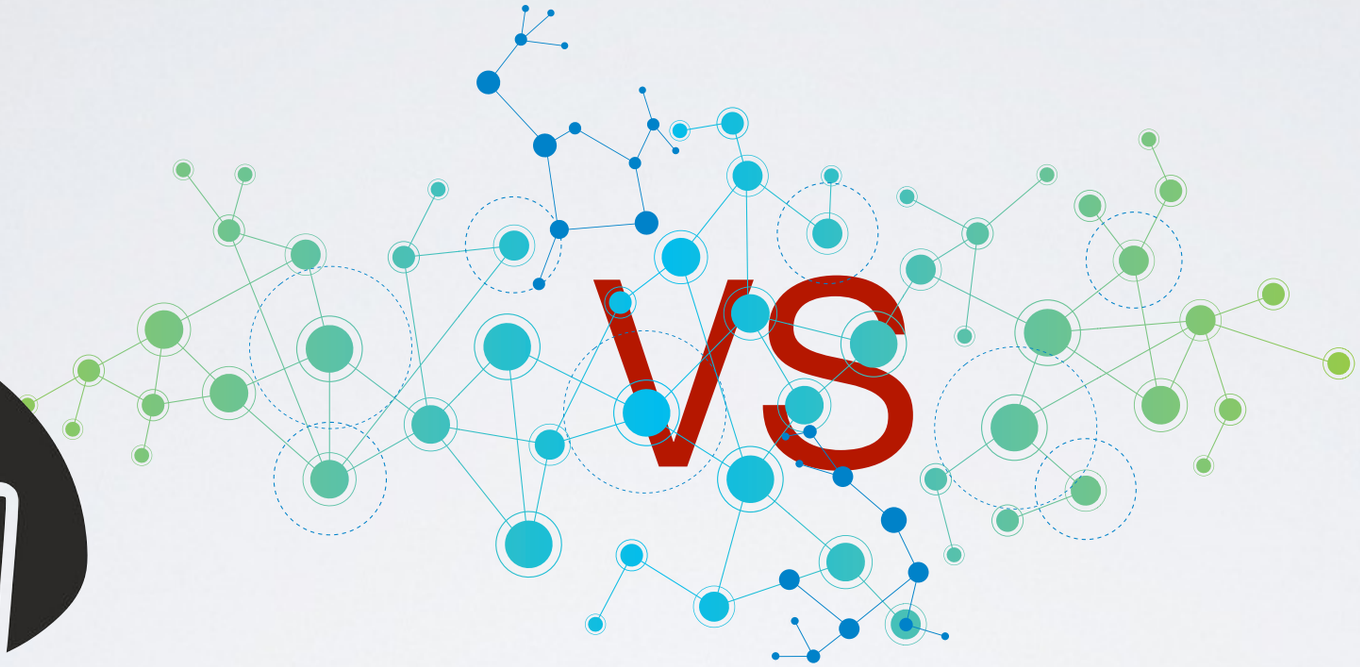
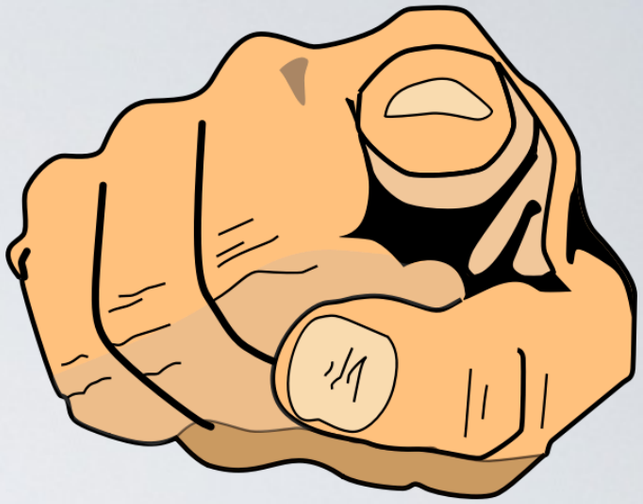
Human Insecurity

Kc Udonsi


VS




TOP SECRET
CONFIDENTIAL
TOP SECRET

Threats humans face in cyberspace

- Credential theft
- Identity/PII theft, Impersonation, Account takeover
- Cyber bullying, extortion, stalking
- Online scams e.g moving, job hunt, cheque, delivery etc
- Digital bank fraud, etc

What enables these ? …

➡ **Poorly managed personal digital assets and technology (Bad cyber-hygiene)**

- Use of unsecured/weakly secured networks
- Insecure default router, IoT configuration
- Over sharing (incl. shared devices)
- Weak / no credentials

➡ **Lack of education / awareness**

Data / Digital Asset Theft

Credentials, Identity, PII, account takeover

How do cybercriminals steal your data?

➡ Social Engineering

The act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques - Wikipedia

- Phishing
- Vishing
- Smishing
- Email compromise

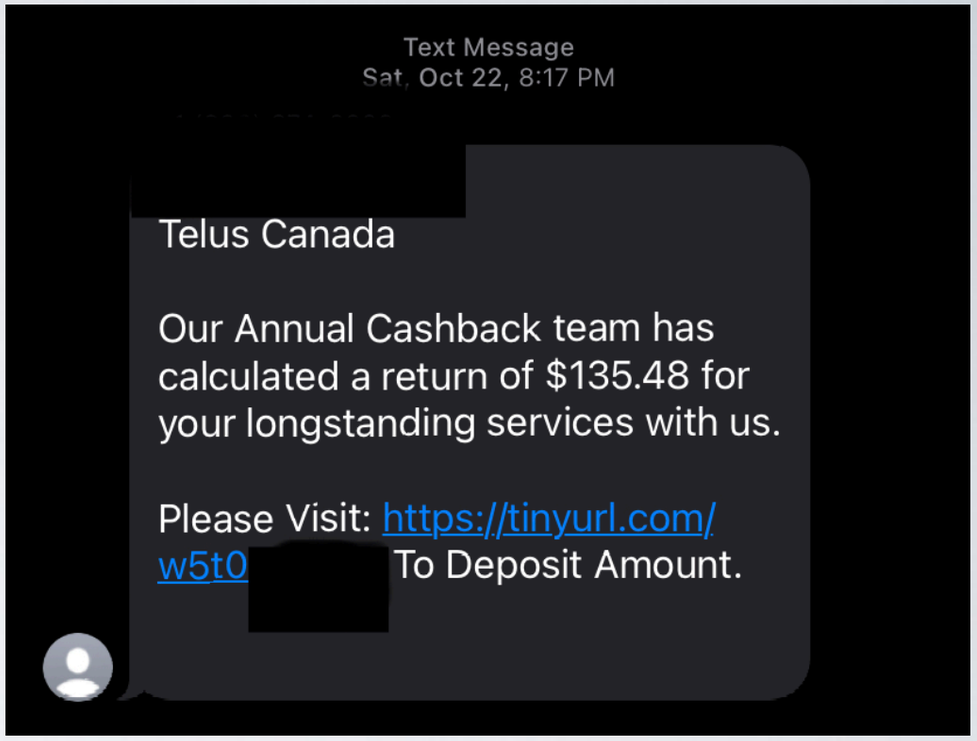
- **Phishing**
  The criminally fraudulent process of attempting to acquire sensitive information […] by masquerading as a trustworthy entity in an electronic communication e.g emails - Wikipedia

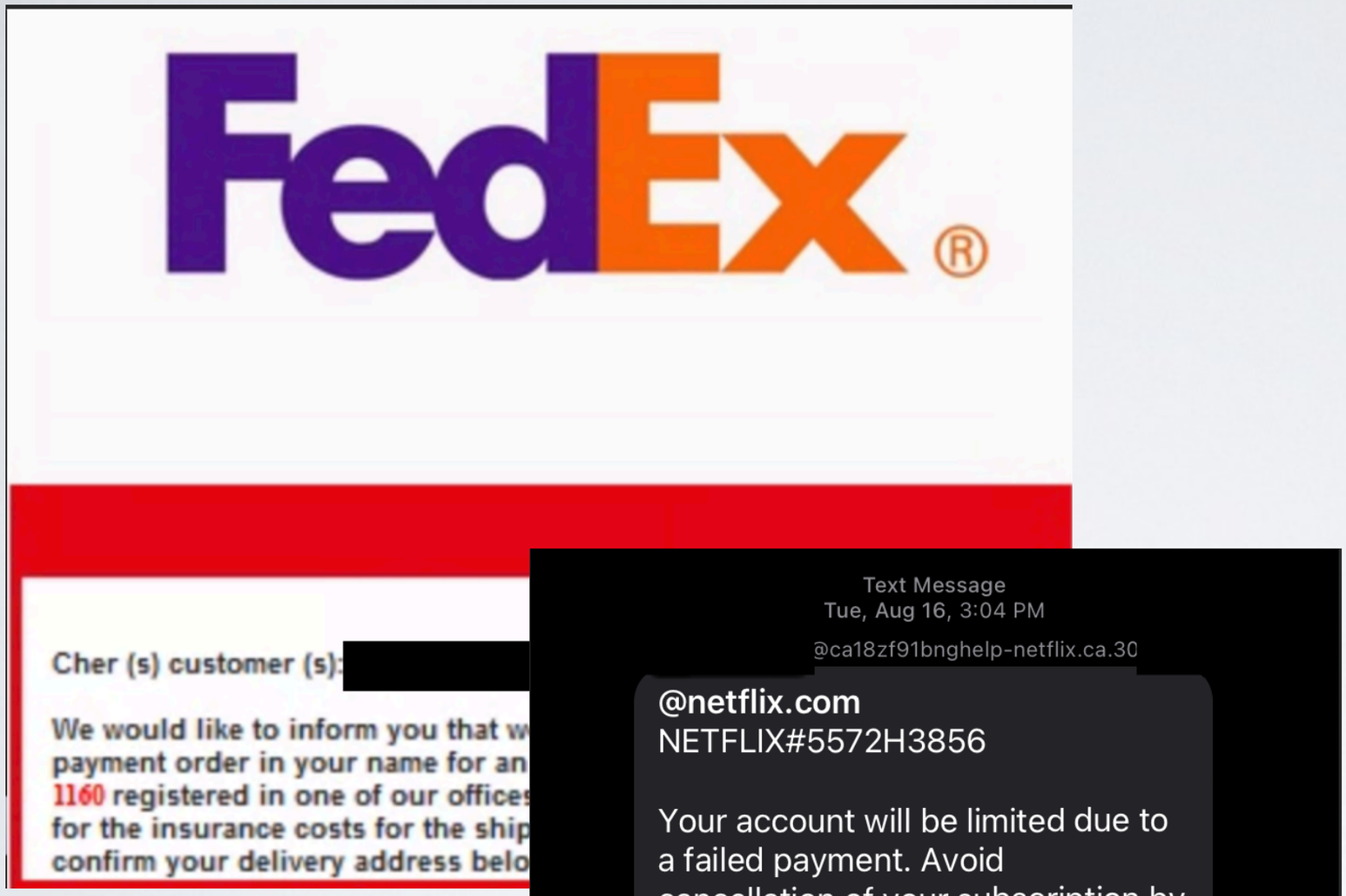
- **Smishing**
  Phishing over SMS or direct message

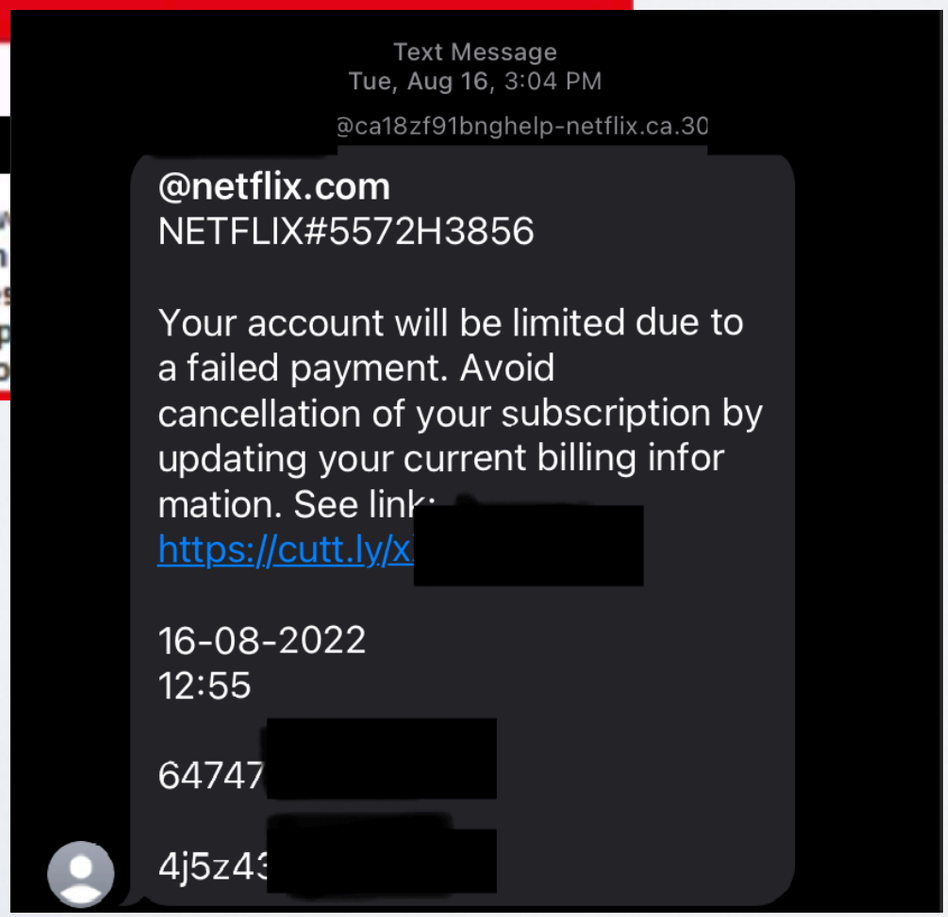
- **Vishing**
  Phishing over voice calls (voice-phishing)

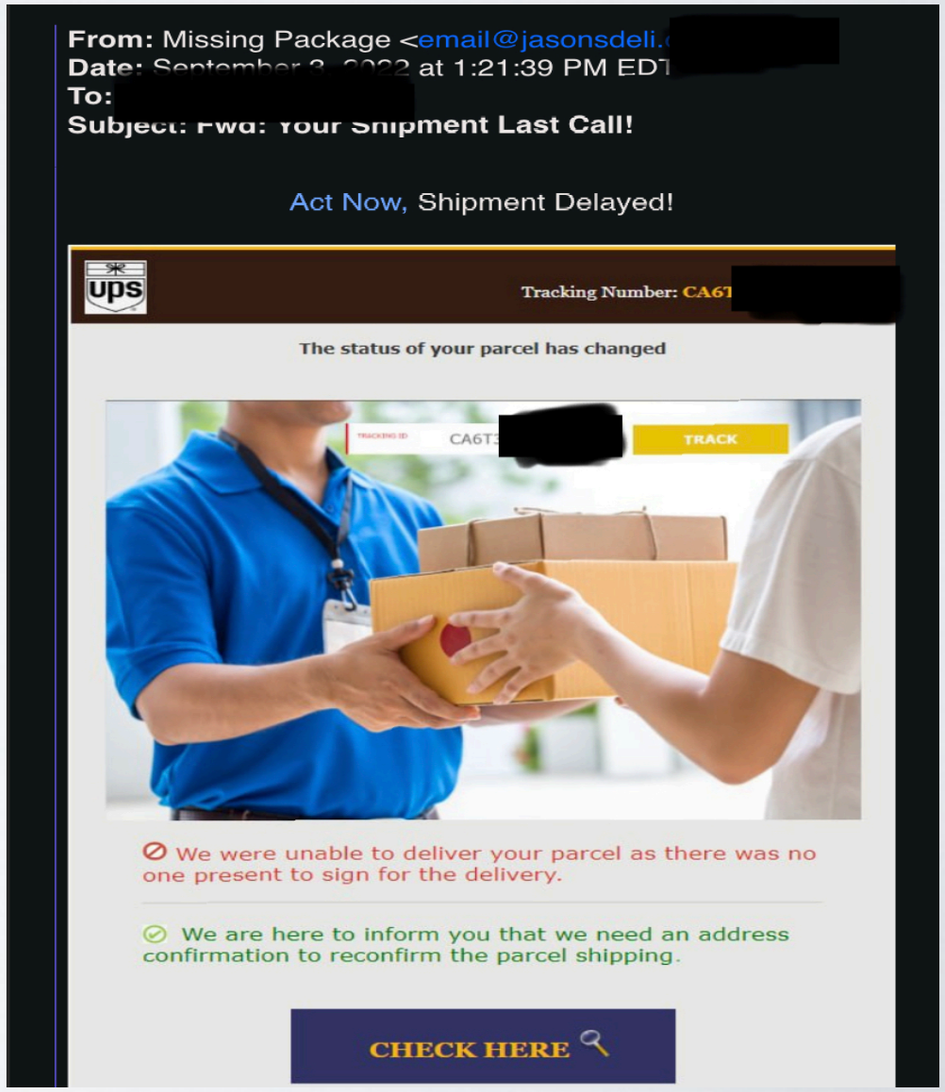
- **Email account compromise**
  Fraudulent email impersonating a known source making a seemingly legitimate request usually involving finance

Examples


Text Message
Sat, Oct 22, 8:17 PM
Telus Canada
Our Annual Cashback team has calculated a return of $135.48 for your longstanding services with us.
Please Visit: https://tinyurl.com/w5t0 To Deposit Amount.


FedEx
Cher (s) customer (s):
We would like to inform you that w
payment order in your name for an
1160 registered in one of our office
for the insurance costs for the ship
confirm your delivery address belo


Text Message
Tue, Aug 16, 3:04 PM
@ca18zf91bnghelp-netflix.ca.30
@netflix.com
NETFLIX#5572H3856
Your account will be limited due to a failed payment. Avoid cancellation of your subscription by updating your current billing infor mation. See link
https://cutt.ly/x
16-08-2022
12:55
64747
4j5z43


From: Missing Package <email@jasonsdeli.
Date: September 3, 2022 at 1:21:39 PM EDT
To:
Subject: Fwd: Your Shipment Last Call!
Act Now, Shipment Delayed!
ups
Tracking Number: CA61
The status of your parcel has changed
TRACK
We were unable to deliver your parcel as there was no one present to sign for the delivery.
We are here to inform you that we need an address confirmation to reconfirm the parcel shipping.
CHECK HERE

Hmm that's suspicious …

Case studies

Case study 1: Fake employment 2020

- Attacker impersonating known Toronto company
- Offer letter includes image of CEO signature
- Follow up email conversation suggests further conversation over Telegram
- Telegram conversation requests banking information for payroll, address and govt. ID for verification and work from home resources

Case study 1: Fake employment 2020 contd.

- Telegram conversation instructs victim to send code received via SMS

- Turns out, attacker was setting up crypto account using victims identity

- Communicated with impersonated corporation and crypto corp to revert attacker activities

Case study 1: Fake employment 2020 contd.

Regards,

Name: _____

Date: _____

CORPORATION Inbox ×

CORPORATION

to me

Hello /

Proceed with adding your Supervisor/Home Office Setup/Training Specialist on Telegram via this link https://t.me/or ha and introduce yourself immediately.

We have received your signed copy of the Employment Contract and will like to say Congratulations on your New Employment with us.

The Management welcomes you into our World of career building opportunities and growth.

Regards,
Gerry Sc

Toronto,Ontario
Canada

Properties

General | Security | Details | Previous Versions

Property	Value
Title	Untitled-1
Subject	
Tags	
Categories	
Comments	

Origin

Authors	PAPA
Last saved by	DELL PC
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	2020-11-12 9:19 AM

steps before you start trading.

Mobile Phone

All About You

Verification

Verify your account

Before you can start trading, we'll need some details.
The verification of this information is required by law.

Items Needed

MOBILE NUMBER

UTILITY BILL OR BANK STATEMENT

GOVERNMENT ID

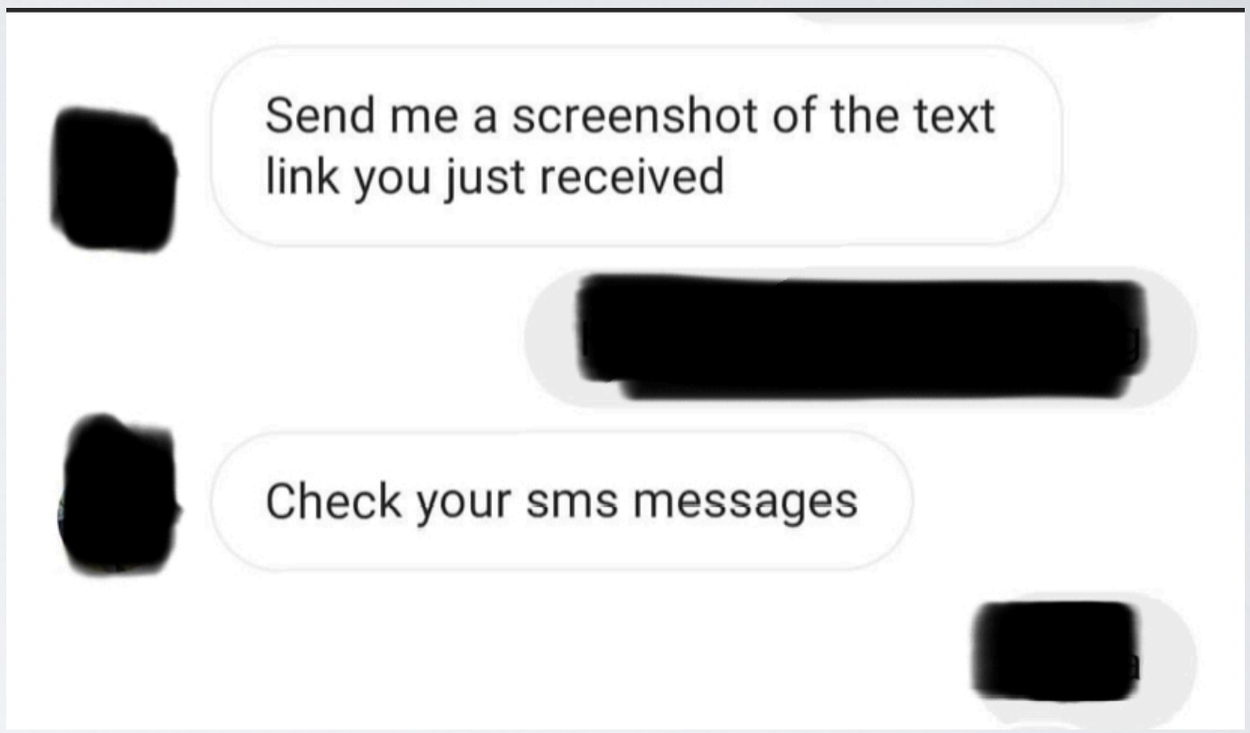
Case study 1: Fake employment 2020 Lessons.

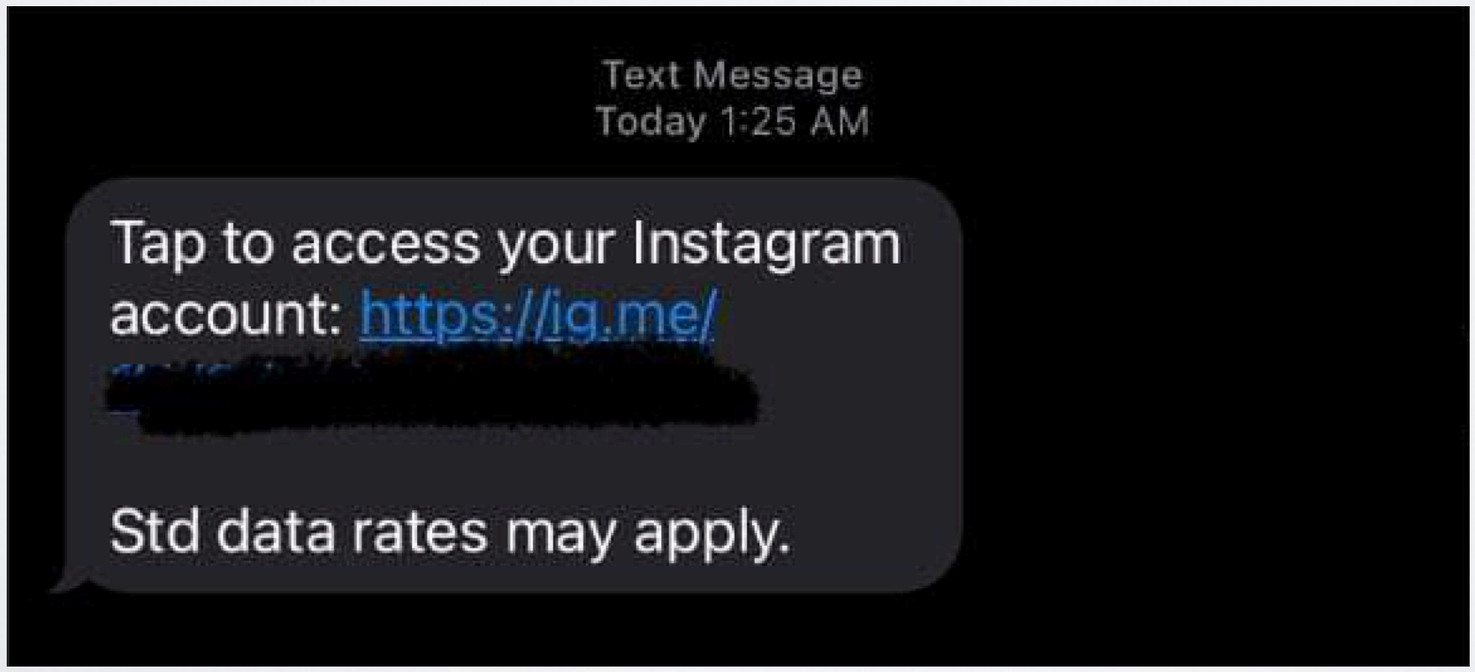
- Attacker leveraged desperate job search
- Attacker leverage publicly available information of corp executives such as names, job roles and signatures
- Victim was unaware of adversarial tactics such as phishing and the dangers of sharing one time codes

Case study II: Instagram account takeover

- Attacker impersonates previously compromised victim's buddy
- Attack suggests victim to vote for buddy in an ongoing election
- If victim indicates interest, attacker instructs victim to send link received in SMS
- Naive victim sends link from SMS to impersonated buddy
- Attacker logs into victim's account, resets email and enables MFA

Case study II: Instagram account takeover





Case study II: Instagram account takeover. Lessons

- Attacker leverages circle of trust. Unsuspecting victim trust's buddy
- Victim was unaware of adversarial tactics such as phishing
- Victim felt "off" but fell prey due to blind trust. It wasn't unusual for buddy to have victim's cell number
- **Fun fact:** SMS was sent by Instagram!
- SMS link is password reset link from as shortened URL

Cyber Harassment

Bullying, Extortion, Stalking

Forms of Harassment

- Sending mean or threatening electronic communication
- Posting or threatening to post embarrassing or demeaning photos of or about someone online
- Impersonation
- Coercing someone to disclose demeaning or embarrassing content about themselves
- Sharing someone else's PII without their explicit and informed consent

Scams and Fraud

Bullying, Extortion, Stalking

Forms of Scam and Fraud

- Frantic calls impersonating authorities or companies claiming fines and fees or "urgent" messages
- Suggesting over-payment in cheque and requesting victim to forward payment
- Fake dating sites and online relationships soliciting sexual content via streaming
- "Congratulations you have [won | been selected | …]"
- Discounted vacation.

Forms of Scam and Fraud

Prepaid cards, bitcoin, e-transfers payments

The Government of Canada will not demand immediate payment by Interac e-transfer, bitcoin, prepaid credit cards or gift cards.

If you are sure you owe the Government of Canada money, there are accepted methods of payment. For example, the Canada Revenue Agency has a Payment options for individuals and businesses page that lists accepted payment methods.

- If it's too good to be true or invoking heightened emotional response. Pause it's probably scam/fraud. Report it
- https://antifraudcentre-centreantifraude.ca/index-eng.htm

Techniques of the trade

- **Open Source Intelligence**
  Qualitative and quantitative methodology for gathering and analyzing data accessible in publicly available domains for intelligence purposes.

- **Google Hacking / Dorking**
  Advanced use of Google query engine to discover poorly configured and unsecured digital assets e.g surveillance cams.

- **Darkweb**
  Exchange of stolen information, expert consultancy and kit services often including customer support

Techniques of the trade contd.

- **Pretexting**
  Calls or texts meant to improve the perceived legitimacy of a phishing attack

- **Cybersquatting/Typosquatting**
  Registering of domains often mistyped by users in other to divert them to an impersonating malicious site.

- **Malware**
  Often delivered by drive by downloads, trojans, email attachment, fake job interview challenges etc.

Resources

- Get Cyber Safe - Phishing: https://www.getcybersafe.gc.ca/en/phishing
- Canadian Anti-Fraud Centre: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
- TrendMicro Free home tools: https://experience.trendmicro.com/?utm_source=onlinescan
- TrendMicro Scam News: https://news.trendmicro.com/category/scam/