 January, 2012 9:03:02 AM EST
To:

BMO Financial Group

Dear Customer,

BMO Bank of Montreal detected irregular activity on your Account on 23 January 2012. For your protection, you must verify this activity before you can continue using your BMO Bank of Montreal Account.

Click on the link below to access and verify your statement.

https://www1.bmo.com/cgi-bin/netbnx/NBmain?product=1 This instruction has been sent to all bank customers and is obligatory to follow.

Thank you
Customers Support Service
BMO Bank of Montreal.

RBC Financial Group

Due to a recent security breach in the RBC computer systems, we are asking all customers to immediately login with the link below and immediately report any unnoticed password changes, unexplained funds depletion or the likewise. Rest assured that we have the safety and privacy of our customers as our top priority but please help us by following the instructions below.

Update and verify your information by clicking the link below:

https://www1.royalbank.com/cgi-bin/rbaccess/rbunxcgi?F6=1&F7=IB&F21=IB&F22=IB&REQUEST=ClientSignin&LANGUAGE=ENGLISH

TD Canada Trust
EasyWeb

Dear Online Banking Client

We have detected an unusual activity in your account. We have temporarily de-activated your account for your own protection to re-activate your account kindly

Log on to www.access.tdcanadatrust.com

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,

Online Banking Team

TD Canada Trust, N.A. Member FDIC
2012 TD Canada Trust.

Scotiabank — Scotia OnLine® Financial Services

Communications Centre

Dear Scotiabank Customer,

Greetings from Scotiabank.

Welcome to the Scotiabank AAdvantage(R) program, the first and largest loyalty program in the world! We are proud to inform you that today Scotia Bank, launch a new reward program. Please log in to your Scotia Bank account and take the 5 questions survey. For your effort you will be rewarded with $100

Your 100 dollars bonus code is **SCOTIA-005NX-2008NX50**. Please click here Scotia Online AAdvantage(R) program and follow the steps.

Thank you very much for your help and your patient and hope you will enjoy the Scotia Bank reward program in the future

Sincerely,
Thank you.
Scotiabank Head Office
44 King St West
Toronto ON
M5H 1H1
info@scotiabank.com
1-800-4SCOTIA (1-800-472-6842)
1-800-645-0288 (services for the hearing impaired)
(416) 701-7200 (Greater Toronto Area)
Please do not reply to this auto-answer message

CRA SCAMS

From: Canada Revenue Agency <notify-payments.interac@email.com>
To: Recipients <notify@payments.interac.ca>
Sent: Monday, April 24, 2017 2:08 PM
Subject: Action required: INTERAC e-Transfer - Canada Revenue Agency sent you money.

Interac e-Transfer View in browser | Français ?

Hi,

Canada Revenue Agency sent you $896.70 (CAD).

Deposit your money:

BMO

ROMANCE SCAMS

- Person from another country befriends you online, pretending to be interested in a romantic relationship or a friendship that quickly turns into a romance
- A lot of time is invested in gaining your trust
- All of a sudden there is a terrible incident (accident, in jail, robbed, etc.) and they ask you for loan to get bailed out of whatever trouble they are in

Online Dating Scams: What to do

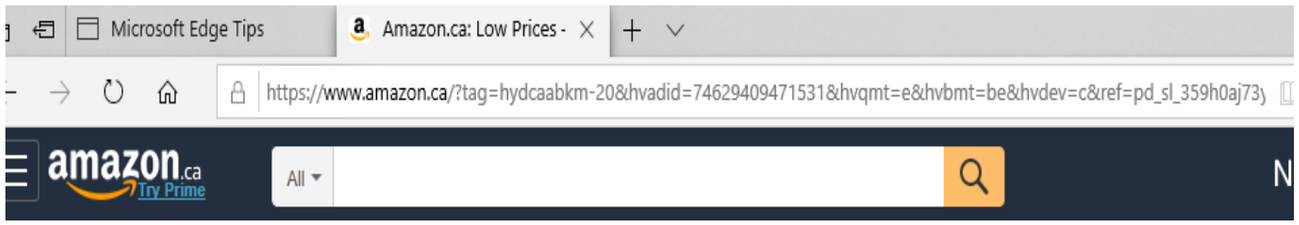
1. **Slow down** — and talk to someone you trust. Don't let a scammer rush you.
2. **Never wire money**, put money on a gift or cash reload card, or send cash to an online love interest. You won't get it back.
3. **Contact your bank right away** if you think you've sent money to a scammer.
4. **Report your experience to:**
   - The online dating site
   - Federal Trade Commission: **ftc.gov/complaint**
   - Federal Bureau of Investigation: **ic3.gov**

FEDERAL TRADE COMMISSION • ftc.gov/imposters

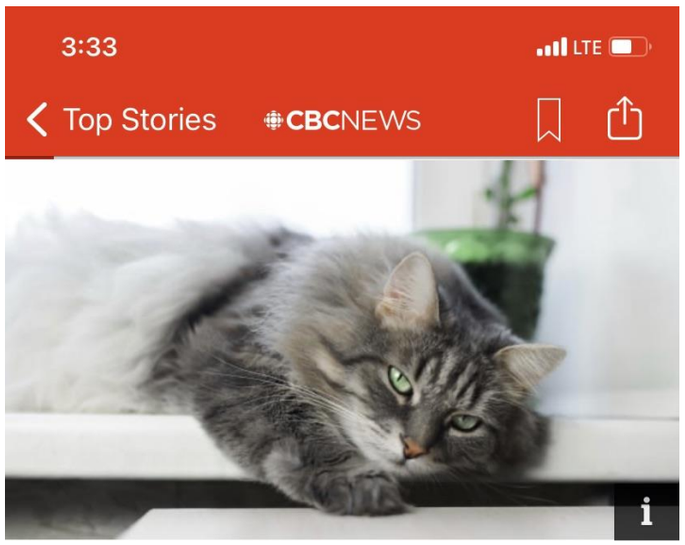
BARRIE POLICE

ONLINE SHOPPING SCAMS

- May receive counterfeit product, lesser valued/unrelated goods, or nothing at all
- Beware of deceptive advertising and deep discounts as “hook”
- Scammers often request payment through wire transfer, courier, money order, e-transfer, bank draft, PayPal or CRYPTOCURRENCY OR GIFTCARDS
- Only purchase through reputable companies and websites.
- Be cautious when shopping online, especially when dealing with “third party sellers”



ONLINE SHOPPING SCAMS



Beware kitten and puppy scams, as pandemic leads to spike in pet ripoffs

Pet scammers target people with cute photos and stories to lure them into sending money

Posted: November 30, 2022 4:00 AM EST
Last Updated: 2 hours ago

Yvette Brend, CBC News

It starts with a photo — a big, doe-eyed close-up — of a kitten or puppy.

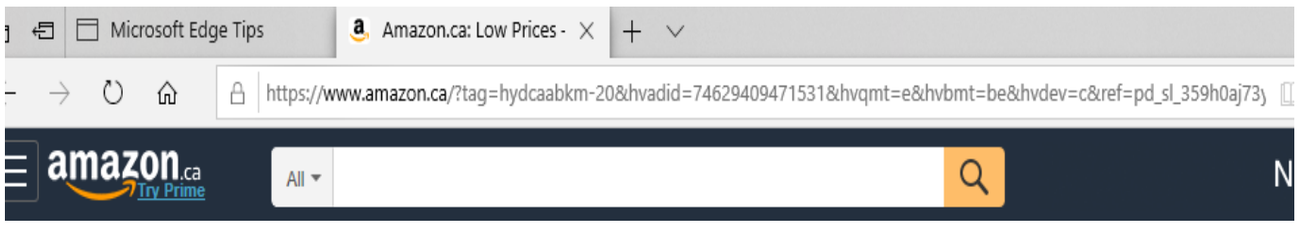
To many, the price seems impossibly low for that promise of fluffy affection.

That's how to hook a buyer, and unscrupulous scammers know it.

- Rental scams
- Pet adoption scams

WHAT TO LOOK FOR WHEN SHOPPING…

- **Prices that are too low -** There's a limit to how much consumers can expect to save.
- **Red flags about payment -** For legitimate businesses' online stores, the process for paying for merchandise online should be straightforward and standardized - Canadians should be wary of processes that seem overly complicated.
- **Sites that look poorly designed -** Most legitimate online stores will invest time and effort into the user experience, with nice images, an easy-to-navigate website and a smooth check-out process. Spoofed stores don't apply the same standards.
- **Stores that are missing key information -** The majority of legitimate retailers will always have a return policy, a privacy policy and proper contact information for the business.
- **Stores that are missing security elements -** A padlock symbol next to the URL in the address bar that is open or missing indicates the website's data is not secure.
- **Typos or errors in the URL of the store -** A common method of spoofing websites of popular brands is to substitute correct letters for ones that appear to be accurate, for example Go0gle.com.



STAY SAFE WHEN SHOPPING!

- Never save credit card information in a browser
- Make online purchases through personal Wi-Fi networks. If purchases must be made when not at home, use cellular data instead of public networks
- Purchase familiar brands and from proven retailers
- Do research and read reviews

LETTER FRAUD SCAM

- People will receive a letter or e-mail from someone claiming to be a Prince, bank a lawyer or government official from a foreign country.

- The person is very wealthy or there is a large amount of money in an account and wants to get money out of the country.

- Offer to give you money for use of your bank account and ask you to send your banking info, passwords etc.

- This is nothing more than another attempt to get access to your bank account.

LETTER FRAUD SCAM

Send | Cc... | Subject: FW: re

From: Gilbert Melue <geeeeeeeeee09@libero.it>
Date: March 18, 2013 6:21:07 PM GMT-04:00
Subject: re
Reply-To: Gilbert Melue <geeeeeeeeee09@libero.it>

Dear Friend,

Please forgive my using this means to reach you but I can't think of any other way of letting you know the urgent matter at hand. I don't actually know if this is the right medium to communicate with you but I don't have any option right now considering the incessant letters from the banking authority withholding the funds. This letter of high confidentiality and therefore I will appreciate you treat with utmost maturity and confidentiality.

The amount involved is US$7.5 M and it's safe in the deceased coded account. More details will be relayed to you only if I receive your positive response through my private mailbox: (gilbertmelue@hotmail.com) I have decided to share with you the proceeds of the inheritance claim. 35% will be for you for gratification and input. 30% will be used to build an orphanage in the name of the deceased as he wished before his death in your country and 35% will be for me.

I am a noble man with family and a name to protect and therefore will urge you to treat with maturity. Do get back to me for further details.

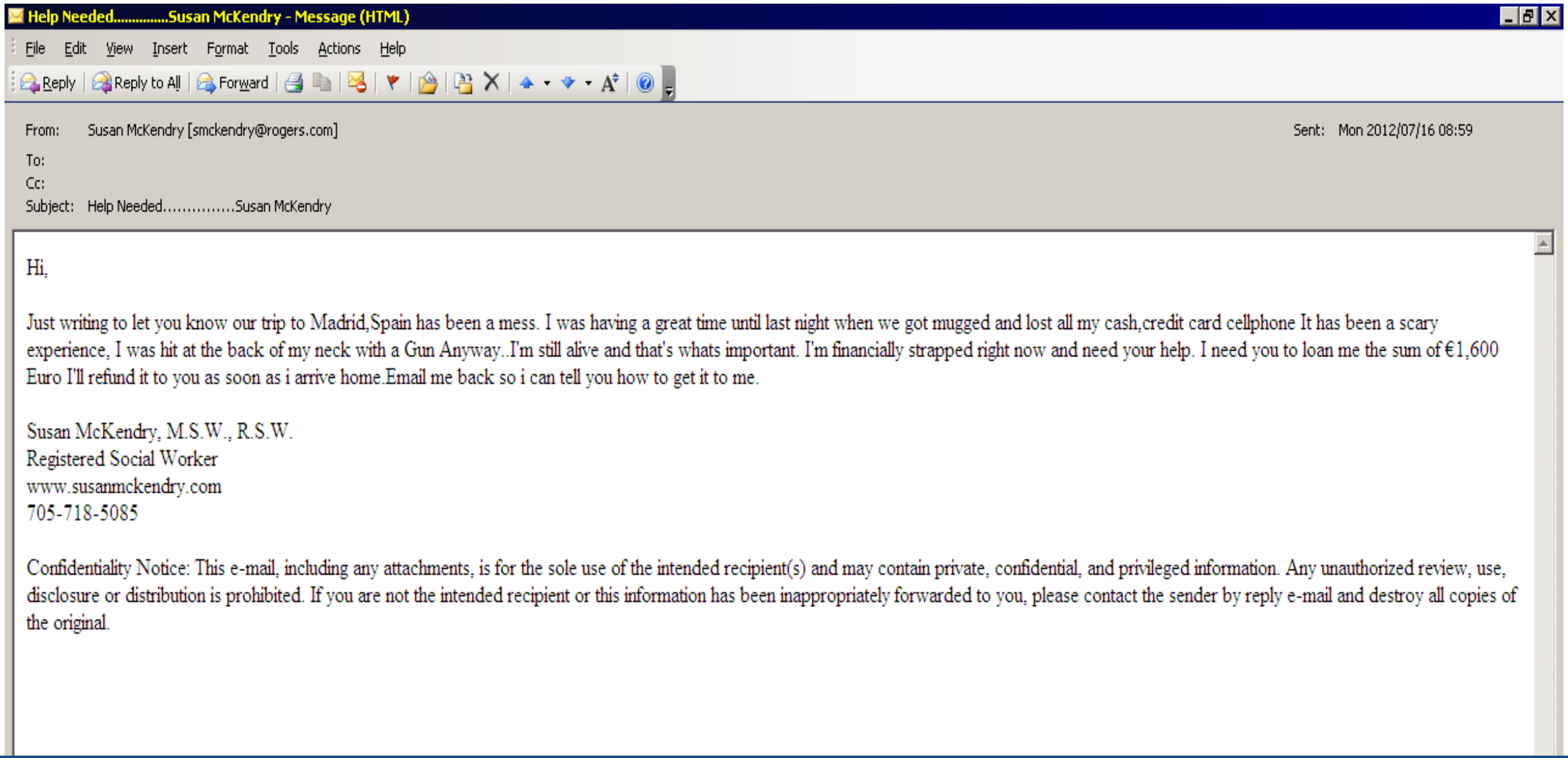
Thank you,

Barr.Gilbert Melue Esq.

BARRIE POLICE

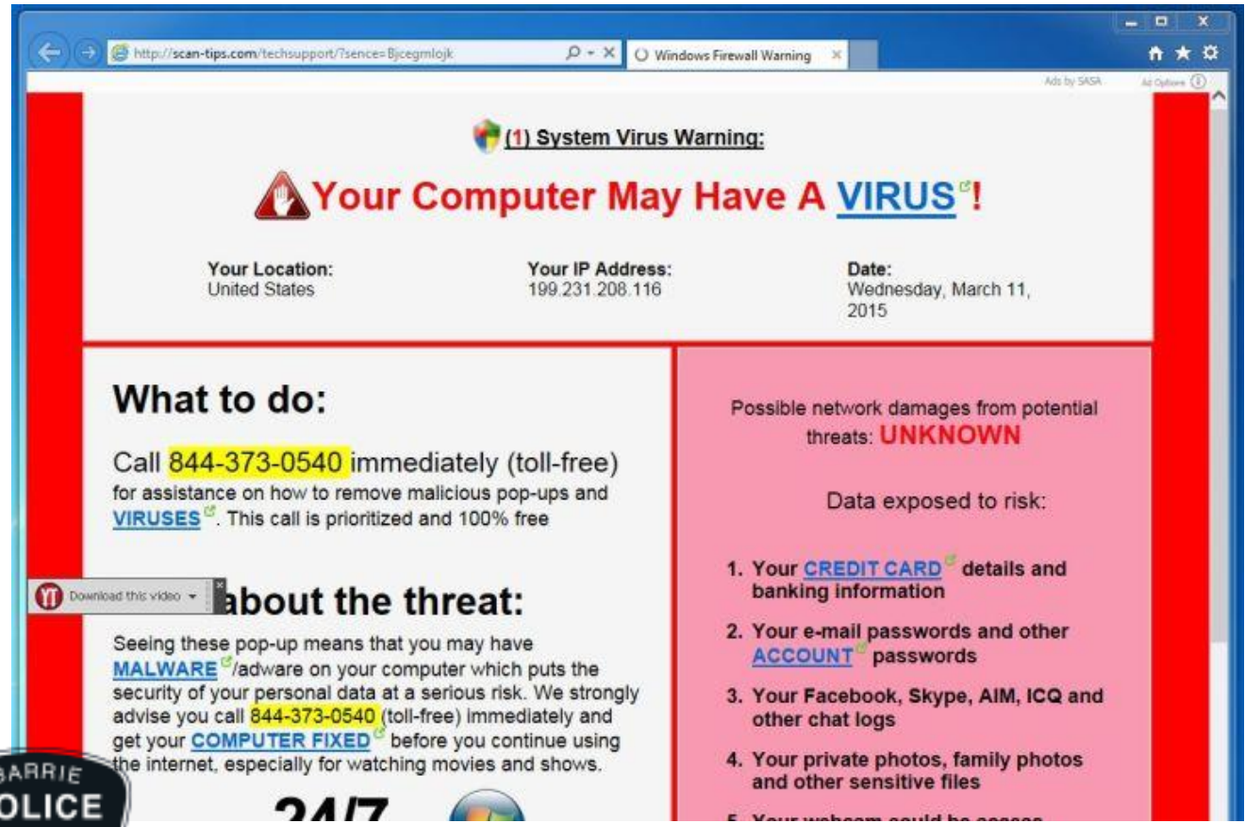
“FRIEND IN NEED” LETTER FRAUD SCAM

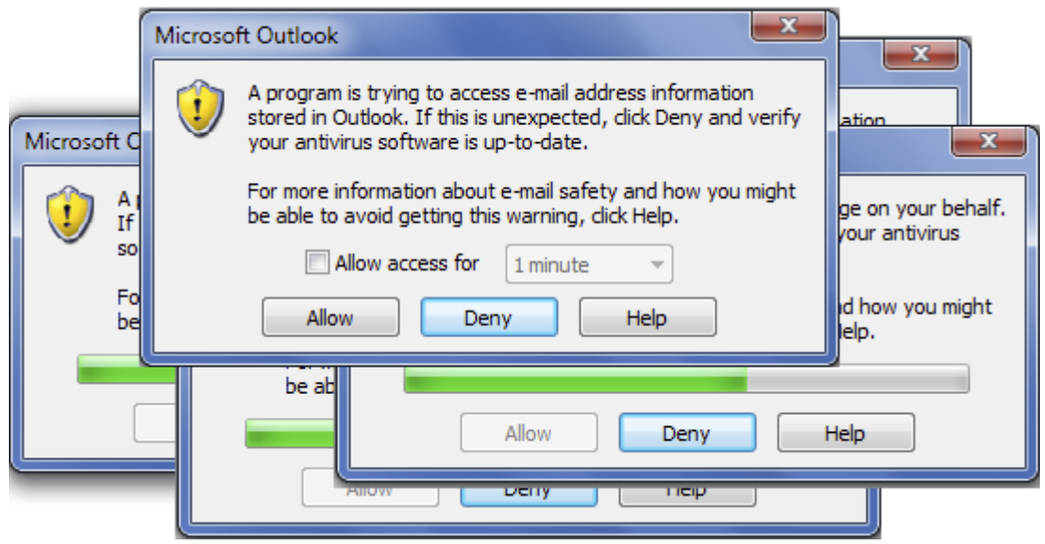
Email supposedly from a person known to you claims that he or she is stranded without money or papers in a foreign land because of a robbery and asks that you send funds urgently via a wire transfer to help the person return home.



INTERNET FIX SCAM

- Caller advises that they can tell your internet is slow, or that you have a particular internet virus (i.e. Zeus)
- For a fee, the caller will take remote control of your computer and “clean it up” or fix it so that it functions faster again
- Scammer may be mining your computer for personal and banking info, or just playing around to get paid for nothing





PROTECTING YOURSELF ON SOCIAL MEDIA

- Great way to connect with friends but criminals use it as well
- Make sure to set your privacy settings so that only your friends have access to your profile
- Never post personal information (phone number, address, bank information)
- Be careful when sharing photographs online…once they are posted they cannot be recovered
- Be leery of strangers attempting to be your friend

HOW CAN I RECOGNIZE A SCAM?

- It sounds too good to be true
- You must pay or you can't play/claim prize
- Someone requests to be paid with gift card codes, cryptocurrencies, by wire transfer or courier
- It's the manager, a lawyer or a prince calling
- The stranger calling/texting/email media wants to become your best friend and/or quickly professes love
- You must give them your private financial information
- Poor spelling and grammar, general address (“Dear User”, “Dear Customer”, etc.)
- Fraudsters often
  - create urgency or include threats
  - encourage secrecy with friends and family
  - offer tips on how to answer bank employees if withdrawals/transfers/wires are questioned

PROTECT YOURSELF!

- Never assume that the phone numbers appearing on your call display are accurate
- Government agencies won't contact you and tell you that your SIN is blocked or suspended or threaten you with legal action, demand immediate payment, ask for you to submit your money for investigation, or request payment by Bitcoin, a money service business or gift cards
- Beware of individuals quickly professing their love for you.
- Beware of individuals who claim to be wealthy, but need to borrow money.
- When trying meet in-person, be suspicious if they always provide you with reasons to cancel.
- Never send intimate photos or video of yourself as they may be used to blackmail you.
- Never accept or send money to a third party under any circumstances.
- Never allow an individual to remotely access your computer.

PROTECT YOURSELF!

- Verify any incoming calls with your credit card company by calling the number on the back of the card.
- Never provide any personal or financial information over the telephone.
- Only a credit card company can adjust the interest rate on their own product.
- Research all companies and contractors offering services before hiring them.
- Financial institutions will never ask for assistance from the public for internal investigations.
- The only way to participate in any foreign lottery is to go to the country of origin and purchase a ticket. A ticket cannot be purchased on your behalf.
- In Canada, if you win a lottery, you are not required to pay any fees or taxes in advance.
- Confirm with other relatives the whereabouts of a family member or friend asking for financial assistance

HOW CAN I RECOGNIZE AN EMAIL SCAM?

You can use this checklist to remind you what to look for

Phishing checklist:

- ❑ Does the email ask for your personal information?
- ❑ Check the sender's email address.
- ❑ Is the greeting personal?
- ❑ Is there poor spelling and grammar in the email?
- ❑ Does the signature look legitimate and have contact information?
- ❑ Is the attachment necessary?
- ❑ Does the attachment end in .exe?
- ❑ Hover over all links to make sure they will lead you to the right place.
- ❑ Are there any clear signs of common phishing tactics?
- ❑ Do you feel it is suspicious? If so, report it or contact the company directly to find out more

CONTACTS

Police Related Support:

- Emergency – 911
- Barrie Police Services - (705) 725-7025
- Crime Stoppers – 1-800-222-TIPS (8477)
- www.barriepolice.ca

FRAUD:

Recognize It.

Report It.

Stop It.

Thank You

PC Julie Reynolds #6058
Barrie Police Service
Crime Prevention Unit
705-725-7025 ext. 2615