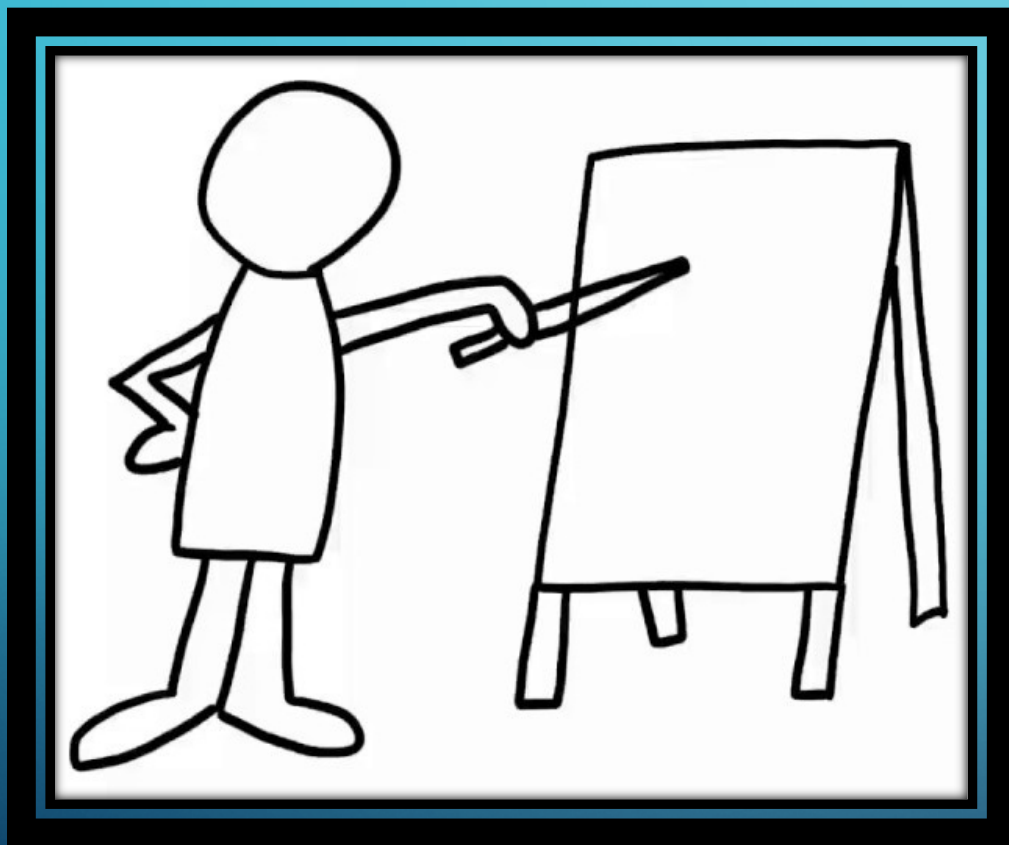


SCAMMER AWARENESS: KEEPING INFORMED IN 2023

PRESENTED BY ALEX STEPHENS



PRESENTATION FORMAT



Approximately 40 minutes
with open discussion following

Introduction

Part 1: The State of Scamming in 2023

Part 2: Common Scams & Case Studies

Part 3: Strategies to Keep You Safe

Conclusion

INTRODUCTION

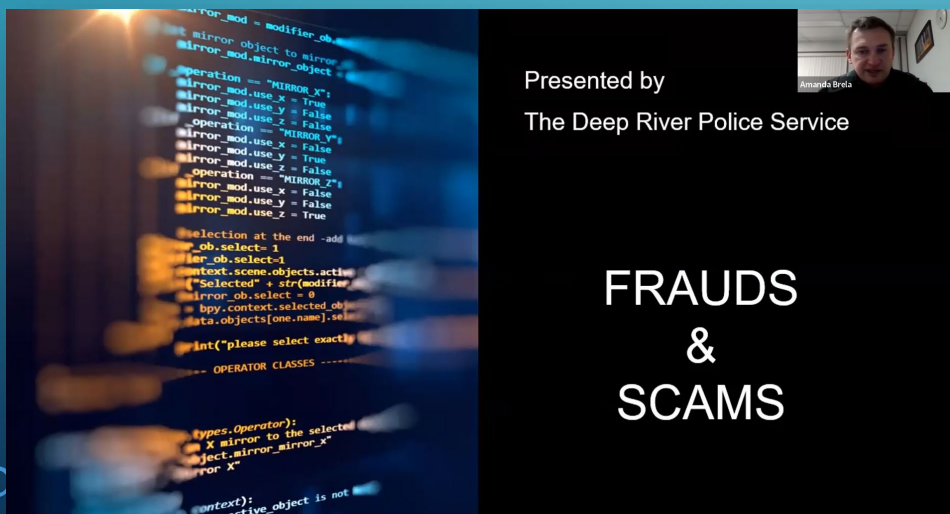
- Hello!
- Who am I?
 - I'm Alex and I was scammed once (more on that later)...
- What are we discussing?
 - Scams in 2023 with an emphasis on local scams and strategies to keep yourself safe.
- What is my authority on the matter?
 - Largely practical, hands-on experience and I endeavour to keep informed.



INTRODUCTION

I should mention...

- Deep River Police and Ross Judd online presentation in December, 2021.
 - Excellent information provided which I may reference
 - Link available to anyone who would like to view



INTRODUCTION

I should also mention...

- Additional sources of information:
 - Canadian Anti-Fraud Centre
 - Government of Canada website
 - National Cybercrime Coordination Centre (NC3)
 - Antivirus platforms: Kaspersky, Bitdefender, Norton, McAfee, Avast, Panda, Malwarebytes, etc.
 - Newspapers: NRT included
 - Standard news outlets
 - Peers & old co-workers
 - Reddit and other information-sharing websites
 - Personal experience
- 



INTRODUCTION

I feel that while on the surface this topic is about information and technology, it can be highly emotionally-charged. Everyone has their own stories.

At the end of the day this is a topic about people.

The rabbit hole is very deep so my approach is to touch on relevant concepts and then introduce some practical information you can use.



PART 1: THE STATE OF SCAMMING IN 2023

- Think of information as a currency
 - You are within your own bubble and you must protect it
- Real-time threat maps
 - Illustrate that digitally, the world is small
 - Kaspersky – headquarters in Moscow
 - In 2017, banned from installation on any US government institution computer
 - In 2022, FCC issued warning to business about using this software
 - This is a grey area but consider how it makes you feel using this software...



PART 1: THE STATE OF SCAMMING IN 2023

Scamming is old business, but let's define it:

- **Scam (noun):** A fraudulent or deceptive act or operation
 - An insurance scam
- **Scam (verb):** To deceive and defraud (someone)
 - To obtain (something, such as money) by a scam



“A Boston hedge fund manager who scammed millions of dollars from friends, family and other investors in what authorities say was a Ponzi scheme has been sent to prison for more than 14 years.”

The Worcester (Massachusetts) Telegram & Gazette

*Merriam-Webster Dictionary

PART 1: THE STATE OF SCAMMING IN 2023

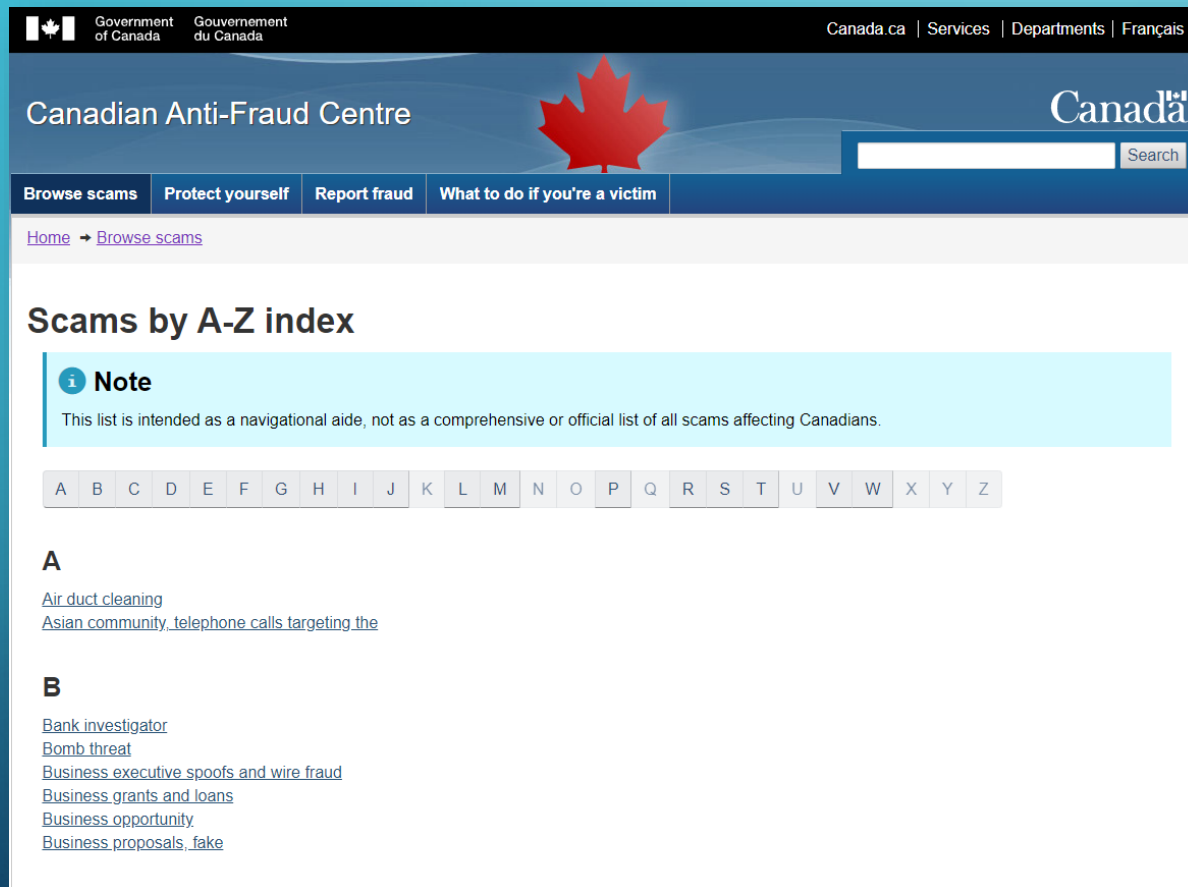
In other words...

“blackmail, deceit, deception, extortion, fraud, hoax, racket, rip-off, shakedown, sham, cheating, con, double-dealing, flimflam, hosing, hustle, sting, con game, crooked deal, dirty pool, double cross, fast one, shady deal, shell game, sucker game”



*www.thesaurus.com

PART 1: THE STATE OF SCAMMING IN 2023



The CAFC has an A-Z index to classify all the ongoing types of scamming, and more are being added all the time.

Common scams include:

- Phishing
- Spam e-mails
- Covid-19 and benefits
- CRA impersonation
- Home HVAC, furnace calls
- Fake calls and texts
- Facebook profile hijacking
- Anything involving gift cards

To name but a few...

*Canadian Anti-Fraud Centre

PART 1: THE STATE OF SCAMMING IN 2023

The impact of fraud so far this year

As of December 31, 2022

Reports of fraud:

90,137

(107,381 in 2021)

Victims of fraud:

56,352

(68,087 in 2021)

Lost to fraud:

\$530 M

(\$384 M in 2021)

Funds recovered with CAFC assistance

As of October 31, 2022

\$2,400,000

(\$3.35 M in 2021)

=0.4528 %

Less than half a percent recovered. Is that good?

Keep in mind that a great deal of people who are scammed do not report it for various reasons:

- Fear
- Embarrassment
- Futility
- Lack of knowledge or available resources

*Canadian Anti-Fraud Centre

PART 1: THE STATE OF SCAMMING IN 2023

- There is an intelligence behind scamming; scamming adapts, learns, evolves but relies on many of the same old tricks and centres all around information
- Thinking of information of a currency, consider that there are many online places that gather personal information and people voluntarily divulge:
 - Facebook
 - Amazon (including Alexa)
 - Tik-Tok
 - LinkedIn
 - Websites and services that require personal information to create an account...





*The New York Times – “Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too.”



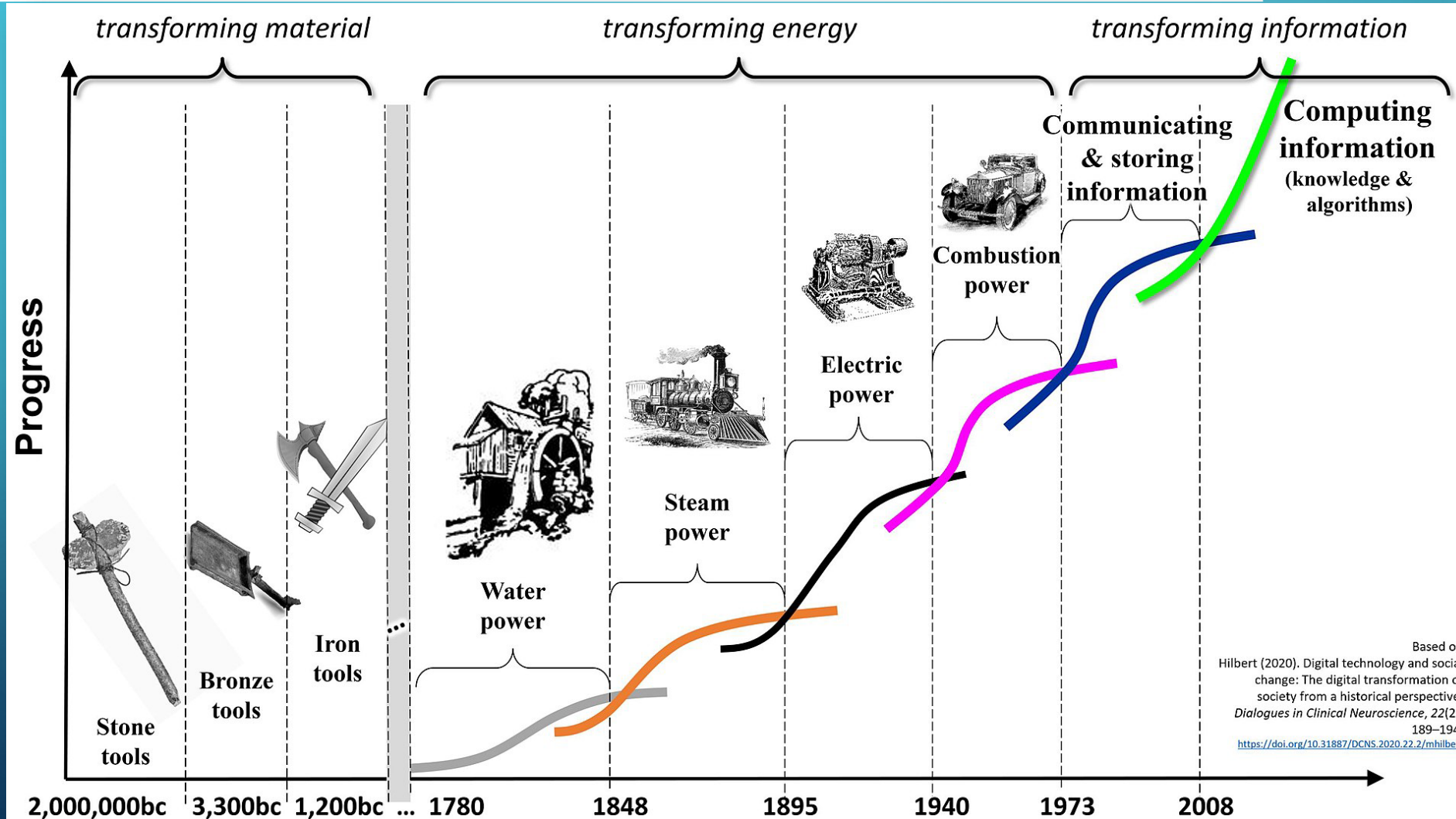
PART 1: THE STATE OF SCAMMING IN 2023

- Interesting article about Amazon – *“The Data Game. What Amazon Knows About You and How to Stop It”* - The Guardian
- Alexa and Ring doorbells collect data, connected to home networks
- The short answer is, do not use Amazon or:

A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.



PART 1: THE STATE OF SCAMMING IN 2023



PART 1: THE STATE OF SCAMMING IN 2023

- The point of all this is what if this data is breached or leaked?
 - A breach is when it is accessed by a cyberattack
 - A leak is when it is unknowingly exposed to the public
- It is best to reduce the size of our bubble to limit the potential dissemination of personal information to those ill-inclined



PART 1: THE STATE OF SCAMMING IN 2023

- An email I received last week:

Indigo an update from us

Dear Valued Customer,

We are very grateful for your support and wanted to ensure you were the first to hear an important update from us.

What happened?

On February 8, 2023, Indigo experienced a cybersecurity incident that affected our systems. We immediately engaged third-party experts to investigate and resolve the situation. Our investigation is not yet complete.

How does this impact you?

Some of you have asked us questions about plum points and credit and debit cards. Here is some information we are happy to share:

- Customer credit and debit card information was not compromised by our recent cybersecurity incident. We do not store full credit or debit card numbers in our systems.
- Customer plum points remain intact and unaffected by the cybersecurity incident.

The relaunch of our online store will happen as soon as we are confident we can provide our seamless online experience to you once again. Stay tuned!

In the meantime, our stores are open and accepting cash, debit, credit, and gift card transactions. We look forward to seeing you! Please note we are temporarily unable to accept exchanges and returns.

We're here to support you and will continue to provide updates as more information becomes available.

If you have any questions or concerns, please contact service@indigo.ca.

Sincerely,
Team Indigo

PART 1: THE STATE OF SCAMMING IN 2023



Meta

- Facebook – 533 million users' data leaked in 2019
- Marriott – 500 million users' data hacked in 2018 including passport info and credit card #'s
- Yahoo – 1 billion accounts reported affected with information breach ultimately revised by Verizon to ALL 3 billion accounts total (yes 3,000,000,000) in 2013
- In a way it's fortunate companies are mostly concerned about protecting themselves which in these cases means beefing up security to avoid litigation, but 'accidents' still happen
- Companies collect huge amounts of data about people, and that data can be copied and used by scammers, including a vast amount of personal information, login details and potentially passwords if they are not protected or encrypted...



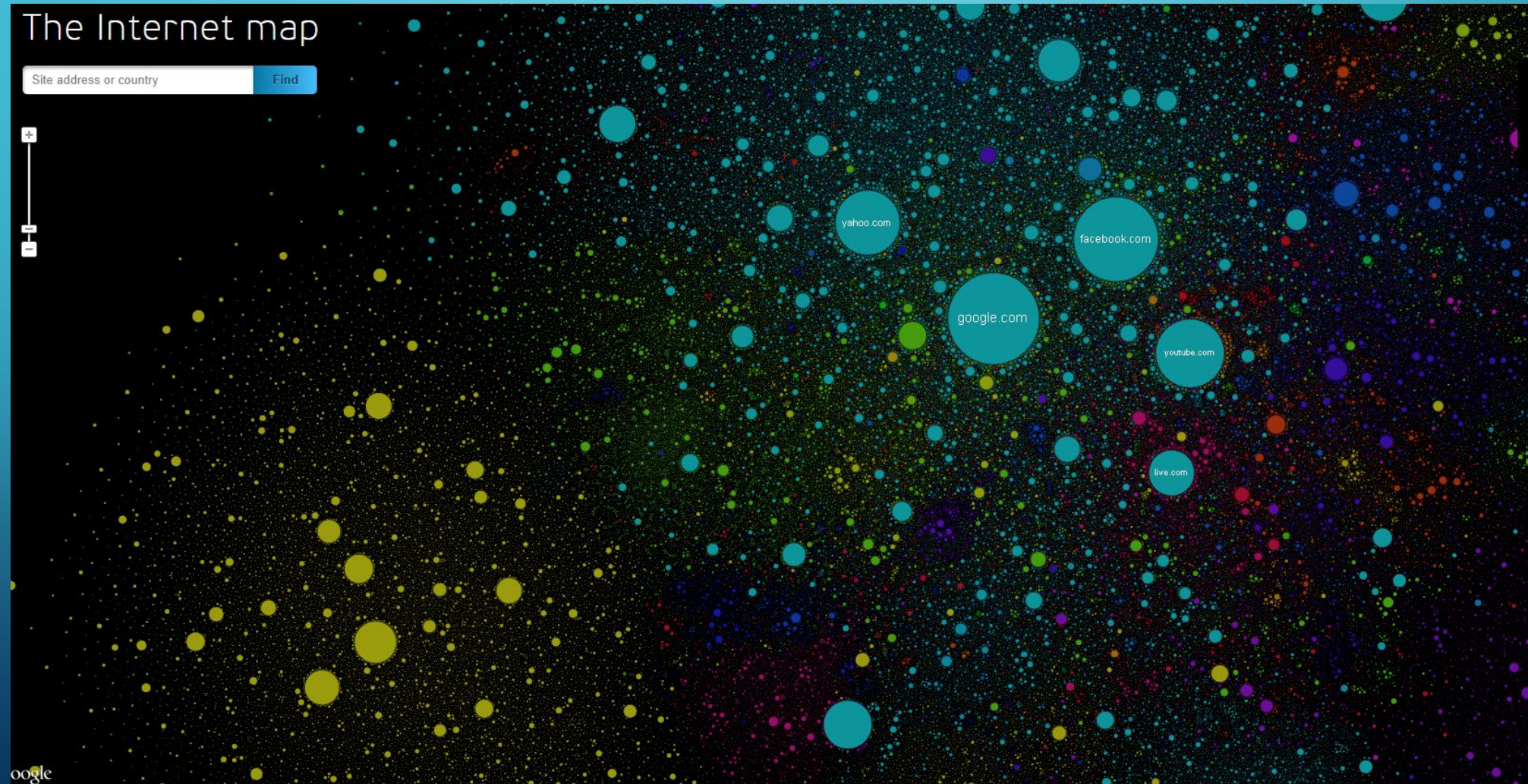
*Business Insider

A MAP OF THE INTERNET



www.kaspersky.com

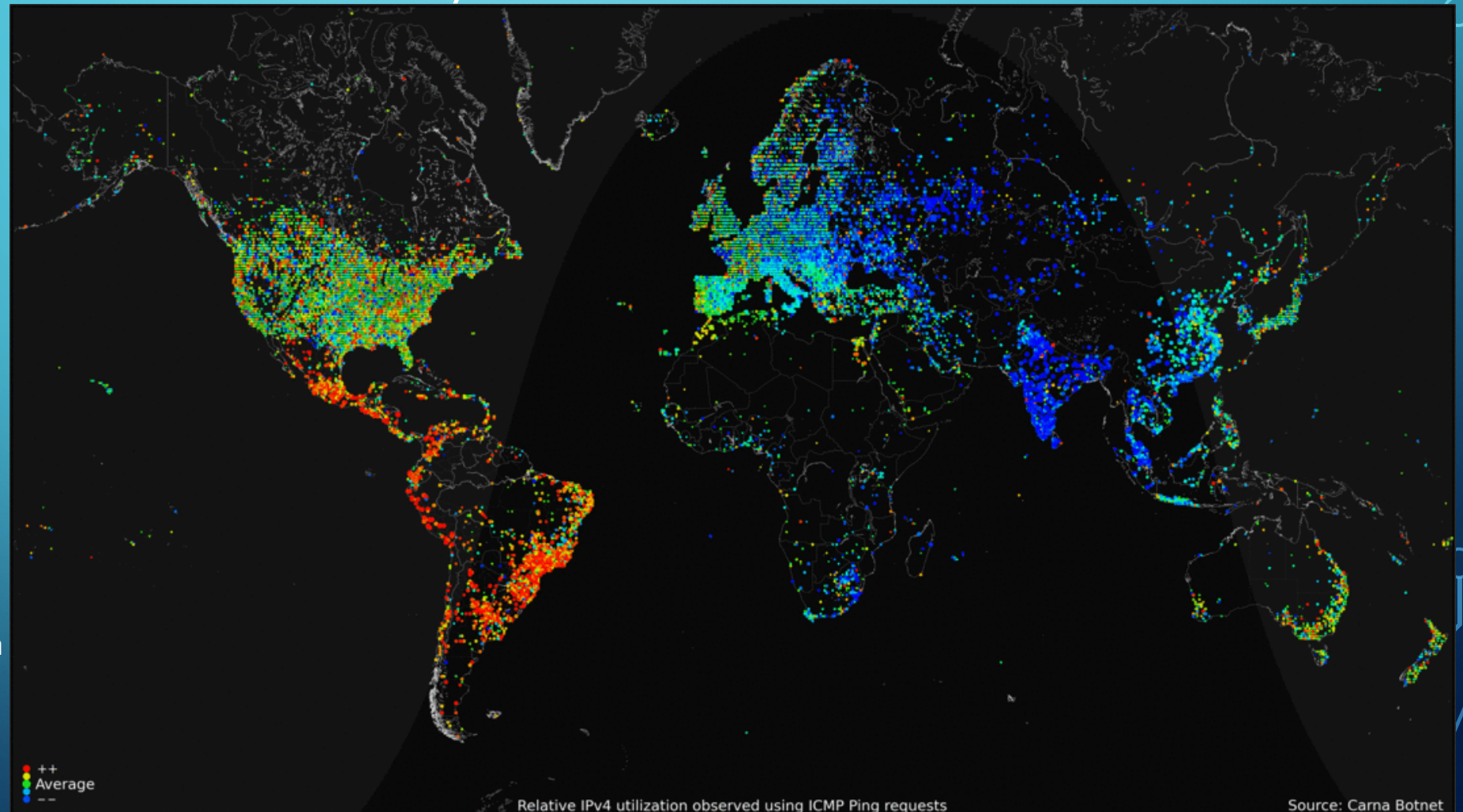
ANOTHER MAP OF THE INTERNET



INTERNET ACTIVITY DAY/NIGHT

Illegal Internet census

Yes, it's possible. In 2012 an anonym created a giant network of infected devices called Carna Botnet, which included 420,000 devices with unreliable passwords. Infected systems were used to ping anything they could reach. In the end the author produced a map, which shows 460 billion devices connected to the Internet.









PART 1: THE STATE OF SCAMMING IN 2023

Does this look familiar?

Once your email ends upon a spam list,
it's very difficult to fully block unwanted
Incoming mail. In my experience,
Gmail is the worst for this.

Advice: Keep a secondary email address
For registering with websites, as always
keep Personal information private.
If available, use email filters or set spam
to go automatically to Trash.

Shipping_Pending Your package  notification  PENDING PACKAGE	8:45 AM
Norton_Antivirus URGENT! You are without virus protection. XXXXX	7:42 AM
Trudeau_Bitcoin Why is now really the best time to invest in Bitcoin? It will recover within 2 months. -----=_mimepart_8babba5708f6cc38f27c933c89254df9 Content-Type: multipart/parallel;	Fri 2:49 PM
Order_Pending Your package notification -----=_mimepart_8babba5708f6cc38f27c933c89254df9 Content-Type: multipart/parallel;	Fri 2:46 PM
PACKAGE.NOTICE  Delivery of your package  Notification ID # 096490080 -371  <https://storage.googleapis.com/chevillotmartine/arhlonrbipiomh.html#WftGGYqgLBhSsDXuOYH.hjoz1rter...>	Fri 12:48 PM
Mcafee™ Final Notice: Your Computer will no longer Protected, Your Subscription may have ended ... -----=_mimepart_8babba5708f6cc38f27c933c89254df9 Content-Type: multipart/parallel;	Fri 11:38 AM
WALMART-WINNER CONGRATULATIONS, YOU HAVE WON DYSON VACUUM Final notice: 2nd attempt for you.	Fri 10:40 AM
Norton-Antivirus URGENT! Your subscription has lapsed! <http://bzq-82-81-85-250.red.bezeqint.net/S5a3PxqQ.swf?fpqfggbcR3TXcypVFcdcW5cKc7D1bh7kGcbbb4V>	Fri 10:18 AM
Order-Pending(1) We Need Your Confirmation To Ship Your Order  . EXPRESS	Fri 7:23 AM
-Currys Rewards- You have won an Makita Power Drill ANSWER & WIN A Brand New Makita Power Drill Congratulations You have been chosen to participate in	Fri 6:52 AM
Congratulations Re: Your Name Came Up For a AirPods customer Gift Re: 2nd attempt for you <https://t.co/crtNBw39lu>	Fri 2:28 AM
-Currys Rewards- You have won an Makita Power Drill	Thu 12:32 PM

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)

'--have i been pwned?

Check if your email or phone is in a data breach

655

pwned websites

12,465,082,651

pwned accounts

115,645

pastes

227,268,534

paste accounts

Largest breaches



772,904,991 [Collection #1 accounts](#)



763,117,241 [Verifications.io accounts](#)



711,477,622 [Onliner Spambot accounts](#)



622,161,052 [Data Enrichment Exposure From PDL Customer accounts](#)



593,427,119 [Exploit.In accounts](#)



509,458,528 [Facebook accounts](#)



457,962,538 [Anti Public Combo List accounts](#)



393,430,309 [River City Media Spam List accounts](#)

myspace

359,420,698 [MySpace accounts](#)



268,765,495 [Wattpad accounts](#)

Recently added breaches



1,117,405 [Weee accounts](#)



23,348 [LimeVPN accounts](#)



8,159,573 [Truth Finder accounts](#)



11,943,887 [Instant Checkmate accounts](#)



18,850 [School District 42 accounts](#)



240,488 [Planet Ice accounts](#)



139,401 [KomplettFritid accounts](#)



20,032 [Autotrader accounts](#)



756,737 [Zurich accounts](#)



367,476 [DoorDash accounts](#)

www.haveibeenpwned.com

- Reputable and can check if your email has been found in data breaches
- You are correct to be suspicious of entering your information anywhere so consider this completely optional
- Run by a single individual, Troy Hunt, who is well-known in the cybersecurity field
- More info here: <https://haveibeenpwned.com/About>



PART 1: THE STATE OF SCAMMING IN 2023

- A word or two about 'hacking'...
 - Hacking is the process of compromising digital platforms, devices, storage mediums...
 - It is often NOT an elegant and sophisticated process but can often be quite simple:
 - Using the email address that was discovered through spamming
 - Combined with the pet name & birthday found on Facebook
 - The common characters people use
 - Information from a leak you heard about in the news
 - OR the scammer was allowed remote access onto the computer, which is among the worst

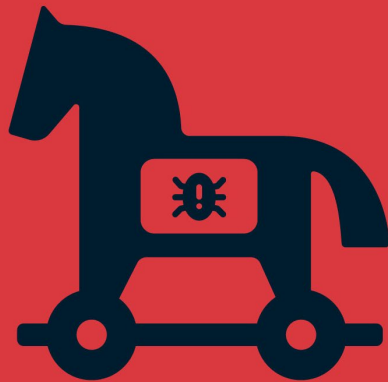
PART 1: THE STATE OF SCAMMING IN 2023

- Have you ever heard of 'ethical hacking'?
 - "Certified Ethical Hacker" is a certificate you can attain
 - Black, grey and white hat hackers
 - Grey, Red, Blue, Green, 'Script Kiddies', hacktivists, state-sponsored



The takeaway: There is not one kind of hacker, they are people with different motives and objectives and they are often at odds with one another. There is a 'good' and 'bad' and 'somewhere in between'.

PART 1: THE STATE OF SCAMMING IN 2023



- Some of the ways scammers/hackers can collect your information through your computer:
 - Malware
 - Spam and e-mail
 - Key loggers
 - Viruses
 - Trojans
 - Fake online surveys asking for personal info (street you grew up on, name of first pet, etc.)

PART 1: THE STATE OF SCAMMING IN 2023

- Information is bought, sold and traded
 - It is not always an individual scammer, but a group/organization or multiple and completely different groups sharing the same information (DRP Presentation)
- What about those telephone scammers?
 - Masking their phone numbers to look local
 - Can detect if phone was picked up
 - Record information over time with different attempts
 - Advice: Do not engage whatsoever, do not taunt, just ignore them



PART 1: THE STATE OF SCAMMING IN 2023

- Why aren't the big telecommunication companies doing more about this?
 - No, honestly, I would like to know, but I can speculate
 - I have some information from someone who sounds knowledgeable
 - [LINK HERE](#)
 - Concept of the "POTS" or "Plain Old Telephone System"
 - Not economical, copper cable infrastructure can't track these calls, lack of resources, scammers keep on top of anything they try (call control, etc.). Supposedly the answer is complicated...
 - It is widely thought that for the international centres either the authorities turn a blind eye or they are intermingled with legitimate businesses – needle in a haystack

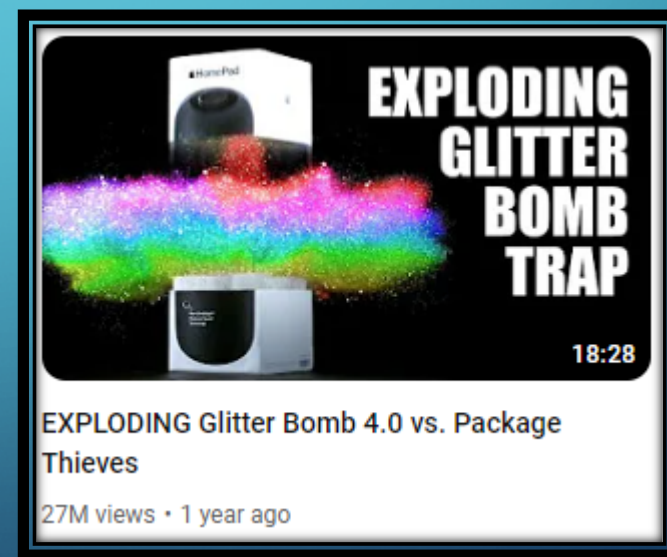


PART 1: THE STATE OF SCAMMING IN 2023

- Do not take it upon yourself to “scambait” or seek revenge or antagonize
- There are scammer payback channels if you want to see some payback

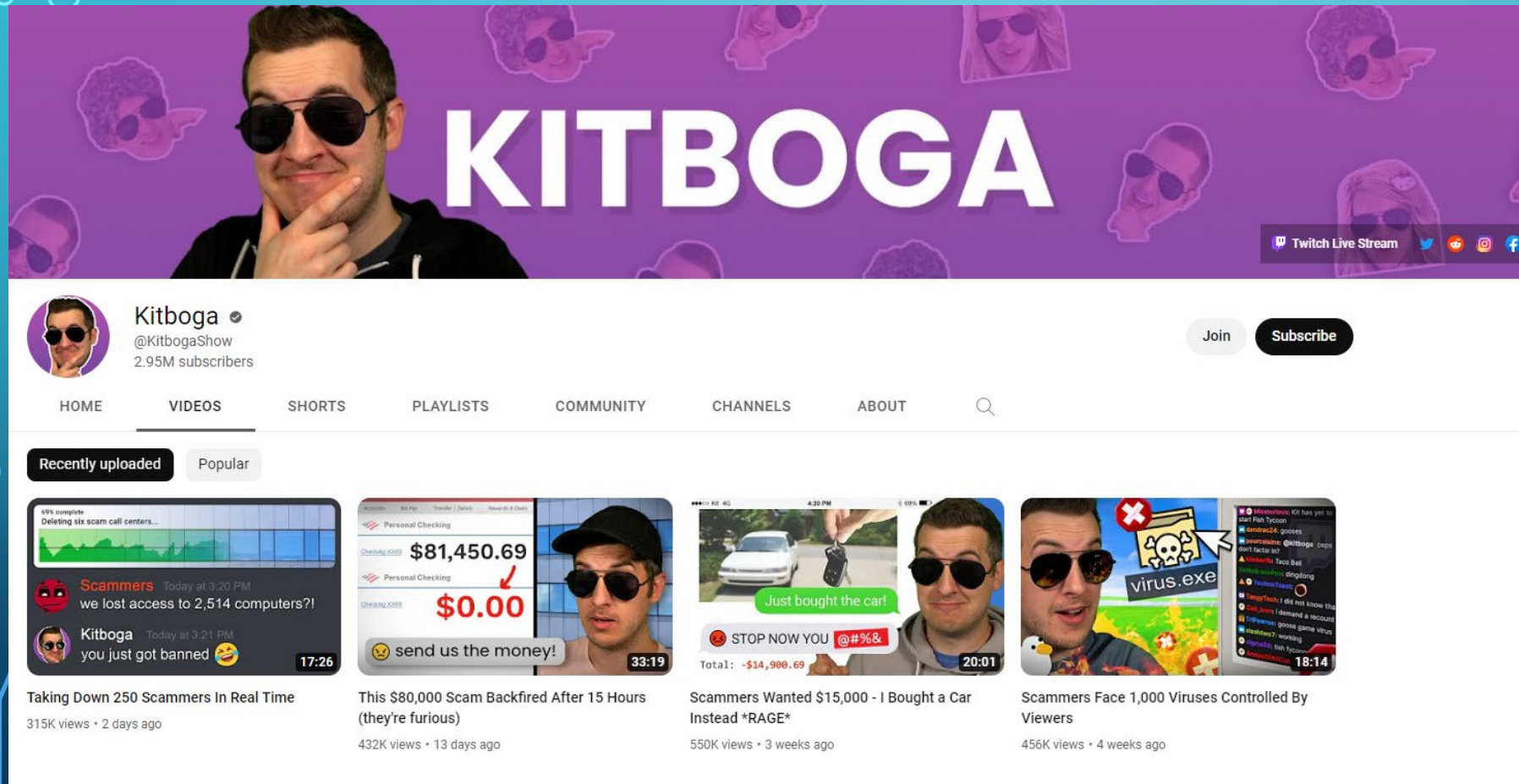


Scammer Payback



Mark Rober

- A story I read about yesterday (Feb 21st) about AnyDesk (a remote-access application company) helping an anti-scammer ban scam accounts



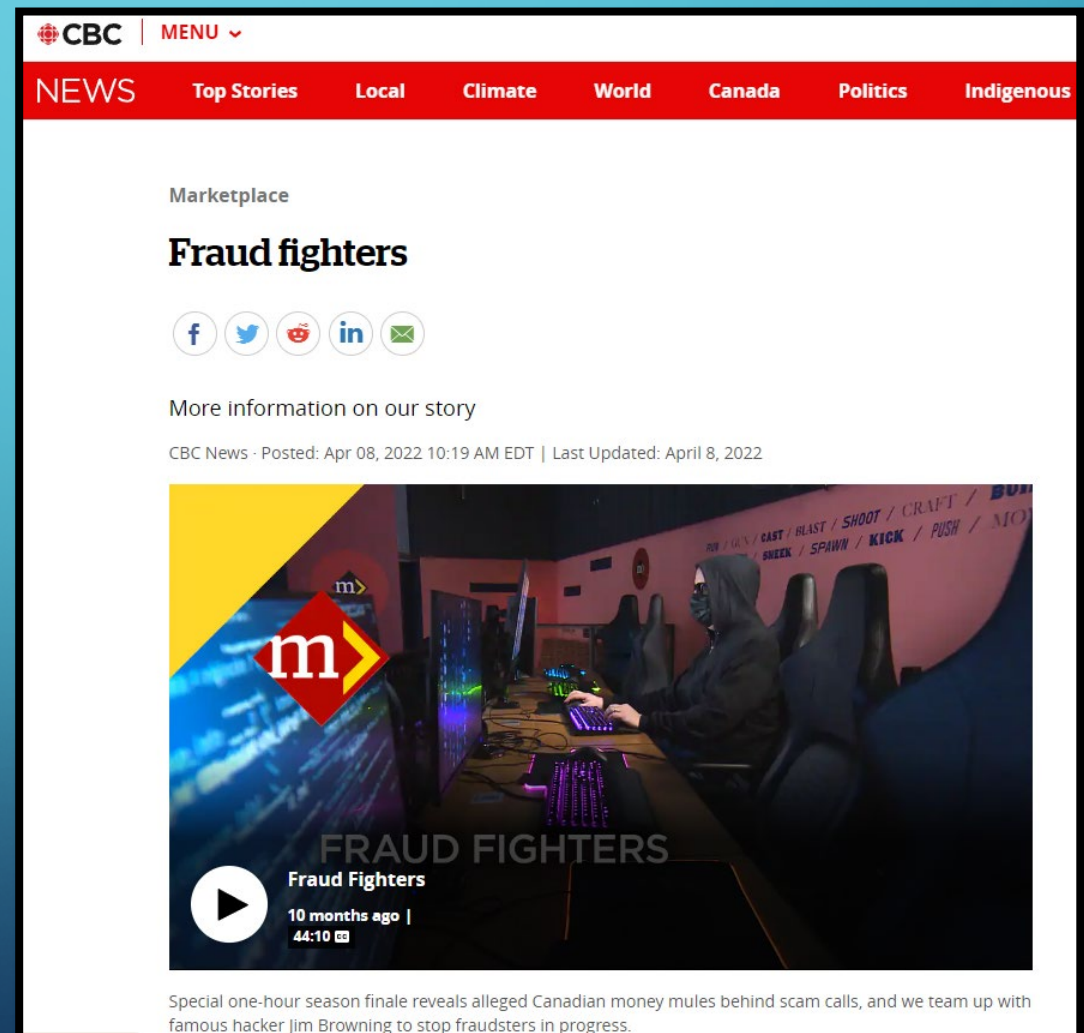
[LINK TO VIDEO](#)

[LINK TO REDDIT](#)

PART 1: THE STATE OF SCAMMING IN 2023

An excellent, short and recent
CBC Marketplace documentary.

“Fraud Fighters” - [LINK](#)



PART 2: COMMON SCAMS & CASE STUDIES

- Okay, that's plenty of background. What about something practical?



PART 2: COMMON SCAMS & CASE STUDIES

Is Your Credit Card Stolen? Check for free! +

Free! Check if your credit card has been stolen!

If you fear your credit card info has been stolen, enter it here and you can find out for **free**. Avoiding fraud has never been easier!



[About](#)

Credit card issuer

Credit card number

Name on credit card

Expiration Date /

 Verified Secure 

Advice: Ignore this, using common sense. No company, service or bank would utilize a tool like this.

PART 2: COMMON SCAMS & CASE STUDIES

Work



Work Email <workemail9876543210@gmail.com>

To

[Redacted]

Follow up.



5FC99766-93B0-4B75-8A44-502968881F9B.jpeg
3 MB



Reply

Reply All

Forward



Thu 2023-01-19 11:37 AM

PART 2: COMMON SCAMS & CASE STUDIES



Advice: The beginnings of phishing – they are expecting a response and will extra information over time.

PART 2: COMMON SCAMS & CASE STUDIES

Please confirm receipt



nespress <communications40a@podescoffier.edu>

To bandarisacoke@gmail.com



← Reply

[⏪ Reply All](#)

→ Forward



Thu 2023-01-05 4:02 AM

i Follow up.

If there are problems with how this message is displayed, [click here to view it in a web browser](#).

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Congratulations!

**You have been selected to participate
in our Loyalty Program!!**

GET YOURS NOW!

[illegible]

WALLPAPER PAINT WALL MURALS WALL ART



PART 2: COMMON SCAMS & CASE STUDIES

Please confirm receipt



nespress <communications40a@podescoffier.edu>

To bandarisacoke@gmail.com



← Reply

 Reply All

→ Forward



Thu 2023-01-05 4:02 AM

i Follow up.

If there are problems with how this message is displayed, [click here to view it in a web browser](#).

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Congratulations!

You have been selected to participate in our Loyalty Program!!

GET YOURS NOW!

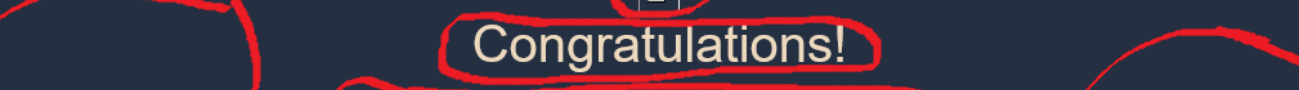
[illegible]

WALLPAPER PAINT WALL MURALS WALL ART

Be careful of buttons, text, links
and especially unsubscribing!!!

The screenshot shows an email interface with a dark blue header. The sender is 'nespress' with a contact email address. The subject is 'Congratulations! You have been selected to participate in our Loyalty Program!!'. The body of the email is mostly blacked out with a large black rectangle. Red annotations highlight several areas: a red circle around the 'Follow up' link; a red circle around the 'Congratulation!' text; a red circle around the 'You have been selected to participate in our Loyalty Program!!' text; a red circle around the 'IT'S YOURS NOW!' button; a red circle around the 'Shop The Collection Now' link; and a red circle around the 'WALLPAPER PAINT WALL MURALS WALL ART' link. The footer contains a long string of text that appears to be a mix of random characters and words, possibly a spam filter or a redaction.

 **nespress** <communications40a@podescoffier.edu>
To: bandarissacoke@gmail.com



Congratulations!

**You have been selected to participate
in our Loyalty Program!!**

GET YOURS NOW:

[WALLPAPER](#) [PAINT](#) [WALL MURALS](#) [WALL ART](#)

Be careful of buttons, text, links
and especially unsubscribing!!!

PART 2: COMMON SCAMS & CASE STUDIES

- There is a great chance you magically won this free ticket in the post! You will have to call a number for a prize, wherein you will either have to register information or have an agent come by your home. Often associated with attempts to get you to purchase home utilities, oddly enough.



PART 2: COMMON SCAMS & CASE STUDIES

- Some scammers are very bold.
 - Telephone call asking if you have a security system...
 - A call pretending to be a relative or grandchild



Advice: Do not engage. Hang up the phone and do not provide any information.

PART 2: COMMON SCAMS & CASE STUDIES

- Amazon charge phone call – press a number to dispute the charge



- These calls may take many forms:
 - Canada Revenue Agency
 - Energy providers
 - Random computer technical support



Advice: Do not engage and use common sense. Find the official contact details for the company and check with them.

PART 2: COMMON SCAMS & CASE STUDIES

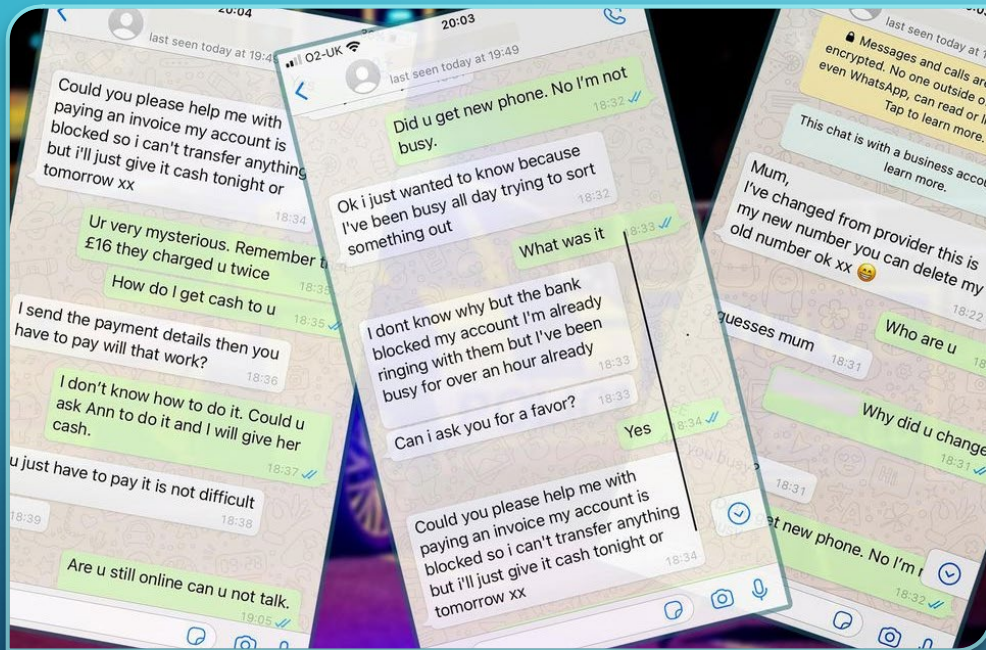
Case study 1: Remote access via TeamViewer (or AnyDesk, etc.)

- Access is voluntarily given by allowing application to be installed or connection to be established
- Once on the scammer obfuscates the view and accesses documents, downloads, personal files, passwords, etc.

Advice: Do not interact. If remote access has happened, disconnect from network, turn off and seek assistance. In this case the best course of action was to back-up personal data and reinstall Windows to be certain.



PART 2: COMMON SCAMS & CASE STUDIES



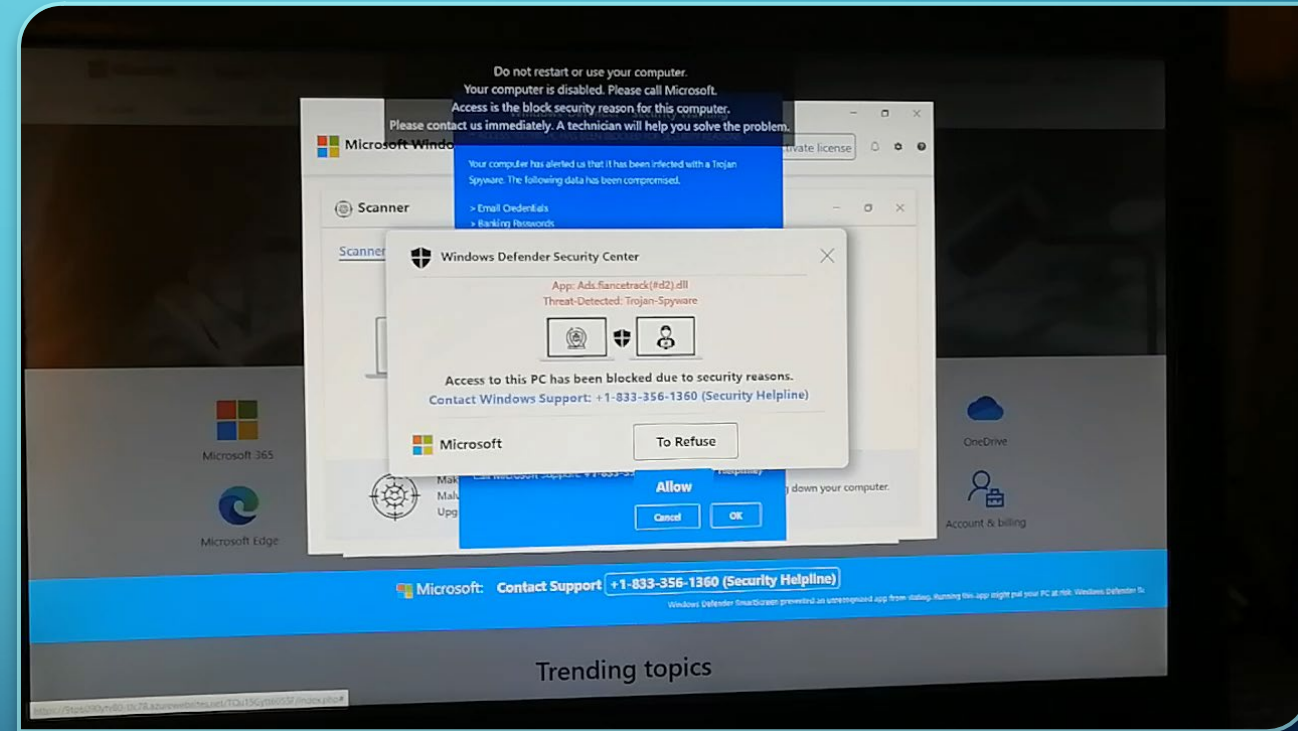
- **Case study 2: Fake Text Scam**

- Text messages from someone claiming to have once known family member with that number and wished the person with the phone number well
- Beginnings of phishing and will lead to extracting information or requesting money

Advice: Do not interact. Ignore or block number. Never send personal information or money. If you have sent bank or login information for anything, check with that company/service and change information.

PART 2: COMMON SCAMS & CASE STUDIES

- **Case study 3: Lockout of a PC through a highly malicious popup/ad**
- Any interaction within the popup can result in being routed to an external URL or more popups are created
- Solution is to hit ESC key and CTRL-ALT-DEL to access Task Manager and kill it from there



Advice: Never call the number, it is NOT Microsoft on the other end. Hit ESC, CTRL + ALT + DEL or seek assistance.

PART 2: COMMON SCAMS & CASE STUDIES

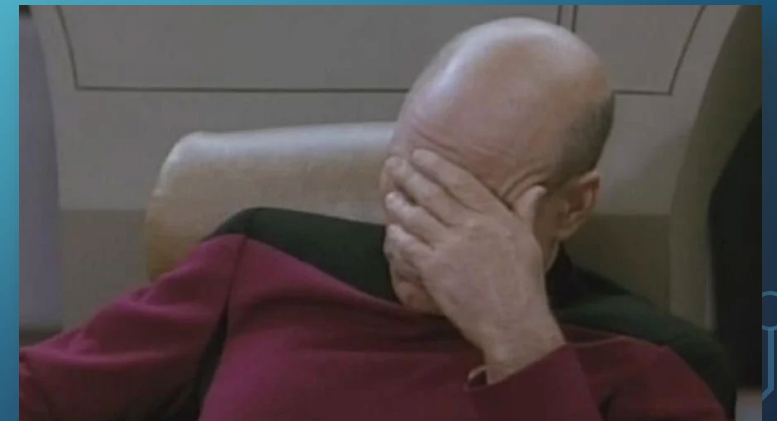
- **Case study 4: Telephone Scammer and Me...**

Intrusive scam call looking for a family member, when I denied them they raised their voice, got very commanding and insistent.

I swore at scammer. They called back and taunted me.

Rang again, I picked it up and it wasn't he scammer...

Embarrassing but I learned a lesson.



Advice: Do NOT engage! Do not 'feed the trolls'. Ignore, add to block list if possible. Hang up on suspicion.

PART 2: COMMON SCAMS & CASE STUDIES



- **Case study 5: Local group's website targeted for 'ransom'**
 - Claim to be holding website for ransom plus impersonation of group member
 - Entirely bogus, no access to anything, this is an attempt to intimidate you into paying or providing information or to trick one member into paying/providing information to the scammer

Advice: Do NOT engage! Do not 'feed the trolls'. Ignore, block email if possible. Inform members of the group.

- **Case study 6:**

Gaming account

‘accidentally’ reported
and may be suspended.

A fake representative is
Provided to speak to and
‘assist’ with the matter

Advice: Ignore these
attempts, block the user
and report this through
Official channels.

The screenshot shows a Steam chat window with a contact named 'Mr. Ethan (Official)'. The chat history includes:

- 12:12: [Redacted] Sorry to disturb you can we talk for just a minute, please? it's a very important matter. If you notice my message please reply this is so important
- 12:12: [Redacted] What's up?
- 12:13: [Redacted] Sorry for disturbing you cause I accidentally report you for doing illegal purchased instead of someone else the admin said your account will be suspended
- 12:13: [Redacted] Huh?
- 12:13: [Redacted] I'm really sorry I tried to tell him that it was a mistake profile ID but he won't listen to me
- 12:13: [Redacted] Who?
- 12:13: [Redacted] I didn't mean to report you, can you please help me to explain to him?
- 12:14: [Redacted] Who?
- 12:14: [Redacted] (typing indicator)

In the middle of the chat, a link is shared for 'Steam Community :: Mr. Ethan (Official)'. The link preview shows a profile picture of a man in a suit with a white bird mask, and text: 'Feel free to ask me for Community Service Security | Services', 'Valve | Steamworks |', and 'STEAMCOMMUNITY.COM'.

Below the link, the chat continues:

- that's him add him and explain that I report you it was accidentally only please help me to clarify on him I don't know what to do if you will get suspended I'm really sorry I didn't mean to report you I hope you are not mad
- 12:15: [Redacted] Hang on. Let me check my status
- 12:15: [Redacted] okay just add him cause his waiting to your request are you talking to him now?
- 12:18: [Redacted] I am chatting with him now.

Red arrows point from text annotations to specific elements in the chat:

- An arrow points from the first message to the annotation: **YOU'LL GET A CHAT REQUEST FROM SOMEONE ON YOUR FRIENDS LIST CLAIMING THEY SCREWED UP**
- An arrow points from the link preview to the annotation: **THIS USER ACCOUNT HAS PROBABLY BEEN STOLEN**
- An arrow points from the link preview to the annotation: **SENDS A LINK TO WHAT IS SUPPOSE TO BE A STEAM REP**
- An arrow points from the final message to the annotation: **THIS IS THE LURE INTO THE TRAP**

PART 2: COMMON SCAMS & CASE STUDIES

It's enough to make your head spin!



PART 3: STRATEGIES TO KEEP YOU SAFE

- It would be nice to think there is a big entity out there with sweeping powers to smother all this out, but at the moment there isn't. We ultimately have to take responsibility for our safety and privacy for ourselves, our families and communities.



PART 3: STRATEGIES TO KEEP YOU SAFE

- Scam awareness in the NRT

December 7th, 2022.

The most popular holiday scams



The spirit of the holidays is a time of giving for most but, for scammers, it is a time of taking. The Canadian Anti-Fraud Centre (CAFC) highlights the most popular holiday scams so that you can recognize, reject, report and be merry.

Online Shopping – Fraudsters pose as genuine sellers and post fake ads for items that do not exist. The listing price for almost any item (e.g., event ticket, rental, vehicle, puppy) is usually too good to be true. Research before you buy. Whenever possible, exchange goods in person or use your credit card for payment.

Phishing Emails and Texts – You may receive messages claiming to be from a recognizable source (e.g., financial institution, telecommunications company, service provider, shipping company, family member or friend) asking you to submit or confirm your information. They may even include a malicious link for you to click.

Secret Santa – You may have noticed multiple gift exchange posts on your social media feeds. This may seem like a fun activity where you only have to send one gift and receive multiples in return. Unfortunately, this exchange collects some of your personal information and also hides a pyramid scheme where only those on the top profit. Pyramid schemes are illegal in Canada. To keep it safe, keep the exchanges to close friends and family and conduct them in person.

Gift Cards – Gift cards are a popular and convenient way to give a gift. They should also be considered like cash; once they are exchanged, it is unlikely that you are getting your money back. Gift cards are not meant for payments and no legitimate business or organization will request these as payments, especially under pressure.

Charity Scams – During the season of giving, make sure your donations are going to the right places. Charity/donation scams involve any false, deceptive, misleading, or fraudulent solicitation for a donation to a charity, association, federation, or religious cause. Refuse high pressure requests for donations, ask for written information about the charity and do your own research. Remember to always ask the solicitor for the charitable tax number and confirm their registration with the Canada Revenue Agency or by phone at 1-800-267-2384.

PART 3: STRATEGIES TO KEEP YOU SAFE

- Scam awareness in the NRT
January 25th, 2023.

“Green energy” scam

The Upper Ottawa Valley detachment of the Ontario Provincial Police (OPP) is warning residents of a potential scam that has been reported in the area.

Police urge residents to beware of individuals going door-to-door offering to conduct an energy assessment to qualify the homeowner for a green energy rebate.

The scammer typically asks to inspect the victim’s furnace and water heater and, once in the home, the individual will use high pressure sales tactics to have the homeowner purchase products and services in order to qualify for a rebate. They may also ask for personal information and banking information, such a void cheque, for the transaction.

Jan. 25,
2023.
NRT

Advice: Be assertive. Say **“NO!”**. Call the police.

PART 3: STRATEGIES TO KEEP YOU SAFE

- Scam awareness on the Deep River Police Facebook page February 7th, 2023.



Marek Brela

3h · 🌐

The Deep River Police Service would like to raise awareness about the significant increase in emergency-grandparent scams targeting Canadian seniors.

In 2022, the CAFC received fraud reports totalling a staggering **\$530 million** in victim losses. This was nearly a 40 per cent increase from the 2021 unprecedented **\$380 million** in losses.

Fraudsters target anyone and everyone, particularly the vulnerable and seniors. In 2022, more than **\$9.2 million** was reported lost to emergency scams, according to the CAFC. This was a drastic increase from **\$2.4 million** in 2021.



👍👍 You and 3 others

2 shares



Like



Comment

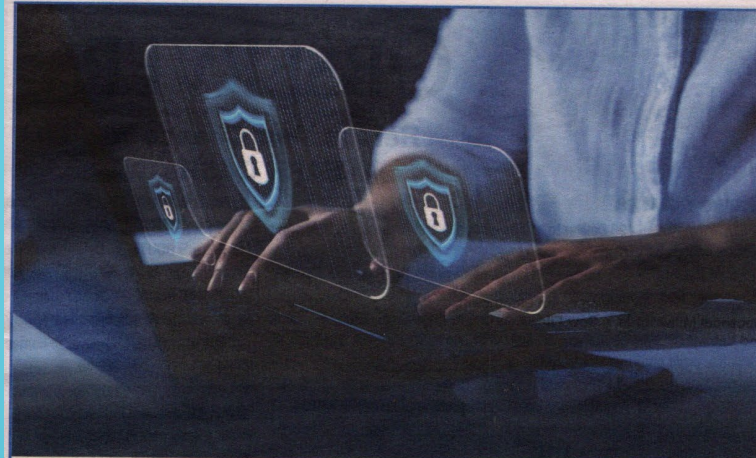


Share

- Fraud awareness in the
Pembroke Observer
February 16th, 2023.

Thursday, Feb. 16

PEMBROKE OBSERVER AND NEWS



Invest in YOUR future.

Fraudsters are out there every day looking for victims. They will target you online, over the phone, by mail or in person.

Watch for these WARNING SIGNS in an online relationship:

- When someone you met and only communicate with online professes their love to you
- If the person wants to quickly move to a private or different mode of communication (email, text, Whatsapp, Google Hangouts etc.)
- If they always have an excuse not to meet in person
- If you receive poorly/oddly written messages, sometimes even addressing you by the wrong name
- If the individual claims to live close to you but is working overseas
- If they act distressed or angry to guilt you into sending money
- Beware if the individual wants you to keep the relationship a secret. A secret relationship is not a healthy relationship.

For more info or support,

contact your local OPP, Victim Services of Renfrew County at 1.877.568.5730, Older Adult Protection Services at 1.800.363.7222 or the Canadian Anti-Fraud Centre at www.antifraudcentre.ca

You work hard for your money. You deserve to invest in YOUR future – not a fraudsters'.

This message is brought to you by the Upper Ottawa Valley OPP and Victim Services of Renfrew County Inc through funding by the Safer and Vital Communities Grant Fund





Hello,

Stay safe from scammers this holiday season by getting to know their most common scams:

- **Order confirmation scams.** These are unexpected calls/texts/emails that often refer to an unauthorized purchase and ask you to act urgently to confirm or cancel the purchase. These scammers try to convince you to provide payment or bank account information, install software to your computer/device, or purchase gift cards.

Remember, if you received correspondence regarding an order you weren't expecting, you can verify orders by logging into your Amazon account. Only legitimate purchases will appear in your order history - and Customer Service is available 24/7 to assist.

- **Tech support scams.** Scammers create fake websites claiming to provide tech support for your devices and Amazon services. Customers who land on these pages are lured to contact the scammer and fall prey to their schemes.

Remember, go directly to the help section of our website when seeking help with Amazon devices or services. If you do use a search engine, use caution. Legitimate Amazon websites contain "amazon.ca" such as "help.amazon.ca".

Here are some important tips so that you can identify scams and keep your account and information safe:

1. **Trust Amazon-owned channels.** Always go through the Amazon mobile app or website when seeking customer service, tech support, or when looking to make changes to your account.
2. **Be wary of false urgency.** Scammers may try to create a sense of urgency to persuade you to do what they're asking. Be wary any time someone tries to convince you that you must act now.
3. **Never pay over the phone.** Amazon will never ask you to provide payment information, including gift cards (or "verification cards", as some scammers call them) for products or services over the phone.

If you receive correspondence you think may not be from Amazon, please [report it to us](#). For more information on how to stay safe online, visit Security & Privacy on the Amazon Customer Service page.

Additional resources:

- [Tips to determine](#) if an email, phone call, text message, or webpage is really from Amazon.
- Amazon offers [Cybersecurity Awareness Training](#) free to individuals and businesses around the world.
- If you're concerned about your account security, go to [Protect Your System](#) for tips and recommendations.

Sincerely,
Amazon

PART 3: STRATEGIES TO KEEP YOU SAFE

- From Amazon recently
about scams involving them

PART 3: STRATEGIES TO KEEP YOU SAFE

- What to do if you are a victim?

WHAT TO DO IF YOU'RE THE VICTIM

1

Stay calm. Gather all documents and information about the fraud

2

Contact your financial institutions – place flags on your accounts and change all your passwords

3

Contact Equifax and TransUnion

4

Report the Fraud to the police

5

Report the Fraud to the Canadian Anti-Fraud Centre



PART 3: STRATEGIES TO KEEP YOU SAFE

- What to do if you are a victim?

Resources & Phone Numbers

Deep River Police Service – Non Emergency 613-584-3500

Canadian Anti-Fraud Centre – Toll Free 1-888-495-8501

www.antifraudcentre-centreantifraude.ca

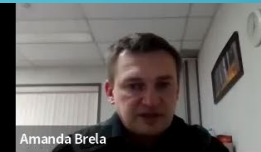
Equifax – www.consumer.Equifax.ca/personal/

TransUnion – www.transunion.ca

Service Canada – 1-866-274-6627

Canada Revenue Agency – 1-800-959-8281

Get Cyber Safe – www.getcybersafe.gc.ca/en/secure-your-accounts



Protect Online Information



- *Control physical access* to your electronic devices – computers, tablets and smart phones. Take appropriate measures to prevent unauthorized persons from using them.
- If you are using a device and need to walk away from it for any reason, *log off or lock the device*.
- *Select passwords that would be difficult for others to guess and change them frequently*. Use a combination of upper and lower case letters, numbers and special characters.
- *Do not give out your password to anyone*. Do not save passwords on a website or leave written notes with your password information. If you have a lot of password consider using a password vault, like LastPass or Norton Password Manager
- Public computers and other devices may not have appropriate security controls and could be compromised. These include Internet cafes, computer labs, shared systems, kiosk systems, conferences, and airport lounges. Only use these computers for anonymous Internet browsing preferably over VPN (Virtual Private Network) connection.
- *Use your online accounts at least every month* to check balances and activity.
- *Always log off* your business or personal Internet banking application when you are done.
- Do not respond to or follow instructions from unusual e-mail or text messages. Many frauds are started by messages with a fake "From:" address. Do not assume a message is legitimate solely based on the "From:" address.

Protect Your Devices – Computers, Tablets and Smart



- Install virus management software on your devices and scan them regularly.
- Keep your virus files up to date (i.e., latest signature files, product upgrades).
- Install a firewall to protect each computer or a home router that includes a firewall to protect your home network.
- Keep your devices up to date with current security patches. Set up your devices to automatically install patches so you don't have to remember. Note: Windows 7 has reached end of life and is no longer supported. If you are still using it, consider upgrading.
- Be cautious when downloading and running programs or Java or ActiveX applets as they may contain unsecure data which cannot be filtered, for example, using firewall or anti-virus software. Only download from a trusted site.
- Use extreme caution when opening email received from unknown sources and pay special attention to any attachments. Do not launch or open an attachment from an unknown source. When in doubt, delete the email without opening it.

PART 3: STRATEGIES TO KEEP YOU SAFE

- What practical steps can I take to keep safe online?



- Use two-factor authentication wherever you can (phone number, e-mail, SMS, mobile app)
- Use a VPN – We leave traces as we navigate the Internet. It may slow your connection down, but it acts as an intermediary and can help protect you from being targeted
- Use dedicated antivirus – There are many options out there, among the most popular are Norton 360 Deluxe, McAfee, Bitdefender, Avast, Panda, Malwarebytes. Windows Defender is good if you are careful enough and it technically the most widely used
- If you have an Apple device, they are less susceptible to malware/viruses but not immune
 - Built-in XProtect is often enough if you're careful, but you can get third-party software

PART 3: STRATEGIES TO KEEP YOU SAFE



- What practical steps can I take to keep safe online?

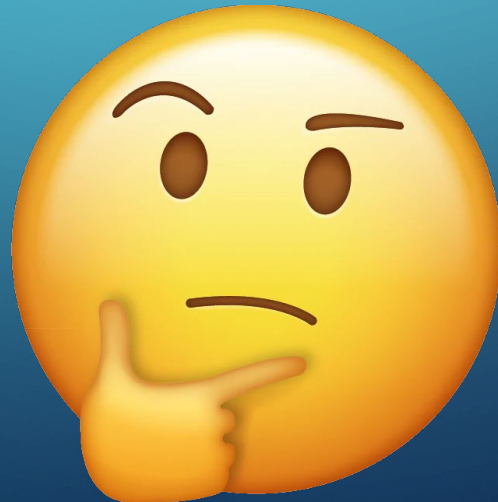


- Have a secondary email address – For when you must register to websites and as backup
- Consider using AdBlock – it will block most forms of advertising online which is a bit of a moral dilemma in some cases, but it may block some nasty ads/popups as well
- If your PC is on Windows 7 or 8, update to 10 or 11 for security
- Be aware of what is in your Documents and Downloads folder – they are often a target
- Use a form of backup for your computer – either external HDD or cloud backup
- Keep informed – Like with the Cybersecurity workshop shared within the group



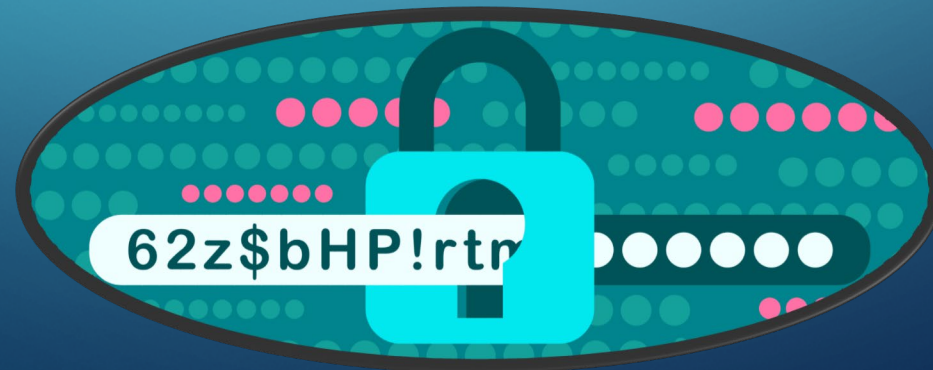
PART 3: STRATEGIES TO KEEP YOU SAFE

- Be careful of:
 - Anything that asks you to install a browser extension – make sure you know what it is
 - Any attachments to an email – familiarize yourself with file formats (e.g. .txt, .jpg, .doc, etc.)
 - How much information you divulge when registering to a website
 - Installing any program, especially if not from a reputable source
 - Listen to your gut and trust your instincts – if something feels off, don't be afraid to disengage



PART 3: STRATEGIES TO KEEP YOU SAFE

- A note on passwords:
 - Passwords are among the most important and most troublesome aspects of being online
 - Use a different password for each login and write it down manually in a book
 - Or use a password manager application. Some options include:
 - Bitwarden, 1Password, Dashlane, Keeper, Nordpass, Norton – there are many others
 - Some are integrated into browsers – if you are using this & should be behind a password
 - Do NOT use the same password, or simple passwords, across multiple sites



PART 3: STRATEGIES TO KEEP YOU SAFE

- What can I do about telephone scammers?
 - Call display has become a necessity but be wary even if it shows it is a local number
 - Call control options (Bell)
 - You can call their tech support for information on setup if you have this feature
 - Complain to your service provider
 - Robokiller for mobile phones
 - Do not engage, do not divulge information, do not seek to confront them, in short:



HOW WAS I SCAMMED?

- Phishing, a long time ago

Fool me once...

Support

iCloud account limited for security reasons

To:



Dear Customer,

We've noticed that some of your account information appears to be missing or incorrect, to avoid the closure of your account please sign in to your Apple ID and securely amend the information in your account. If we don't receive the information before this deadline, we will be forced to disable your account for security reasons. Please amend your account information by clicking on the link below :

[Sign In and Review](#)

Note:

If your account is disabled you will not be able to use your iCloud to unlock your iPhone or be able to use any of the iCloud or App Store features.

Thank you for your patience and understanding. If you need further assistance please click Help at the bottom of Apple page.

Sincerely,

Apple Inc.

This is an automatically generated email. Please do not reply
Read our privacy policy, Security and Protection if you have any questions
Copyright © 1999-2019 Apple Inc All Rights Reserved.

CONCLUSION

- If it's an email, just delete it.
- If it's a phone call, just hang up. Don't speak and don't engage. Ask your phone company for what preventative measures they may have for you.
- If you receive a threat, tell the police.
- Do not let anyone access your devices that you do not trust.
- If your computer has been compromised, ask for help.
- If it's too good to be true online, it almost certainly is.
- Stand your ground and say, "NO!"



THANK YOU!

