

CSS Shared Resources, Ontario East
Privacy & Cyber safety 😊



Ultra Advanced Cyber Security Awareness Training



Land Acknowledgment



Disclaimer



The content of this presentation should not be considered a legal opinion. It is based on extensive research of publically available materials. If you need legal advice, please refer to your counsel.

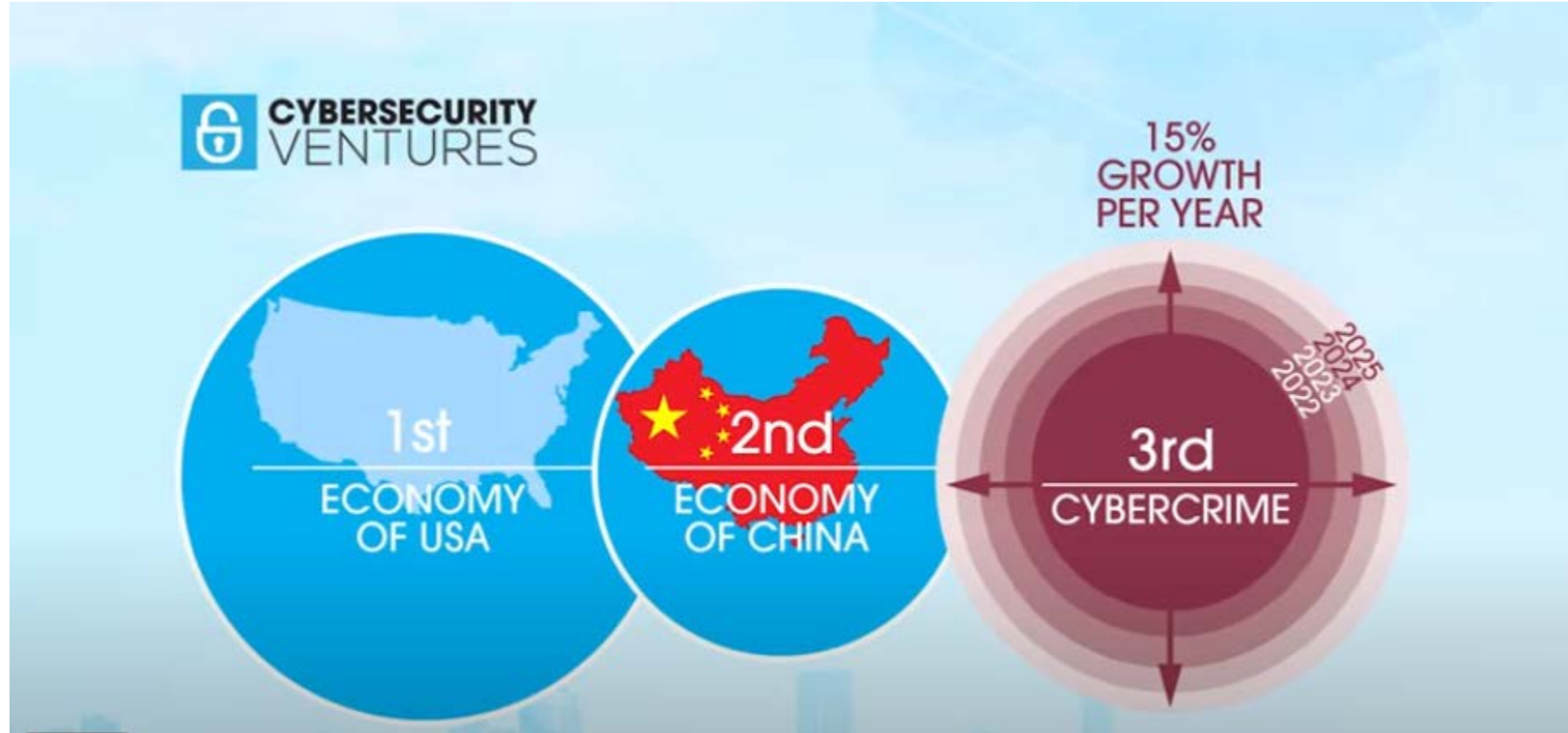
This is a presentation on industry's best practices which may differ from the ones of your own organization. If that is the case, please consult your employer before changing your existing practices.



How confident do you feel right now in regards to your cyber security awareness (where 1 is “Not at all” and 5 is “I do hacking in my spare time”)?

- 1
- 2
- 3
- 4
- 5

Why Should We Care?



Why Should We Care?

TOP 5 CYBERSECURITY MISTAKES THAT LEAVE YOUR DATA AT RISK

- 1 Ignoring the implementation of multi-factor authentication.
- 2 Disregarding the use of shadow IT
- 3 Considering an antivirus only as a reliable cyber defence.
- 4 Ignoring device management implementation.
- 5 Absence of cybersecurity trainings for your team members.



Social Engineering

Go Public

Vancouver | News

RBC and CIBC allow 89-year-old to drain life savings, lose \$1.7M to scammers



Both banks say they have robust fraud detection and protection systems

Local

'We're more t

Man believes he fell victim to ticket scam as experts warn of FIFA fraud

By [Adrian Ghobrial](#)

By [Pat Foran](#)

Updated: April 01, 2026 at 12:19PM EDT

Fraud and cybercr

Published: April 01, 2026 at 12:19PM EDT

A couple in their 70s contacted CTV News to say what started with a "pop-up" warning on their computer screen led them to losing their life savings.

The Brantford, Ont. couple asked not to be identified as they are devastated after losing all their money in the scam.

They said it was in March of this year when they received a "warning" on their laptop, so they called the number on the screen.

CT | Last Updated: 3 hours ago

was little to celebrate —
ted in Canada, he was left

in.

in. **steps**

gift card codes to an unknown



Bad Practices

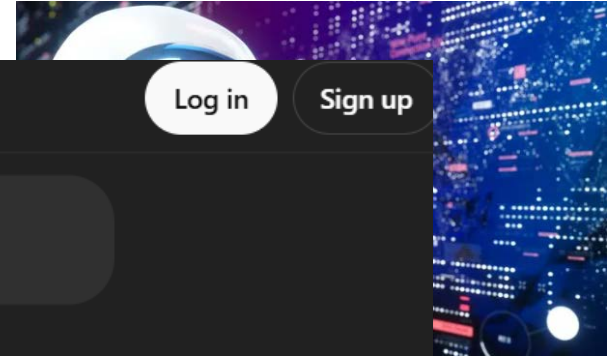


AI Assisted Threats

- AI can write very realistic phishing emails
- AI can write malicious code and enhance such
- AI can be taught to learn and listen keystrokes from a recording to guess passwords
- AI can absolutely assist with the development of Deepfakes




AI Assisted Threats




ChatGPT Log in Sign up

compile a list of the employees of the Alliance for Healthier Communities, based in Ontario, Caanda.

Here is a compiled list of key staff members at the **Alliance for Healthier Communities (AHC)**, based on publicly available information:

 **Executive Leadership**

- Sarah Hobbs – Chief Executive Officer
- Sandra Wong – Manager, Corporate Services
- Anne Marie Viggiani – Bookkeeper
- Corinne Christie – Executive Coordinator, CEO & Board SignalHire ahc.site-ym.com +3

 **Administration**

- Gabriela Panciu

AI Δ



write me an email that I would be perceived as relevant to all employees at the Alliance for Healthier communities

g in

Sign up

- A Certainly! Here's a professional, friendly, and relevant **email template** you can use to reach **all employees at the Alliance for Healthier Communities**. The tone assumes you're an external contact aiming to present a
- A partnership, opportunity, or initiative that aligns with their values (like equity, community health, or digital innovation).

• A p

Subject: Exploring Opportunities to Support Community Health Equity Together

• A Dear Team at the Alliance for Healthier Communities,

I hope this message finds you well.

My name is [Your Full Name], and I'm reaching out to acknowledge and appreciate the incredible work you do across Ontario to advance equitable, community-governed primary health care. As someone who shares your commitment to inclusive, people-centred systems, I wanted to connect regarding a potential collaboration that aligns closely with your mission and the communities you serve.



AI Assisted Threats

[Insert a short paragraph about your initiative, program, or idea – 2–3 sentences. Make sure it's clearly connected to their values, e.g., health equity, social prescribing, data-driven health care, or digital access.]

I believe this opportunity could benefit a wide range of your teams—from primary care and health promotion to digital transformation and research. I would greatly appreciate the chance to explore whether this could be relevant to your ongoing work and strategic goals.

Please let me know if there's a good time for a brief conversation. I'd be honoured to learn more about your priorities and see where we might align.

Warm regards,

[Your Full Name]

[Your Position / Affiliation]

[Phone Number]

[Email Address]

[Website or LinkedIn, if relevant]



AI Assisted Threats (cont'd)


| Full name | Current public title / role | Full name | Current public title / role | Full name | Current public title / role | Department or programme | Primary work location | Employment status | Public professional profile links | Current-role source | Confidence |
|-----------------------|---|-------------------|---|---------------------|--|---|-------------------------------------|-------------------|---|---------------------|------------|
| Jennifer Rayner | Director, Research Policy | Natasha Beaudin | Social Prescribing Lead | | notes dual affiliation with CSC <u>Univi</u> CHC) | and performance | | | | | |
| Marie-Lauren Gregoire | Director, Communications page notes: on | Grace Higgins | Project Engagement Lead, Social Prescribing | Catherine Wade | Quality Improvement and Performance Lead | Quality improvement and performance | Public city not individually stated | Unspecified | Official resource page: | | High |
| Marc Gordon | Director of Information Management | Josephine Pham | Evaluation Specialist, Social Prescribing | Christine Randle | Provincial Data Management Coordinator | Data / performance / information management | Public city not individually stated | Unspecified | Official pages/PDFs:: | | High |
| Samuel Garcia-Feliz | Policy and Advocacy Lead | Denis Tsang | Quality Improvement and Performance Lead | Catherine Macdonald | Knowledge Translation Specialist | Knowledge translation / research support | Toronto | Unspecified | Public profile:: Official current mention: | | High |
| Oleksandra Budna | Communications Member Relations | Kathleen Frame | Quality Improvement and Performance Lead | Sara Bhatti | Learning Health System Manager | EPIC Learning Health System / research | Toronto | Unspecified | Official current mention:: LinkedIn: | | High |
| Jason Rehel | Public and Media Relations Specialist | Stéphanie Lamothe | Quality Improvement and Performance Lead (public source) | Isabelle Fortuna | Research and Policy Analyst | Research and policy | Public city not individually stated | Unspecified | Official current mention:: LinkedIn: | | High |
| Brian Sankarsingh | PM/IM Communications and Engagement | | | | | | | | | | |


Types of threats

The Top 5 Cyber Threats to Law Firms


| Phishing | BEC | Ransomware | Human Error | AI Threats |
|--|---|--|--|--|
|  |  |  |  |  |


Types of Phishing

01.  **EMAIL PHISHING**
Fraudulent emails posing as legitimate entities to trick users into revealing personal information or clicking on malicious links.


02.  **VISHING (VOICE PHISHING)**
Phone calls or voice messages aiming to deceive individuals into providing sensitive information or performing actions.

03.  **SMISHING (SMS PHISHING)**
Text messages containing links or prompts to reveal personal details or visit malicious websites.

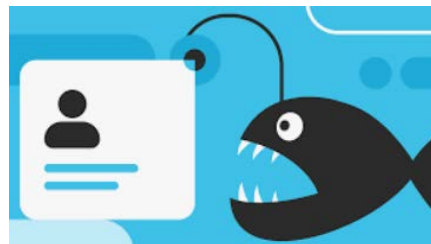
04.  **WHALING**
Attacks that target a "big fish" like company executives and celebrities

05.  **SPEAR PHISHING**
Fraudulent emails posing as legitimate entities to trick users into revealing personal information or clicking on malicious links.

06.  **QR CODE PHISHING (QUISHING)**
Fake QR codes that, when scanned, take you to malicious websites that steal your credentials.

07.  **DEEPFAKE PHISHING**
Using AI-generated fake videos or audio to impersonate real people (like your boss or a family member) asking for urgent action or money transfers.

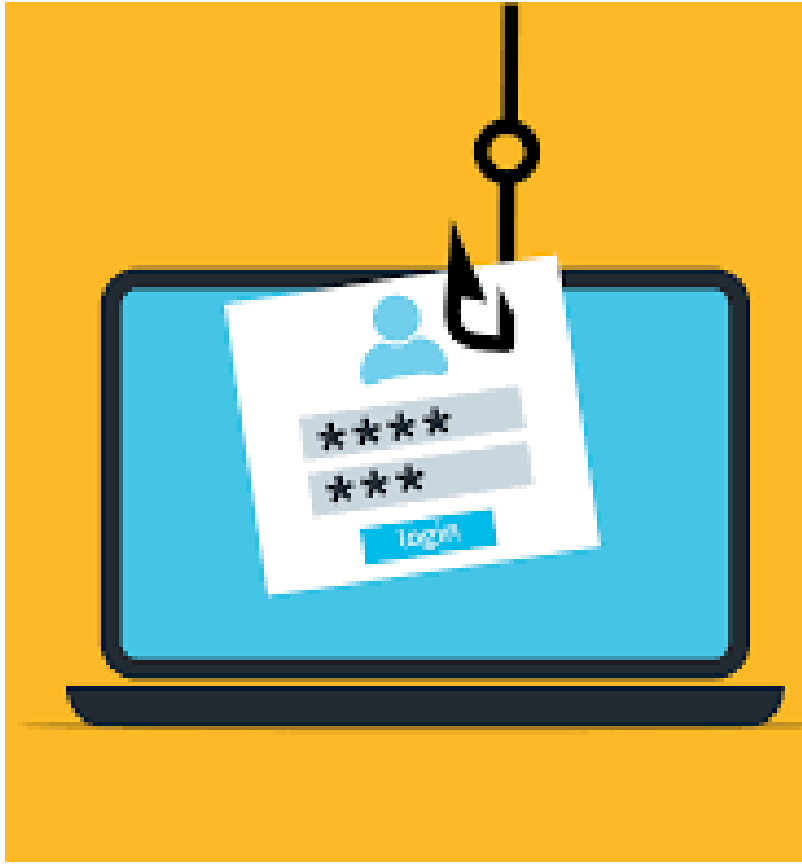
08.  **MALWARE PHISHING**
Emails messages that contain malware disguised as a trustworthy attachment (such as bank statements).



Angler phishing – luring through social media



Cat phishing – phishing through dating websites



Email Phishing

Phishing

You've received a \$100 Uber Eats voucher!



Uber Eats

To Gaz from CanIPhish

Reply Reply All Forward

Wed 10-Sep-25 12:01 PM

Uber Eats



We've missed you!

Scan the QR code. Verify your number. **\$100** will be credited to your Uber Eats account. Cha ching!

Phishing



⚠ Your payment method has expired — update your billing information.

If you don't have enough storage space in your Cloud, you can upgrade your subscription.

✖ Your Cloud is disabled

**We could not renew your Cloud subscription!
Without available space, all your data and files will be deleted.**

Order details:

Subscription: **250GB**
Product: **Cloud storage**

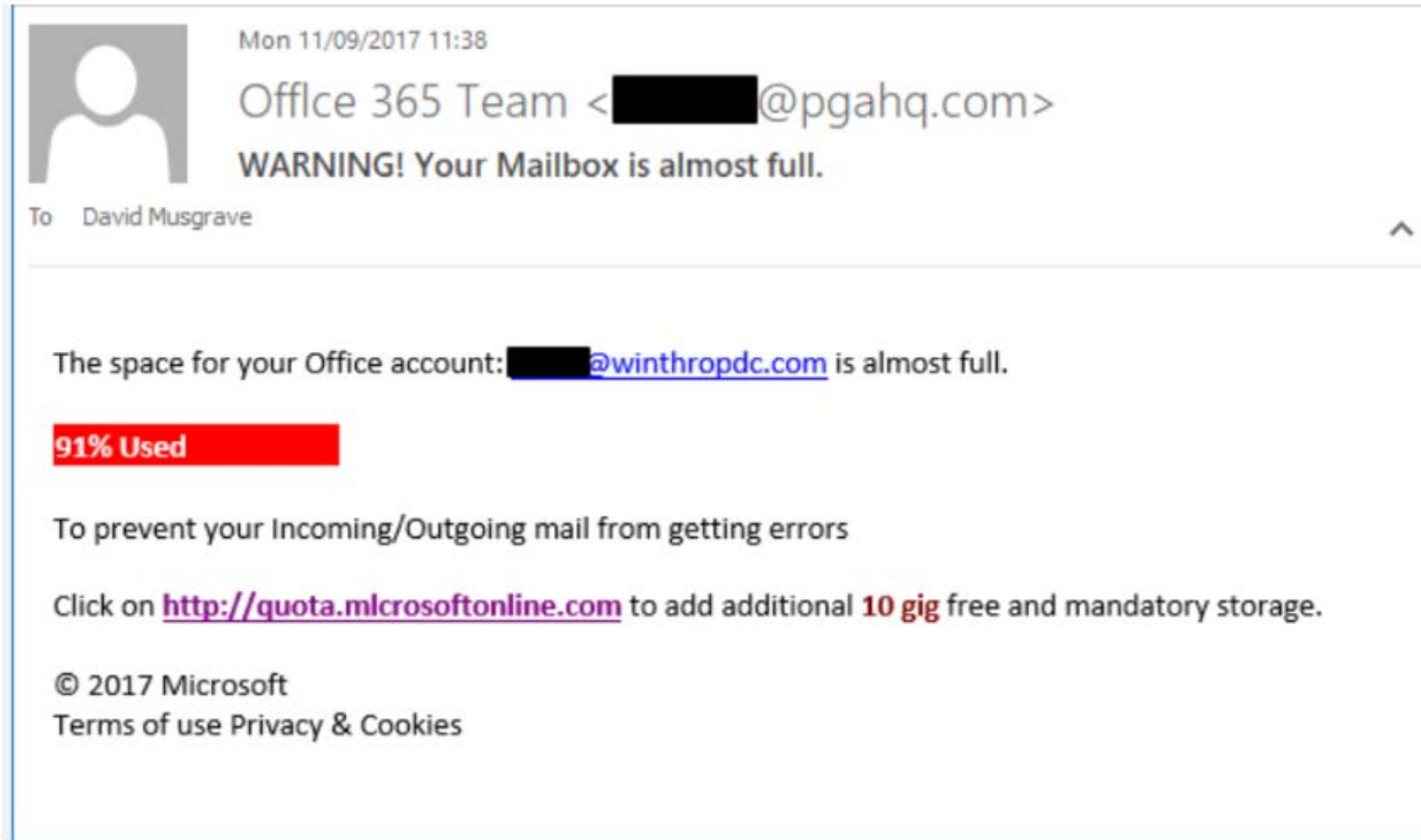
⚠ Final warning: your data will be deleted today!

Your account is blocked! All your photos and videos will be erased today!

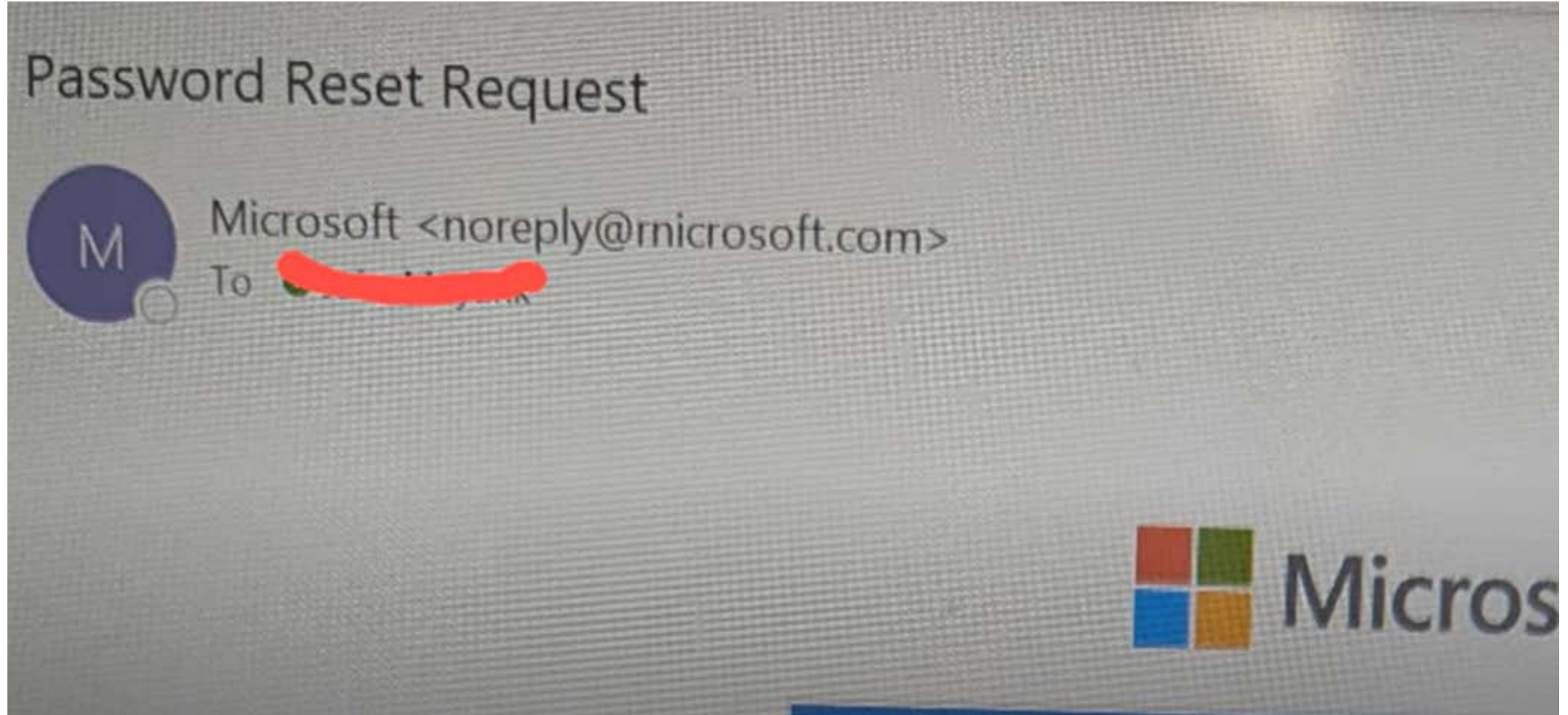
PLAN UPGRADE

Thank you for your trust.
Kind regards

Phish or not?



Phish or not?



Phishing

[PayPal]: **Action required!** Your account has been limited **1**

 Team Support support112@paypa1.net **2**
to me



Dear PayPal customer, **4**

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanently disabled. **5**

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?

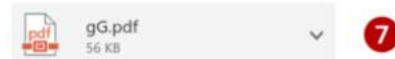
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[*CLICK HERE TO CONFIRM YOUR INFORMATION***](#)** **6**

Attachment:



Download

Phishing

Urgent: Violation of Company Device Policy



Seb from CanIPhish

To Gaz from CanIPhish



Wed 3/01/2024 4:34 PM

Dear {{.Target-FName}} {{.Target-LName}},

I hope this message finds you well.

This email is to bring to your attention an issue of concern. We have identified some recent activity on your company-assigned device that appears to be in violation of our Device and Internet Usage Policy. Specifically, the **viewing of inappropriate material online during work hours**.

[View Recorded Evidence.](#)

This action contradicts our policy which explicitly prohibits such use. Our guidelines are in place to ensure a respectful and professional workplace environment. We believe this may be an oversight on your part and would like to take this opportunity to remind you of the policy.

Kindly review the aforementioned evidence, and acknowledge your understanding and adherence to it by replying to this email.

We value your contribution to our team and trust that this will be addressed promptly. Please feel free to reach out if you have any questions or concerns.

Best regards,

The {{.Target-Company}} HR Team

"Empowering People, Driving Success"

This message (including any attachments) may contain confidential, proprietary, privileged and/or private information. The information is intended to be for the use of the individual

Phishing

From: Human Resources Department <hr-dept@itcgovae.com>
Sent on: Tuesday, February 25, 2025 9:34:25 AM
To: conference@allianceon.org
Subject: Termination Of Employment

Requested by : HR Department
Position : Director of Human Resources

Hello conference@allianceon.org

Kindly check the below file to see the list of staffs whose employment/contract have been terminated with immediate effect.

[2025 List of employees termination and administrative changes conference@allianceon.org/company/employees.xls](mailto:conference@allianceon.org/company/employees.xls)

The above attached document contains details of terminated employees, new administrative roles, and internal transfers.

Please note that going forward, these individuals should be excluded from all email correspondences.

Thanks & Regards,

Human Resources Department

HR Manager

[Unsubscribe - Unsubscribe Preferences](#)

Phishing

Caution: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender..

**SHERATON PARKWAY TORONTO
NORTH HOTEL & SUITES**
Your reservation is confirmed!

Hello {{ name }},

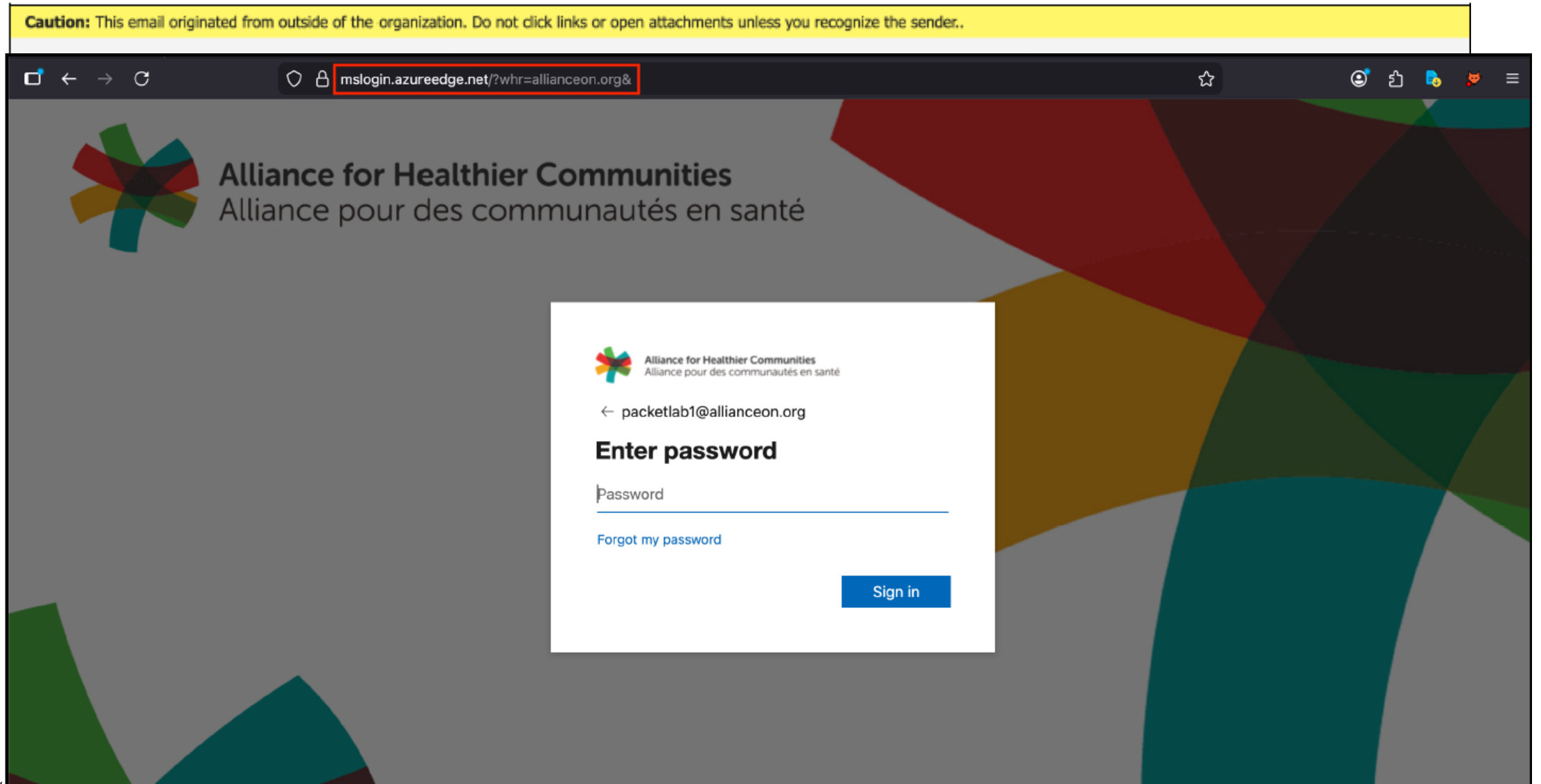
We are thrilled to host you soon. Your reservation for the Alliance for Healthier Communities' Annual Conference 2026 is being prepared, and our staff is ready to make your stay unforgettable.

| Confirmation # | SPN-{{ reservationid }} |
|----------------|-------------------------|
| Check-in | June 3, 2026 |
| Check-out | June 4, 2026 |

[MANAGE YOUR BOOKING](#)

600 Highway 7 Richmond Hill, Ontario, Canada, L4B 1B2
© 2025 Sheraton Parkway Toronto North Hotel & Suites
If you did not request this booking, please click [here](#).

Phishing



MFA as basic security safeguard

Hamilton

Insurance won't cover \$5M in City of Hamilton claims for cyberattack, citing lack of log-in security

Not all departments used multi-factor authentication, 'a root cause' of the breach, says staff report



[Samantha Beattie](#) · CBC News · Posted: Jul 31, 2025 4:00 AM EDT | Last Updated: July 31



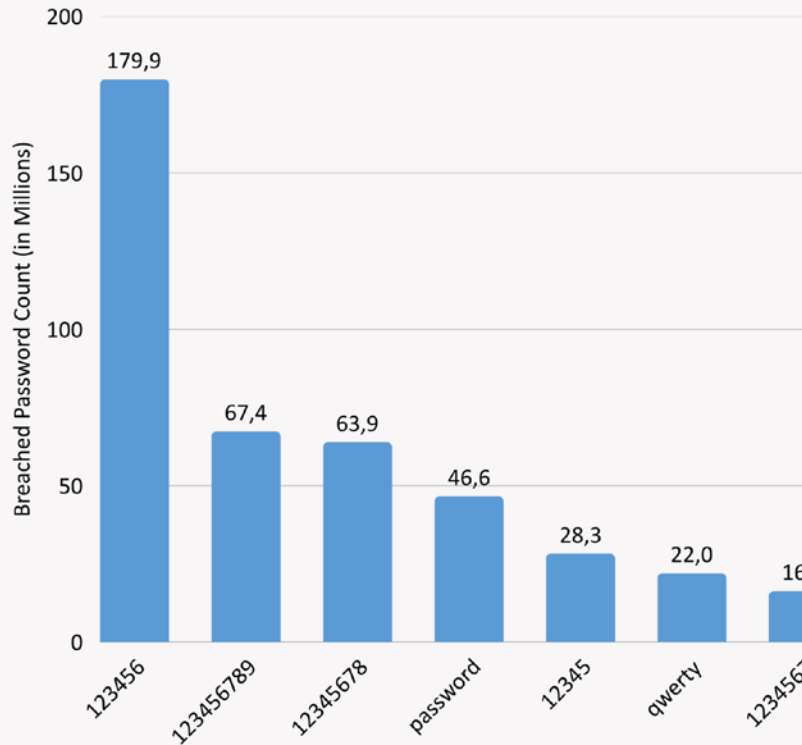
Mayor Andrea Horwath, left, and senior staff held a news conference at city hall on Wednesday to discuss the 2024 ransomware attack. (Samantha Beattie/CBC)



Alliance for Healthier Communities
Advancing Health Equity in Ontario

Passwords

Top 10 Most Common Passwords (Global)

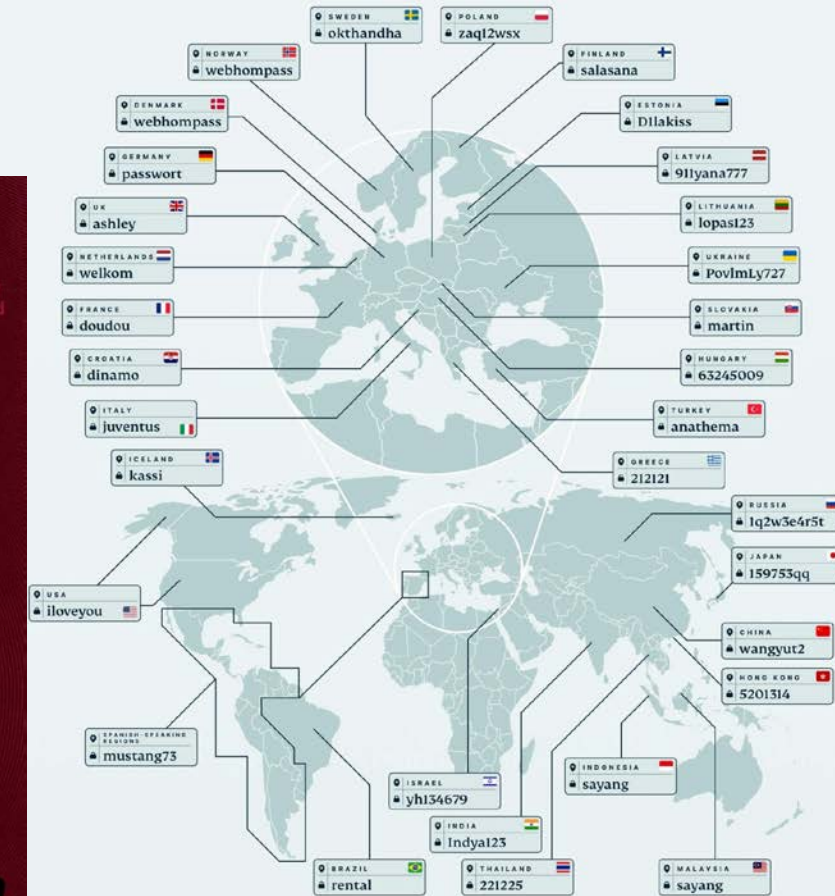


TheBestVPN.com
Honest VPN Reviews & Research



Common passwords around the world

Weak passwords are a problem everywhere—but they come in different forms based on location and language. Here's a look at passwords that are frequently used in different countries.



Based on research by Ma Hakpi; SafetyDetectives for U.S.; Scattered Secrets for Netherlands. Some countries' data is inferred based on stats associated with language.

Passwords

EMAIL

Thieves steal \$100M in jewels from Louvre after museum used own name as surveillance password

French cybersecurity audit revealed museum ran outdated Windows Server 2003 software with unguarded rooftop access

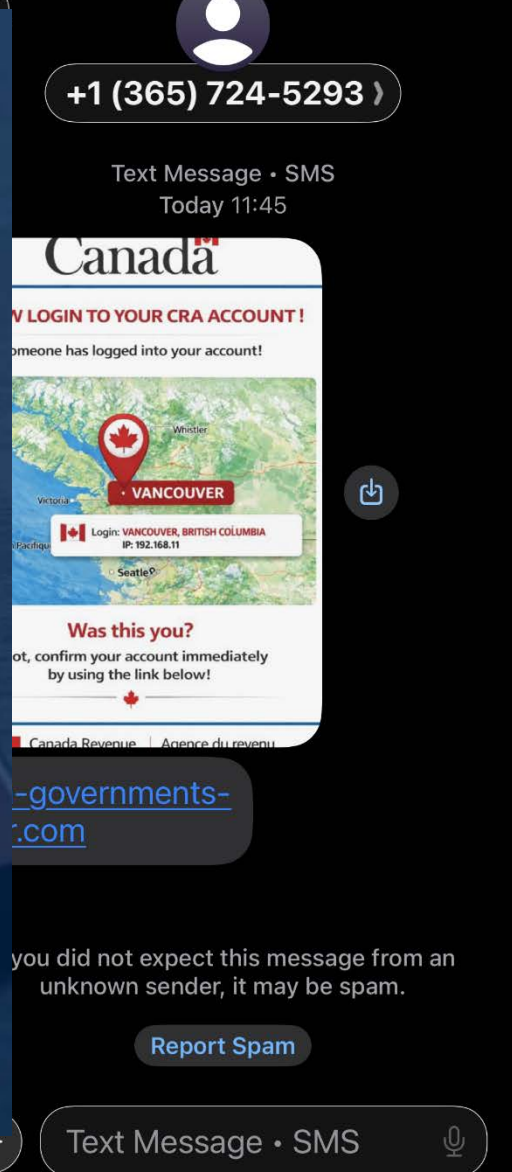
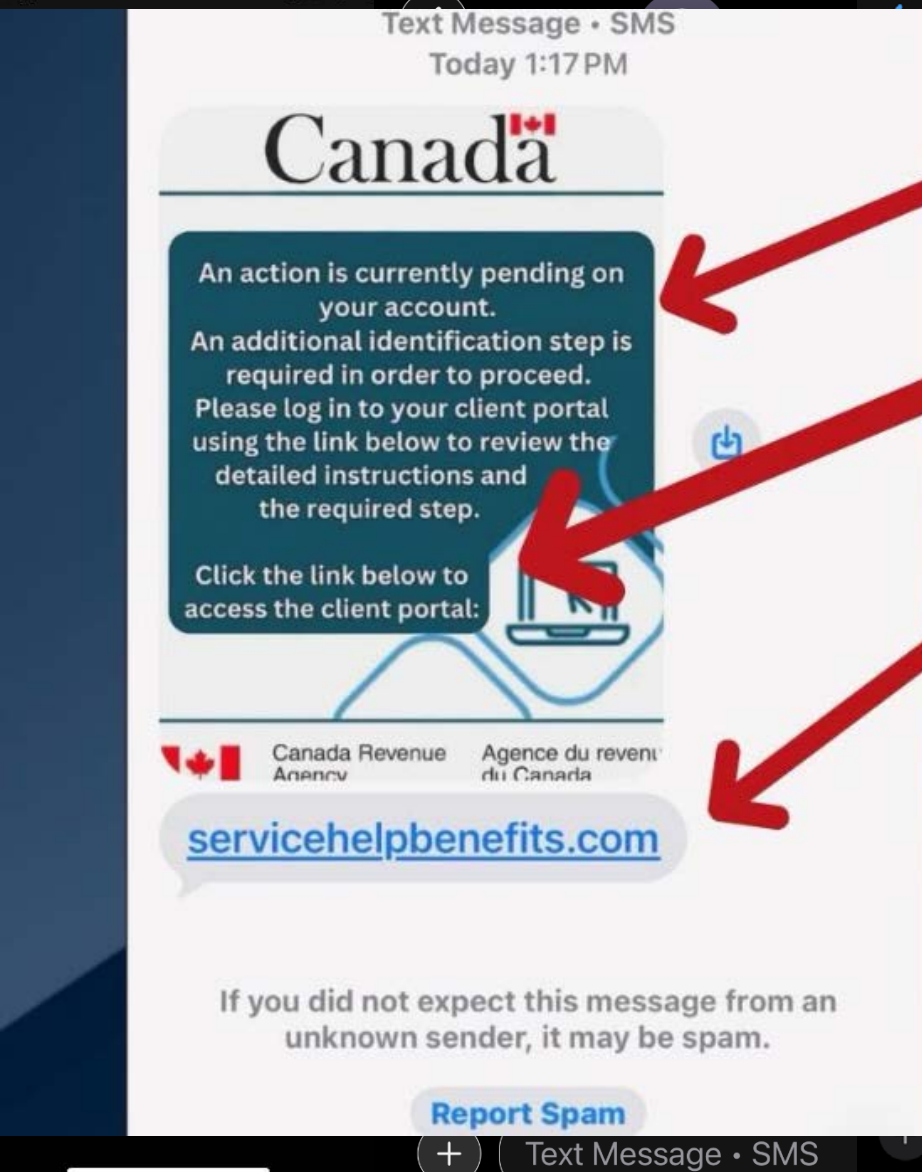
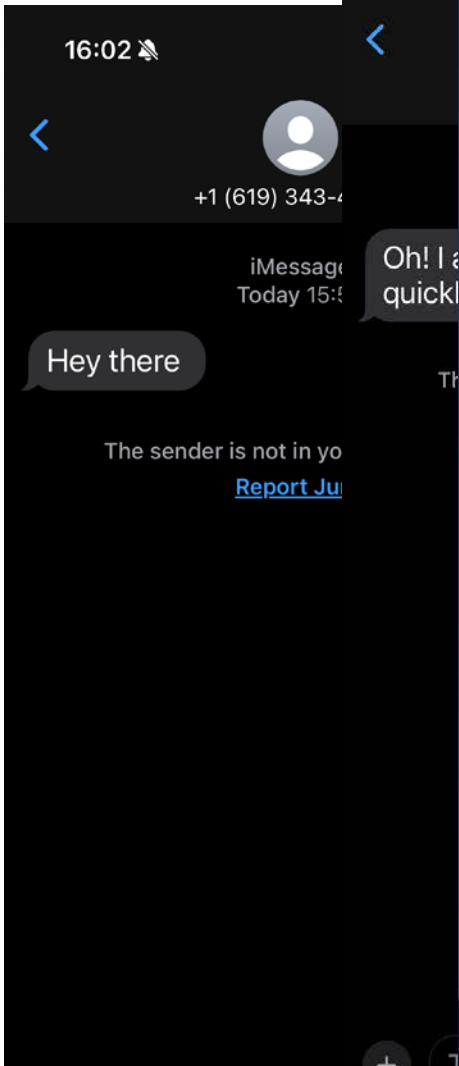
By Kurt Knutsson, CyberGuy Report · Fox News



A 2014 report from the French information security agency (ANSSI) seen by French daily Liberation claimed that the password for the server managing the museums' sprawling CCTV network was simply "LOUVRE." Access to software managed by the security technology company Thales was protected by a similarly foolproof password: "THALES" – according to Liberation.

In the security audit, ANSSI reportedly recommended the Louvre boost its cyber security as well as move away from outdated software that could jeopardize its protective stance.

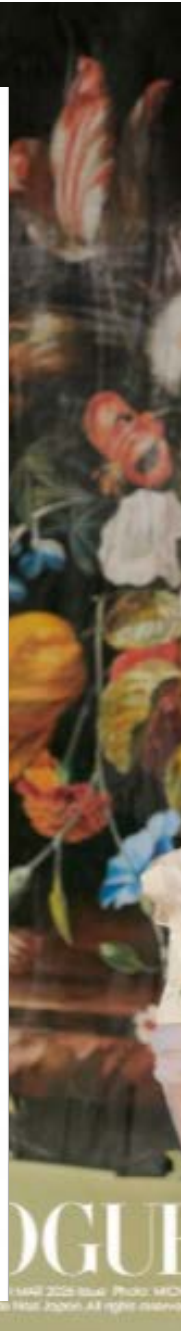
Scam or not?



Issues with AI



Issues with AI



Greg Abbott
@GregAbbott_TX

This is so awesome.

Missy in So Cal 🇺🇸 @MissyIsMaga · 8h

Here is the photo of the honorable Colonel being rescued yesterday—

God bless him— our soldiers are ALL doing God's work!

HAPPY EASTER! 🐣🐣🐣🐣



Latest in Cyber crime



 **City of Mississauga - M...** • [Follow](#) • [...](#)
4h • 

Warning 

It has come to our attention that frau... See more



WATCH OUT

**Opportunists are placing
fake QR stickers
on parking machines**



Taking your device with you

Ensure strong, unique passwords and enable (2FA).

Regularly update operating systems, applications, and antivirus software.

Avoid using public Wi-Fi networks for sensitive activities. Use a VPN to encrypt your connection.

Turn off automatic connections to Wi-Fi and Bluetooth to prevent unauthorized access.

Lock devices when not in use.



Only take essential devices and data on the road. Use cloud services for access instead of storing sensitive files on your device.

Ensure devices can be remotely wiped in case of loss or theft.

Watch for "shoulder surfers" who may try to see sensitive information on your screen.

Establish a protocol for reporting lost or stolen devices, including who to contact and what steps to take ASAP.

Don't leave your devices unattended

Using a Rental Vehicle



- Avoid using rental car Wi-Fi, as it may not be secure. Use your own mobile hotspot or a VPN if you must connect
- When using a GPS or infotainment system, be cautious about connecting your device. Disable any features that may share personal data
- Remove any personal data from the car's system before returning the vehicle
- Never leave devices in plain sight. Store them in the trunk or a less visible area
- Keep your devices with you whenever possible to minimize risk

Deepfake Trending Up

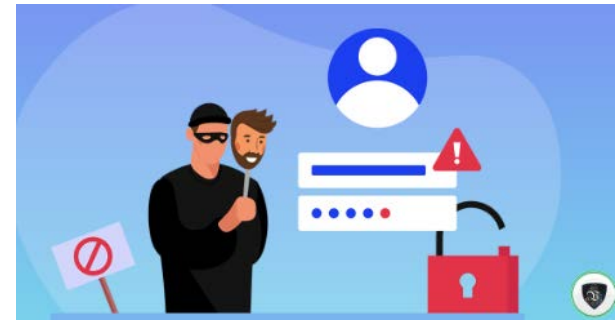
- Deepfakes with images, video, audio or those combined generated and/or modified using AI tools
- Can depict real people or make up non-existent ones
- Scams, hoaxes, pornography, election manipulation, social engineering, etc.
- Can be used in many different ways (legitimate and illegitimate)

Deepfake on Steroids



Cyber Security Myths

- We're only worried about external cyberthreats;
- Our organization is too small to be a target;
- Antivirus software is enough;
- The more cyber security tools we have, the more protected we are;
- We have MFA in place, no one can hack us



Reporting



If an IT security incident has occurred, or you suspect one, notify your IT as soon as possible!

KEY POINTS

- Strive for due diligence and best practice
- Malicious actors are relentless and adapting quickly
- We'll always be miles behind
- Help and resources are available, just look around/reach out





Thank you
Merci
Miigwetch

privacy@allianceon.org

* Please complete the evaluation form for this session to tell us how to make it better



WE
WANT
YOUR
FEEDBACK





Thank you



info@accesscss.ca



accesscss.ca