Protecting Your Identity Online

and Why It's Important to Your Business

NPC DataGuard™

NPC Safe Computing Webinar Series

December 13th, 2022

Larry Keating, President
Darren Mar, National Sales Manager

Presenters

Larry Keating
President

30 years’ experience with information technology, remote communications and data security.

Darren Mar
National Sales Manager

10 years in SMB technology products and services, with emphasis on financial services small office security.

Thank You!

ALIGNED capital partners inc.

Serenia Life FINANCIAL

HUB

PPI

Investment Planning Counsel®
IPC VALEURS MOBILIÈRES

SIDEDRAWER™

Advocis
The Financial Advisors Association of Canada

MANDEVILLE™
PRIVATE CLIENT INC.

EQUITY Associates Inc.

Carte
WEALTH MANAGEMENT INC.
RISK MANAGEMENT INC.

AON

Manulife Securities

GROVE POINT
FINANCIAL

HollisWealth™

IDC WORLDSOURCE
INSURANCE NETWORK INC.

Advisor Research Group Inc.

CI FINANCIAL

IIAC ACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

FINANCIAL LITERACY
COUNSEL INC.

GLOBAL
MAXFIN INVESTMENTS INC.

MFDA™
Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

Agenda

- Protecting Your Identity to Protect Your Business
- Threats to Your Identity
- Best Practices for Personal and Professional Identity Management
- Q&A

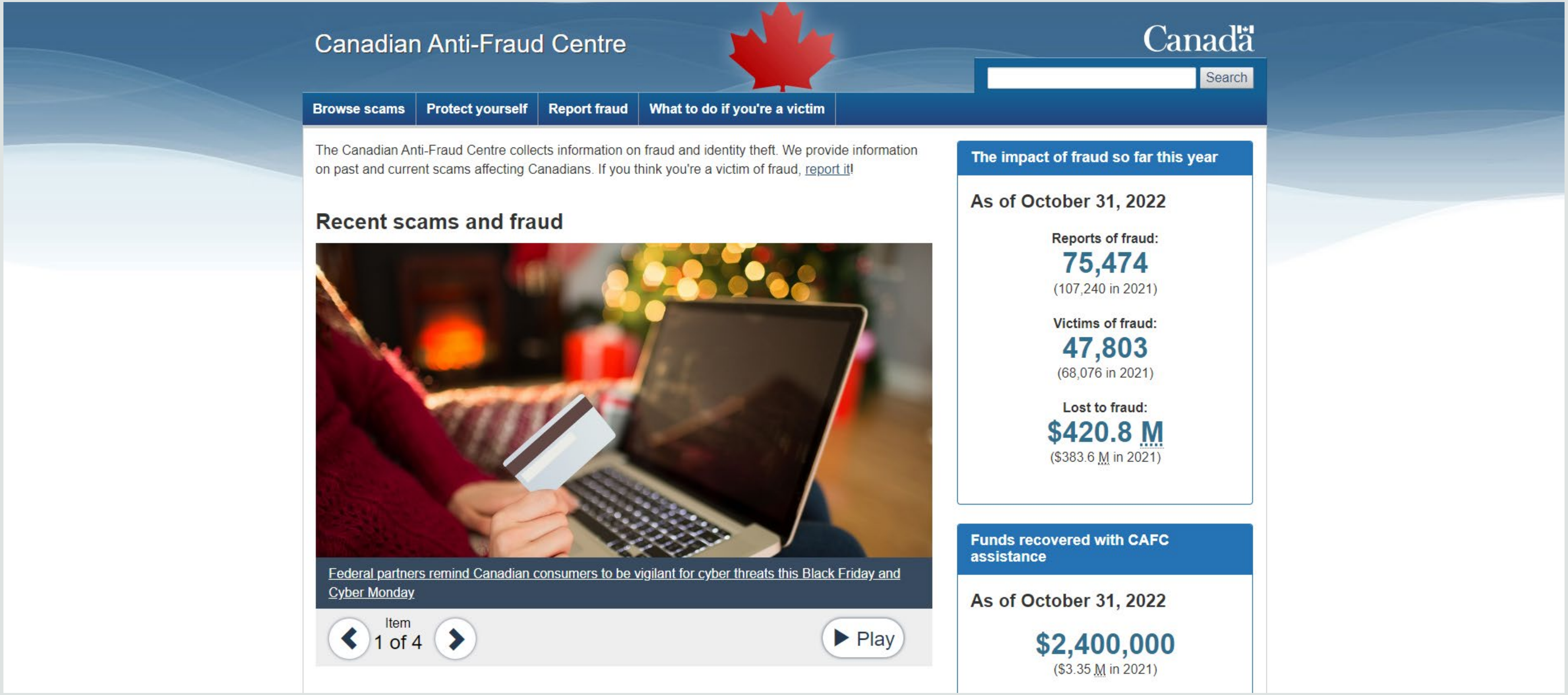
Why Protecting Your Identity Matters to Your Business

Why Protect Yourself

- According to CrowdStrike, 80% of all breaches use compromised identities [1]
- For small business professionals, personal and business identities are closely intertwined
- Many small business professionals are owner, officer, director and key executive, with personal guarantees, or even personal accounts, to run the business

[1] Source: CrowdStrike Blog – June 8, 2022

Identity theft scams on the rise…



The Canadian Anti-Fraud Centre collects information on fraud and identity theft. We provide information on past and current scams affecting Canadians. If you think you're a victim of fraud, report it!

Recent scams and fraud

Federal partners remind Canadian consumers to be vigilant for cyber threats this Black Friday and Cyber Monday

The impact of fraud so far this year

As of October 31, 2022

Reports of fraud:
75,474
(107,240 in 2021)

Victims of fraud:
47,803
(68,076 in 2021)

Lost to fraud:
$420.8 M
($383.6 M in 2021)

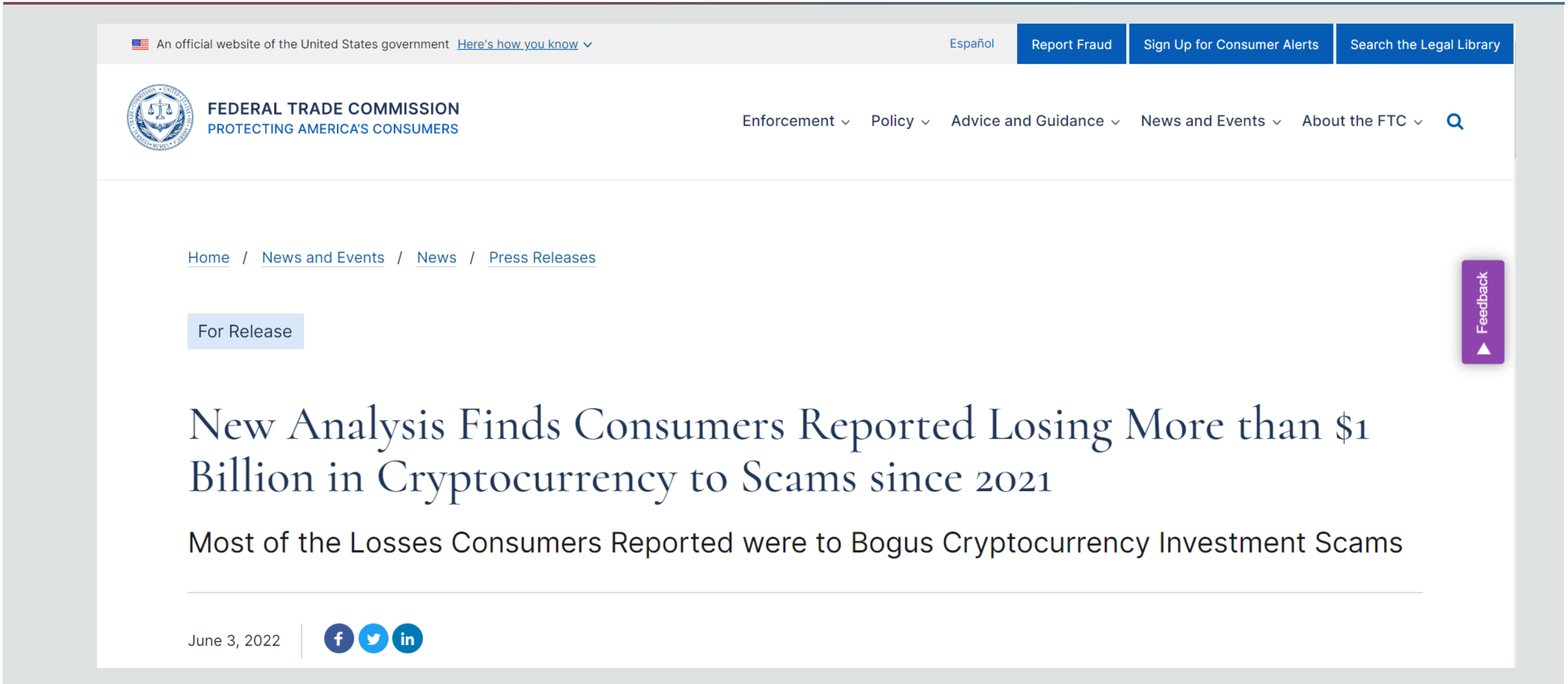
Funds recovered with CAFC assistance

As of October 31, 2022

$2,400,000
($3.35 M in 2021)

Source: Canadian Anti-Fraud Centre

Identity theft scams on the rise…



An official website of the United States government Here's how you know

Español Report Fraud Sign Up for Consumer Alerts Search the Legal Library

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement Policy Advice and Guidance News and Events About the FTC

Home / News and Events / News / Press Releases

For Release

New Analysis Finds Consumers Reported Losing More than $1 Billion in Cryptocurrency to Scams since 2021

Most of the Losses Consumers Reported were to Bogus Cryptocurrency Investment Scams

June 3, 2022

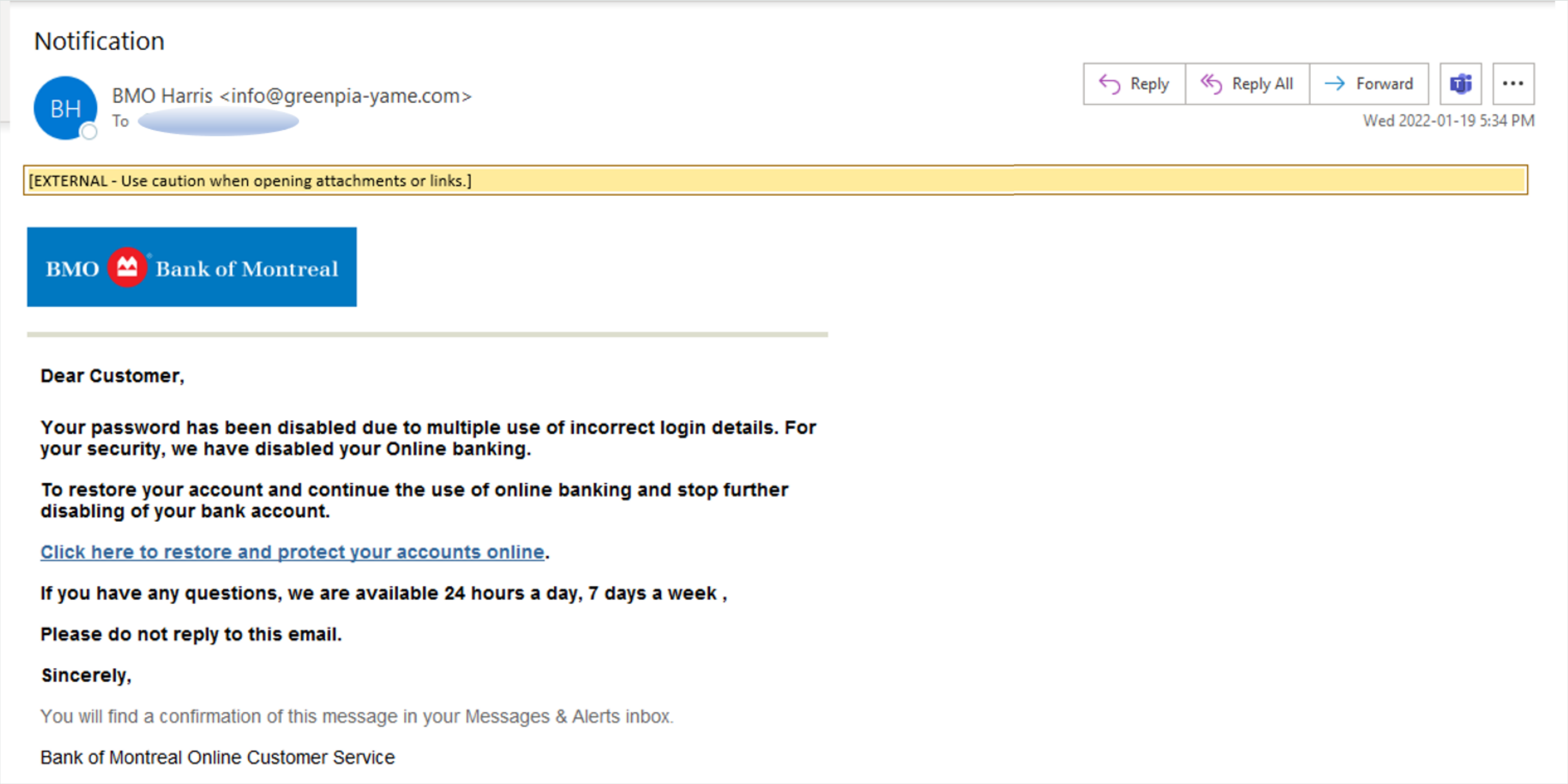
Source: U.S. Federal Trade Commission June 3, 2022

Identity Theft Impact

Fraud and financial theft on an individual can have both an immediate and long-term impact on business credit standing:

- Banking arrangements, payroll and tax payments, etc.
- Illegal purchases from your accounts and credit facilities
- Loans, mortgages and lines of credit taken out in your name
- The sale of your home or other assets
- Crimes committed in your name
- Government benefits and identities in your name

Spoof Email



Notification

BMO Harris <info@greenpia-yame.com>

To [redacted]

Wed 2022-01-19 5:34 PM

[EXTERNAL - Use caution when opening attachments or links.]

Dear Customer,

Your password has been disabled due to multiple use of incorrect login details. For your security, we have disabled your Online banking.

To restore your account and continue the use of online banking and stop further disabling of your bank account.

Click here to restore and protect your accounts online.

If you have any questions, we are available 24 hours a day, 7 days a week ,

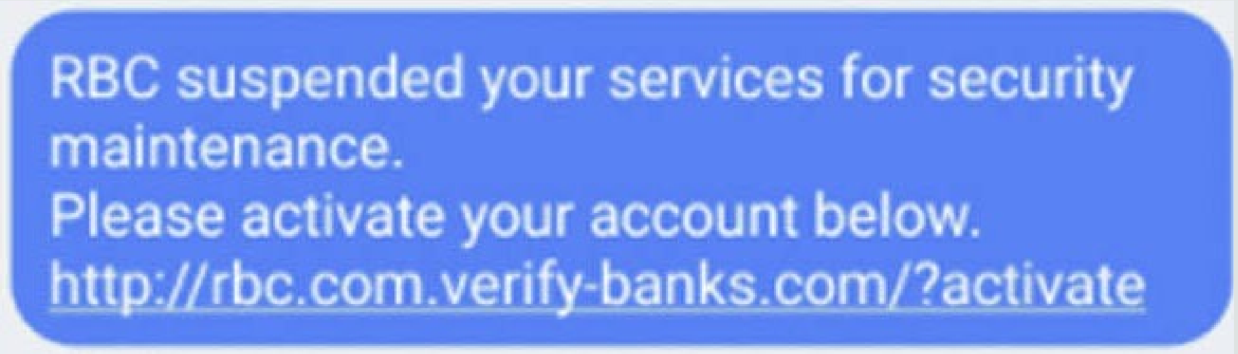
Please do not reply to this email.

Sincerely,

You will find a confirmation of this message in your Messages & Alerts inbox.

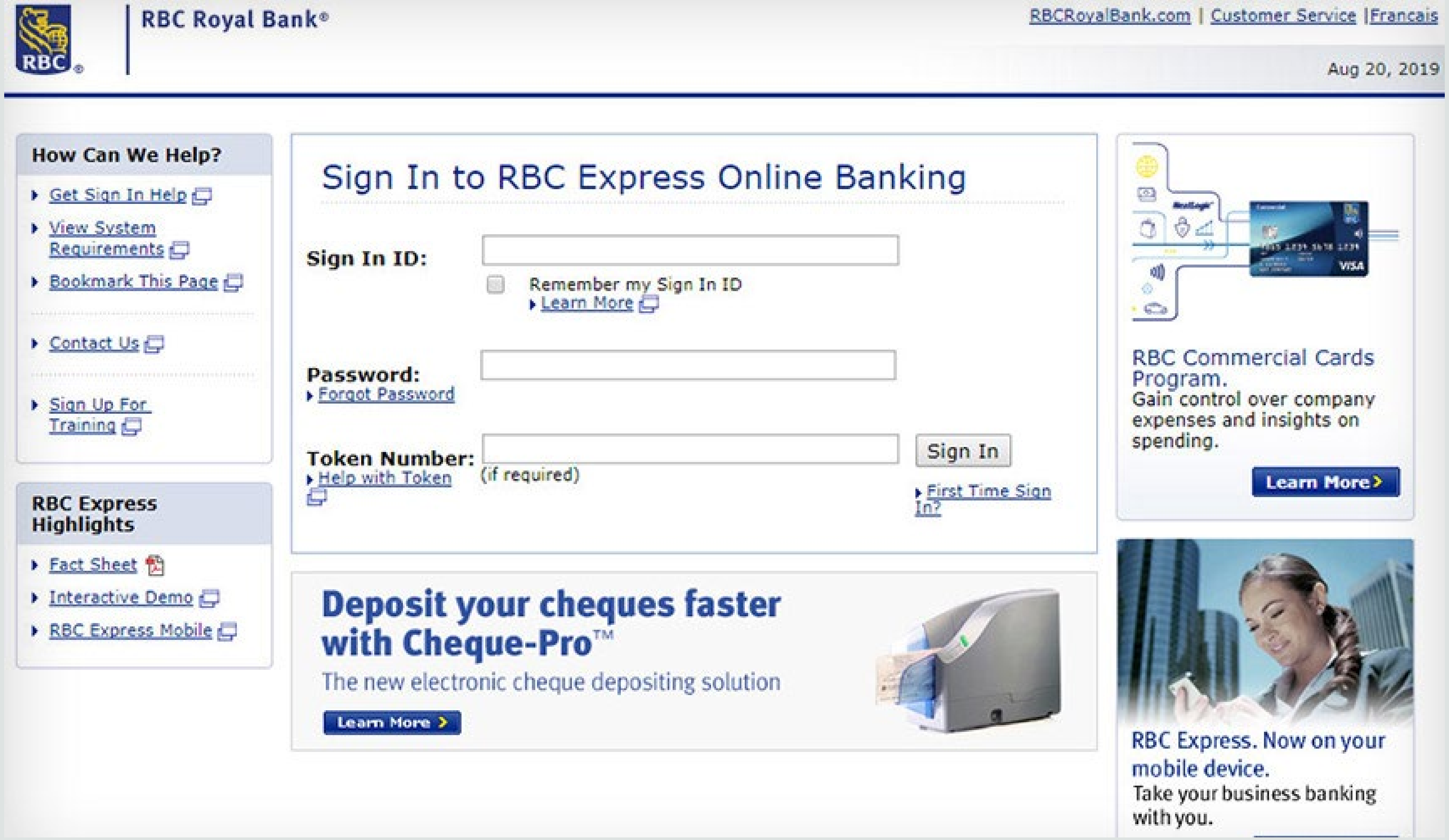
Bank of Montreal Online Customer Service

Spoof Text



RBC suspended your services for security maintenance.
Please activate your account below.
http://rbc.com.verify-banks.com/?activate

Spoof Banking Website



RBC Royal Bank®

RBCRoyalBank.com | Customer Service |Francais

Aug 20, 2019

How Can We Help?

- Get Sign In Help
- View System Requirements
- Bookmark This Page
- Contact Us
- Sign Up For Training

RBC Express Highlights

- Fact Sheet
- Interactive Demo
- RBC Express Mobile

Sign In to RBC Express Online Banking

Sign In ID:

□ Remember my Sign In ID

- Learn More

Password:

- Forgot Password

Token Number: (if required)

- Help with Token

Sign In

- First Time Sign In?

Deposit your cheques faster with Cheque-Pro™

The new electronic cheque depositing solution

Learn More ›

RBC Commercial Cards Program.

Gain control over company expenses and insights on spending.

Learn More ›

RBC Express. Now on your mobile device.

Take your business banking with you.

Identity Fraud

Targeted Information

- What are they looking for?
  - Email address(es)
  - Home address, phone numbers
  - S.I.N. / S.S.N., driver's license, etc.
  - Login credentials
  - Banking information
  - Online transactions
  - Online search activities
  - Medical history
  - Date of birth
  - Browsing history

  - From social media posts:
    - Birthdays, events, school history, relative and pet names, anything that can help bad actors pretend to be you

Best Practices

Checklists!

Browsing

Difference between “Private Mode” (or Incognito) vs “Do Not Track”

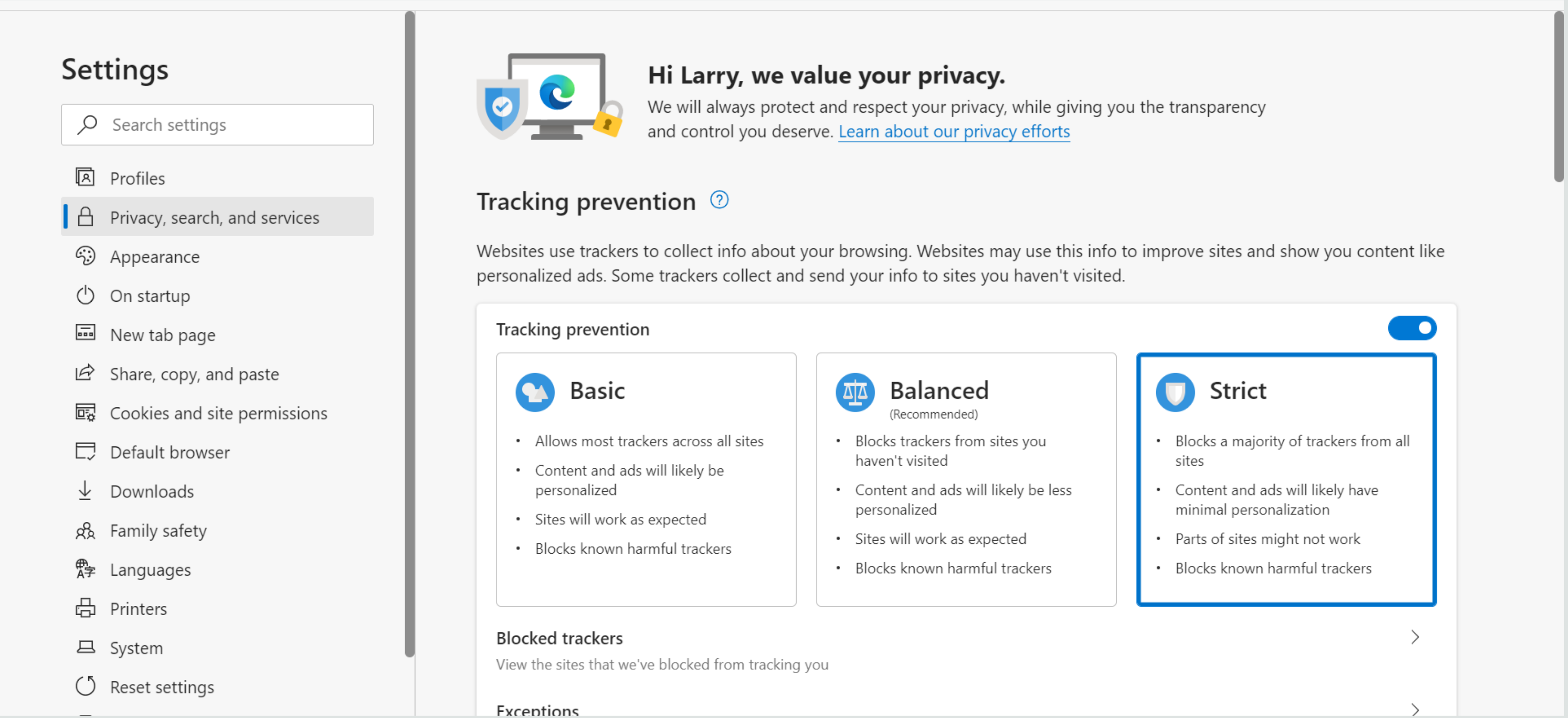
- Private Mode is a browser setting that prevents your search activity and browsed pages history from being stored on your computer

- Do Not Track is a browser setting that tells sites you visit not to place a “cookie” on your system to track you

Neither prevents the collection of information such as your computer name, device type, IP address or operating system, when you visit a site…

Save this **checklist** for later.

Block Tracking & Data Sharing with Your Browser



Settings

Search settings

- Profiles
- Privacy, search, and services
- Appearance
- On startup
- New tab page
- Share, copy, and paste
- Cookies and site permissions
- Default browser
- Downloads
- Family safety
- Languages
- Printers
- System
- Reset settings

Hi Larry, we value your privacy.

We will always protect and respect your privacy, while giving you the transparency and control you deserve. Learn about our privacy efforts

Tracking prevention

Websites use trackers to collect info about your browsing. Websites may use this info to improve sites and show you content like personalized ads. Some trackers collect and send your info to sites you haven't visited.

Tracking prevention ●

Basic

- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

Balanced
(Recommended)

- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

Strict

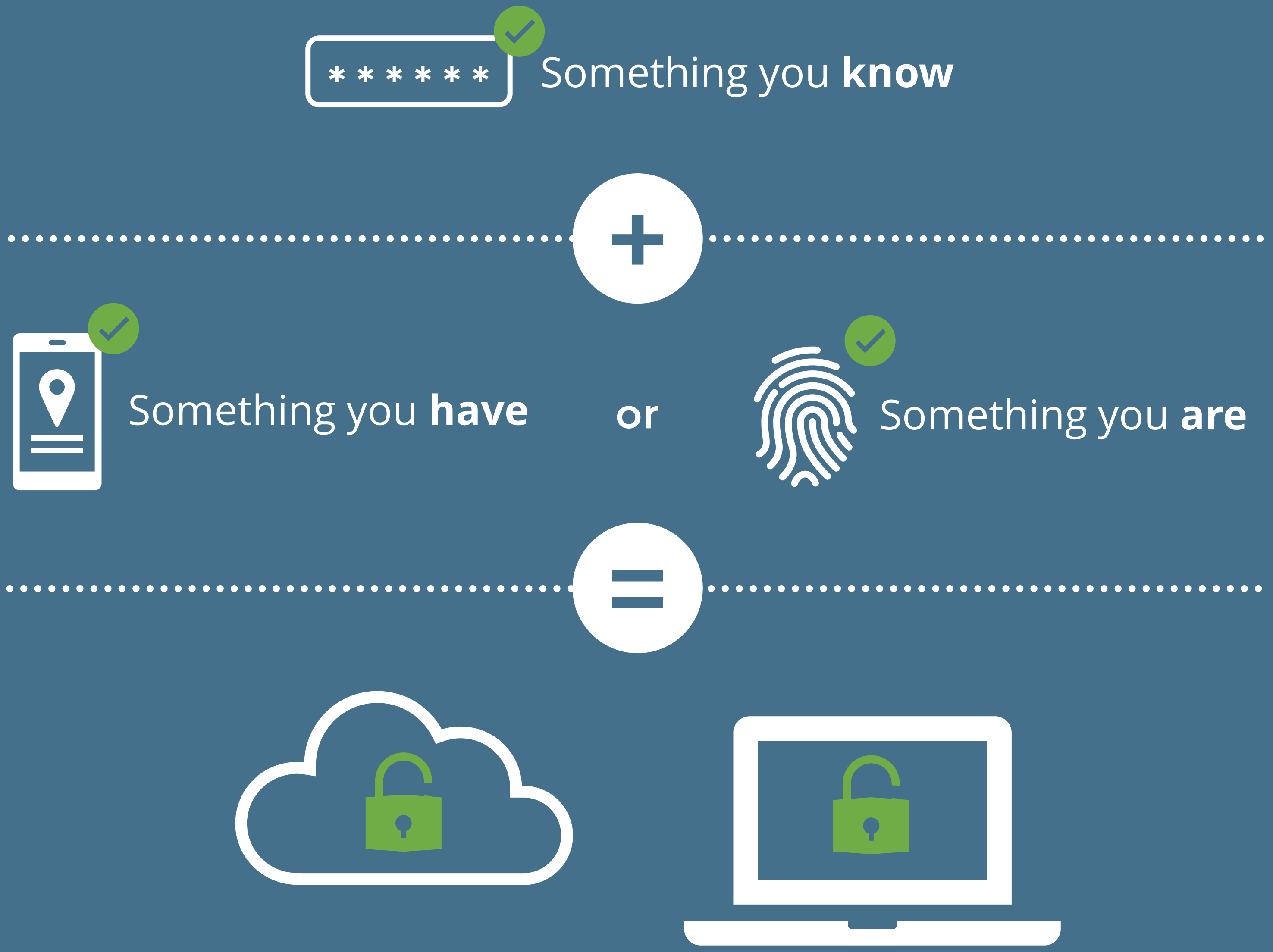
- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Blocked trackers
View the sites that we've blocked from tracking you

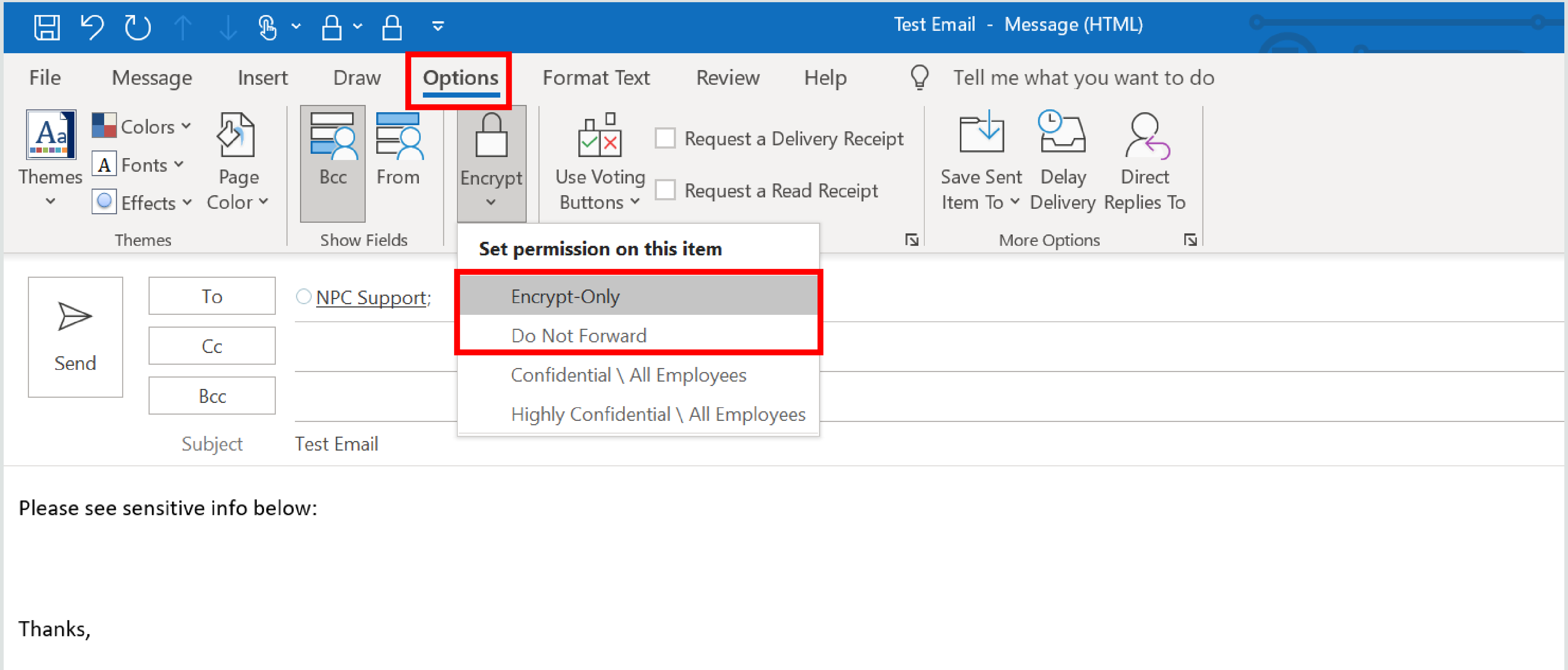
Exceptions

Enable Multi-Factor Authentication

Definition:
A method of allowing access to applications, websites, systems or devices, only after the user presents two or more pieces of authentication evidence.



Encrypt Email



To: NPC Support;

Subject: Test Email

Please see sensitive info below:

Thanks,

Personal Credit Management: Credit Reports

☐ Save this **checklist** for later.

❑ Once a year, obtain a copy of your **credit report** and ensure that it is accurate

- Canada has two national credit bureaus: Equifax Canada and TransUnion Canada
- In the U.S. you can have, by law, one free credit report per year. So order one every four months from one of the three credit bureaus; TransUnion, Equifax, Experian
- The inquiry does not affect your credit, the report does not show your score, just activity

❑ Use a **Credit Monitoring Service**

Canada: Ordering your credit report and score - Canada.ca

U.S.: Credit Reports and Scores | USAGov

NPC

Personal Credit Management: Fraud Alerts

Fraud Alerts – alerts you to the issuance of credit in your name

In the U.S.,

- It is free, you must contact all three credit bureaus
- Must be renewed each year

In Canada,

- Called an **Identity Alert**, bureaus legally required in Ontario and Manitoba to alert you, if it is in place
- A **"Fraud Warning"**
  - Only available to confirmed victims of identity theft or fraud
  - It places a note on your credit report that you are to be called by the lender before issuing credit, but not a legal requirement
- TransUnion does provide for a "Potential Fraud Alert", if, say, you lost your wallet or purse, same conditions as above

Personal Credit Management: Credit Freezes

Credit Freezes – prevents anyone from issuing credit in your name until you approve

In the U.S.,

- Free, you only have to request it at one bureau

In Canada,

- Not available!

Credit Locks – you turn your credit issuance control on and off

- Just developing, as you see in ads for bank and credit card companies. It allows you to lock your credit account activity from an app on your phone. Only locks for the institution that issued the app
- May not stop some organizations from viewing your credit

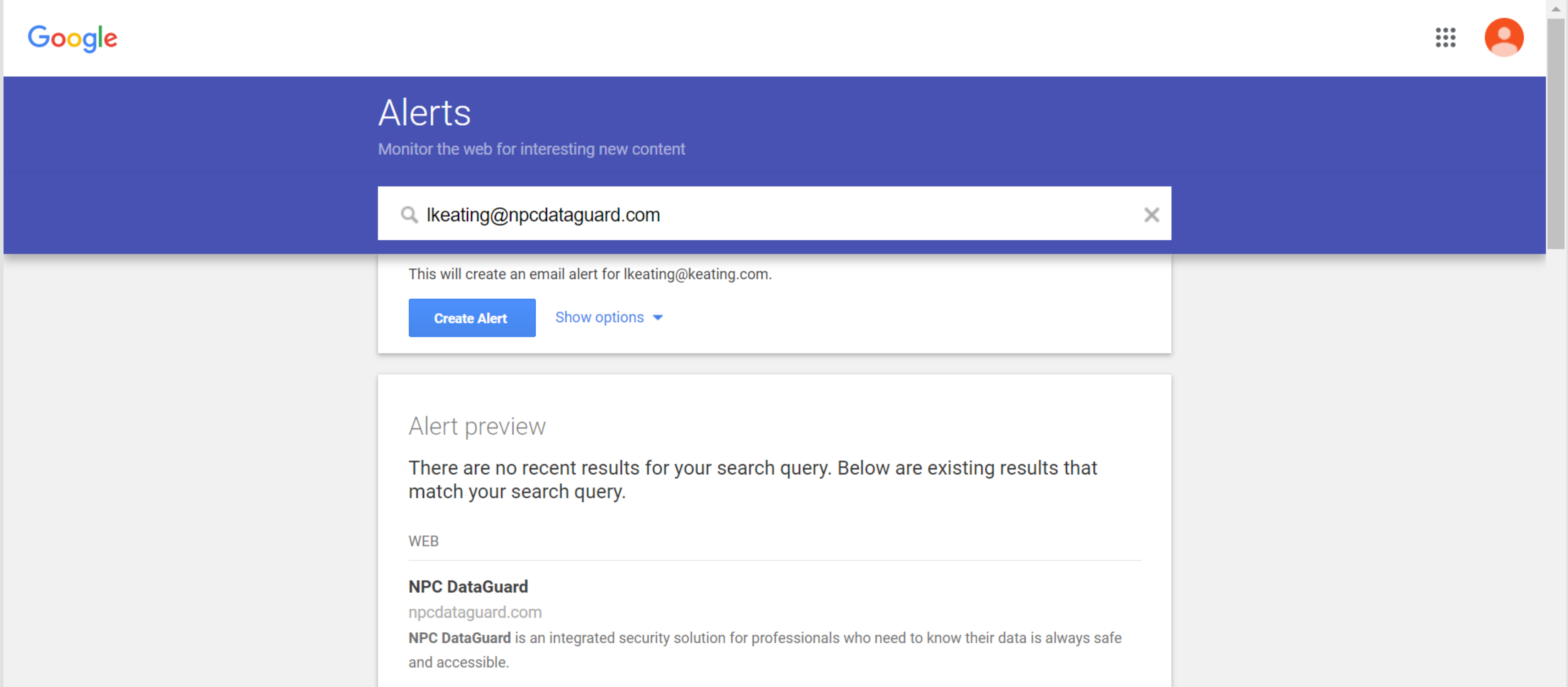
Open Web Monitoring

Google Alerts

Get alerted by Google when information you specify appears on the Internet

- Very simple to set up
- Powerful if someone attempts to impersonate you or your business
- More valuable than in the past because of “doxing”--posting stolen information on the Internet when companies refuse to pay ransoms

www.google.com/alerts



Alerts

Monitor the web for interesting new content

lkeating@npcdataguard.com

This will create an email alert for lkeating@keating.com.

Alert preview

There are no recent results for your search query. Below are existing results that match your search query.

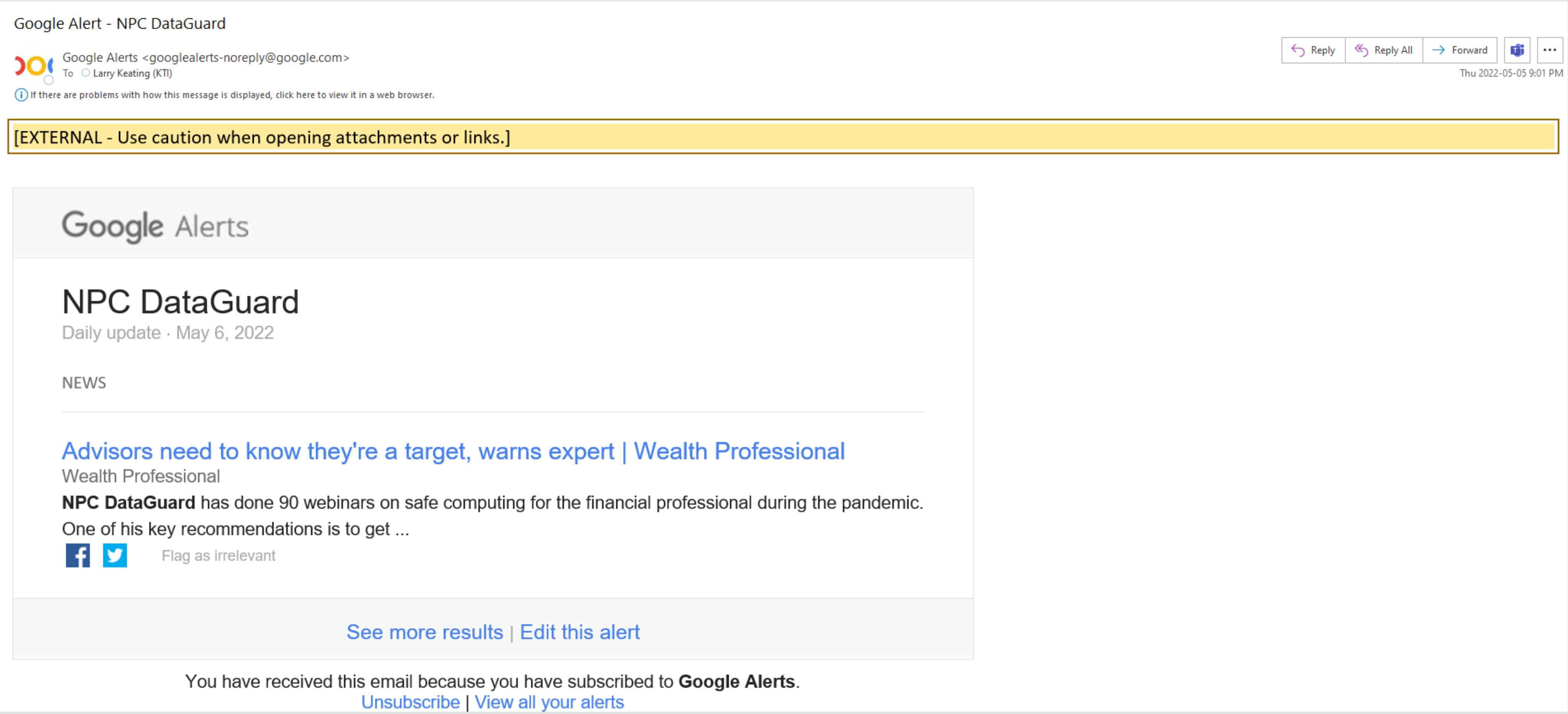
WEB

NPC DataGuard

npcdataguard.com

NPC DataGuard is an integrated security solution for professionals who need to know their data is always safe and accessible.

www.google.com/alerts



Google Alert - NPC DataGuard

Google Alerts <googlealerts-noreply@google.com>
To ○ Larry Keating (KTI)

Thu 2022-05-05 9:01 PM

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

[EXTERNAL - Use caution when opening attachments or links.]

Google Alerts

NPC DataGuard
Daily update · May 6, 2022

NEWS

Advisors need to know they're a target, warns expert | Wealth Professional
Wealth Professional
NPC DataGuard has done 90 webinars on safe computing for the financial professional during the pandemic. One of his key recommendations is to get ...

Flag as irrelevant

See more results | Edit this alert

You have received this email because you have subscribed to **Google Alerts**.
Unsubscribe | View all your alerts

Dark Web Monitoring

Get alerted when information you specify appears on the Dark Web

- A service that navigates the dark web searching for information you specify
- Typically keys on your email address
- By no means a perfect science
- The real value may be in the support the provider offers if there is a hit

Email and Web Site Monitoring

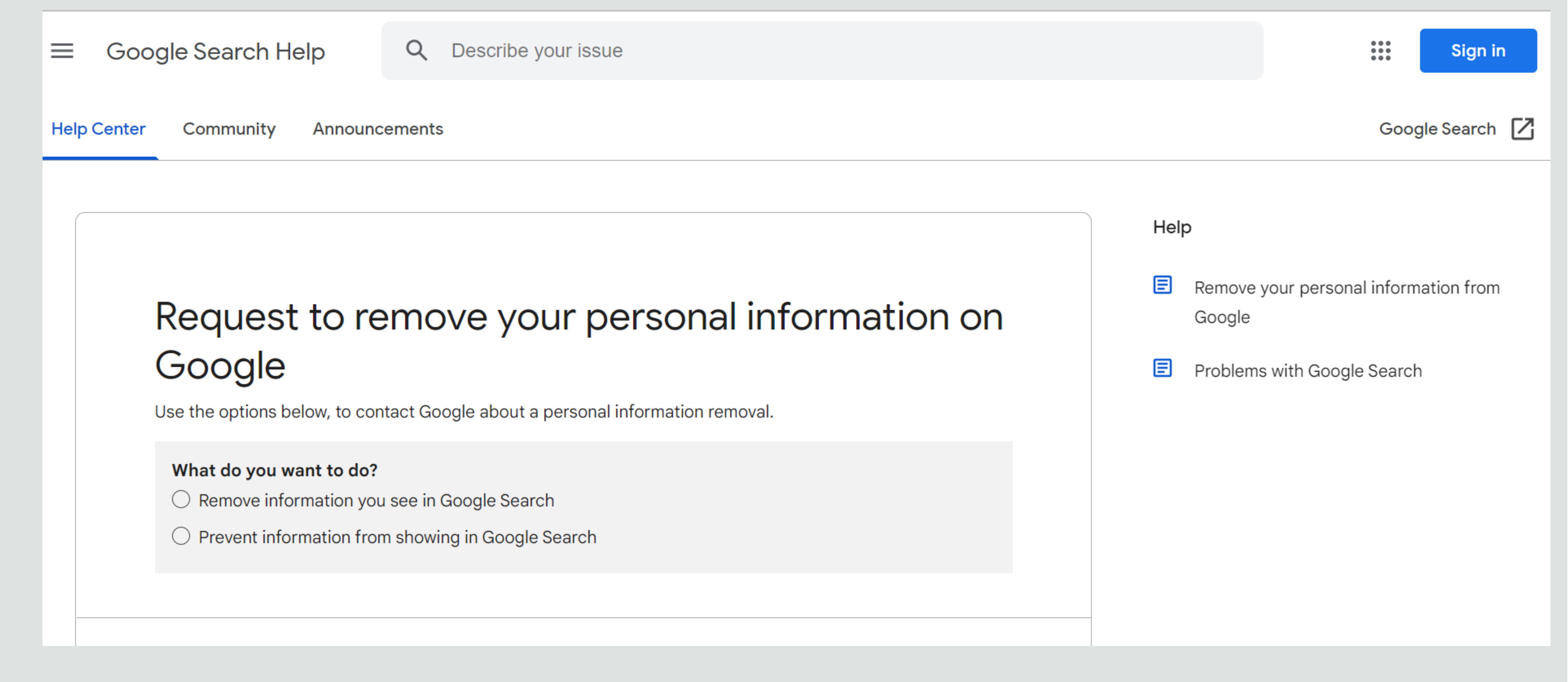
Email address theft monitoring

- www.haveibeenpwnd.com
    - A quick check of your email address taken in major breaches

Website uptime monitoring

- www.siteuptime.com
    - Monitors the web presence of your website or firewall

Google will now remove elements of your PII on request



Google Search Help

Request to remove your personal information on Google

Use the options below, to contact Google about a personal information removal.

What do you want to do?

○ Remove information you see in Google Search

○ Prevent information from showing in Google Search

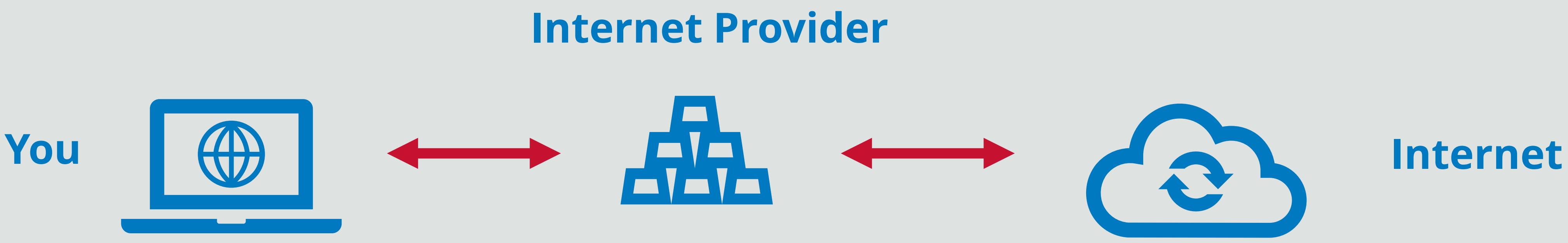
Help

- Remove your personal information from Google
- Problems with Google Search

VPN Benefits

- Provides a secure “tunnel” to connect to websites and services on the Internet
- Hides your search history, even from your ISP
- Hides your IP address and location

No VPN



Internet Provider

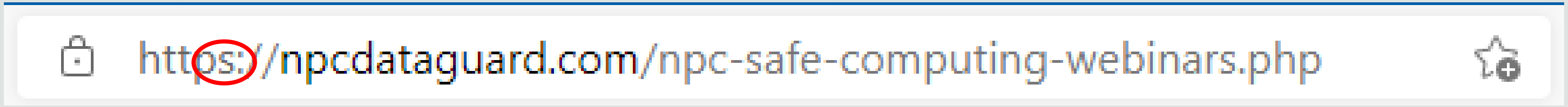
You

Internet

HTTP ✗ 🔓

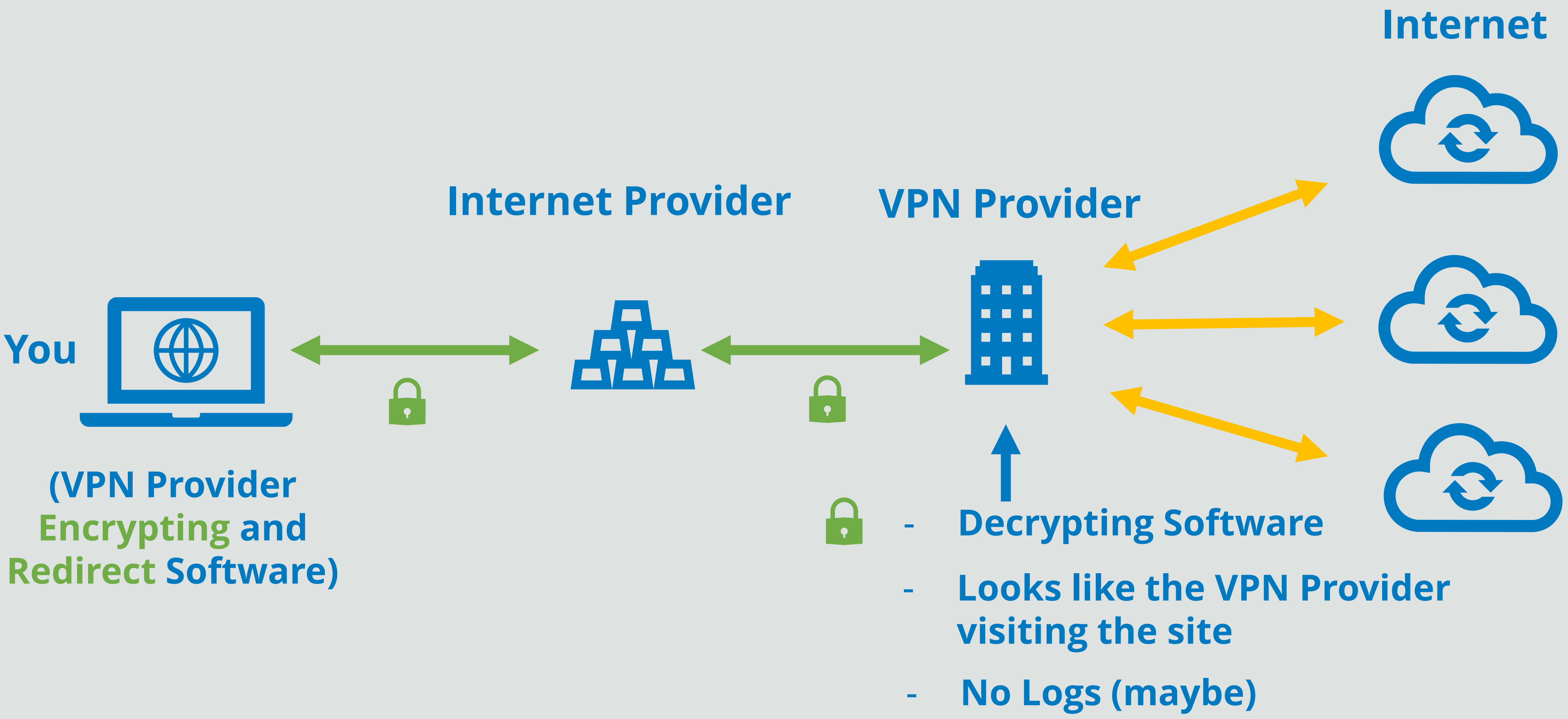
HTTPS ✓ 🔒

🔒 - Encrypts browser traffic, not email, IM, etc.
- Connection Requests visible



https://npcdataguard.com/npc-safe-computing-webinars.php

“Consumer” or “Commercial” VPN



Internet

Internet Provider

VPN Provider

You

(VPN Provider Encrypting and Redirect Software)

- Decrypting Software
- Looks like the VPN Provider visiting the site
- No Logs (maybe)

Choosing a VPN

- Does the VPN Service Provider respect your privacy?
- What country do they operate in?
- Do they log user data?
- Where are their servers located?
- Do they use the most current protocols?
- Are they a credible company?

Banking

- ❑ Watch your personal and business banking and credit card accounts, and statements
- ❑ Consider a separate bank account and credit card for online purchases
- ❑ Understand your banking agreement, what you are responsible for, and what risks you have if you are defrauded
- ❑ If you do not use wire transfers, see if your bank will block it altogether in your account
- ❑ Ask for two-party or two-factor approval for wire transfers
- ❑ Set the maximum transfer limit low

Save this **checklist** for later.

What to Do if Your Identity Has Been Stolen

Save this **checklist** in case of emergency.

- ❑ Call your bank to reverse transactions
- ❑ Lock your credit cards and bank accounts
- ❑ Change all account passwords
- ❑ Call the authorities; law enforcement, Internet crime reporting centers
- ❑ Contact your insurance provider, or identity protection firm

Clients may turn to you for advice if their identity has been stolen!

Canada: Cyber Incidents - Canadian Centre for Cyber Security

U.S: Incident Reporting System | CISA

Additional Resources

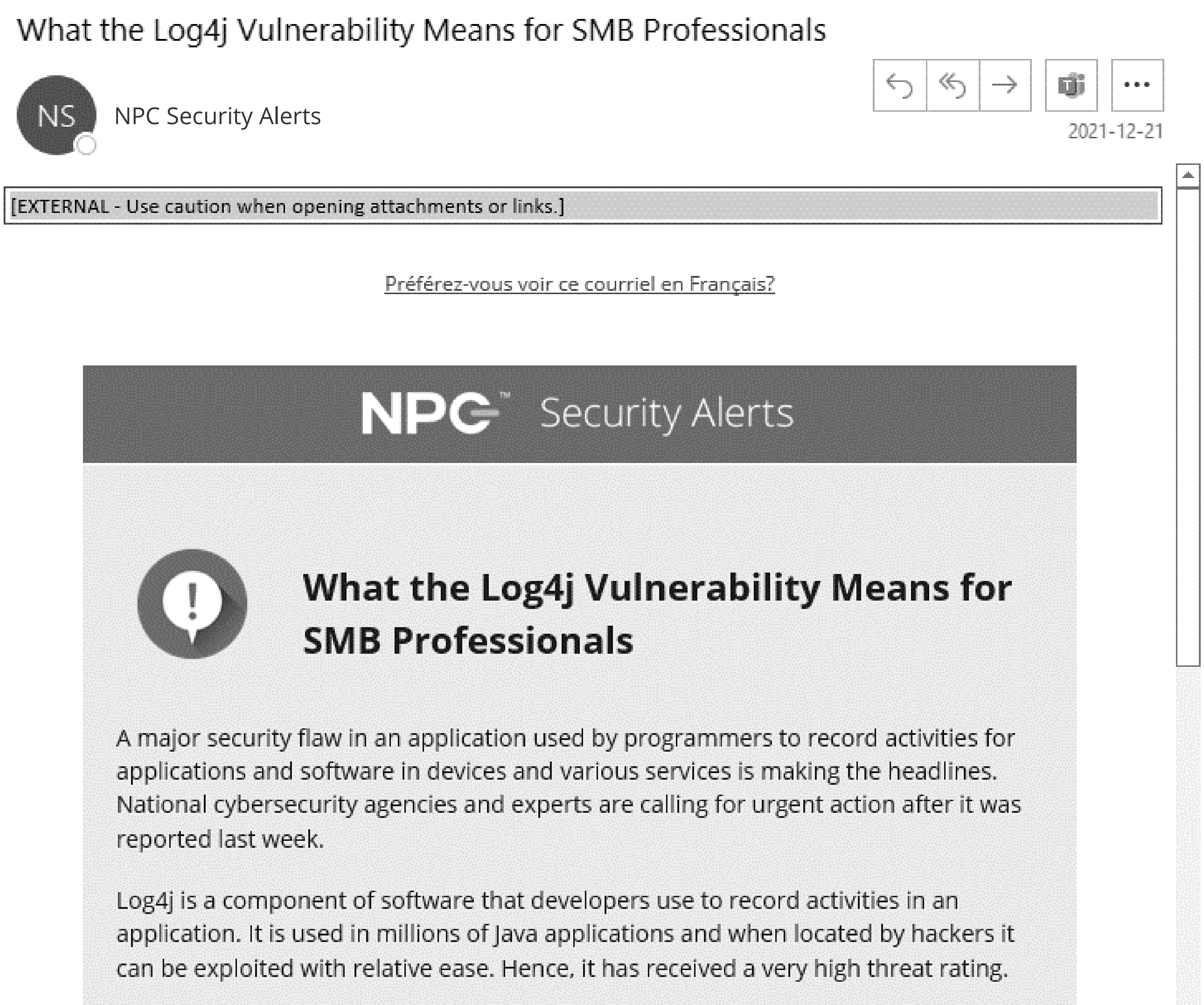
NPC Solutions

Secure managed computers and Microsoft 365 for the professional and SMB office.

- NPC Secure Managed Computers
  - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
  - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Cyber Assessments and Pen Testing

NPC Security Alerts

npcdataguard.com/alerts



What the Log4j Vulnerability Means for SMB Professionals

NPC Security Alerts

2021-12-21

[EXTERNAL - Use caution when opening attachments or links.]

Préférez-vous voir ce courriel en Français?

NPC™ Security Alerts

What the Log4j Vulnerability Means for SMB Professionals

A major security flaw in an application used by programmers to record activities for applications and software in devices and various services is making the headlines. National cybersecurity agencies and experts are calling for urgent action after it was reported last week.

Log4j is a component of software that developers use to record activities in an application. It is used in millions of Java applications and when located by hackers it can be exploited with relative ease. Hence, it has received a very high threat rating.

Upcoming NPC Webinars

npcdataguard.com/webinars

December 15th 1:00 PM EST (30 mins)	NPC DataGuard Solutions Overview
January 17th 1:00 PM EST (60 mins)	Enhancing Password Security and the Power of Multi-Factor Authentication
January 19th 1:00 PM EST (30 mins)	NPC DataGuard Solutions Overview
February 14th 1:00 PM EST (60 mins)	Ransomware 2.0: Prevention Is Your Best Option
February 16th 1:00 PM EST (30 mins)	NPC DataGuard Solutions Overview

NPC Webinars Recordings

→ npcdataguard.com/webinars

Work From Home Securely with Microsoft 365

How to Protect Your Business from Email Compromise Attacks

Increase Revenue and Lower Cost Through As-a-Service Technologies

Five-Step Checkup for Your Cyber Protection

& more, and new topics will be added

Q&A

Larry Keating
lkeating@npcdataguard.com
905-305-6501

Darren Mar
dmar@npcdataguard.com
905-305-6513

Thank You

Please Be Safe & Stay Healthy

NPC™

Smarter Computing

Identity Protection Checklists

Top 10 Computing Basics to Protect Your Identity

Save this **list** for later.

1. Secure your computer
2. Patch your devices and your software
3. Use top quality anti-virus software
4. Use strong, unique passwords
5. Use multi-factor authentication
6. Secure your Wi-Fi
7. Encrypt your data
8. Identify phishing emails
9. Have a second computer for play
10. Lock your phone, put anti-virus software on it, limit its use for work

Advanced Computer Hygiene

- ❑ Delete/archive files with personal information when they are no longer required
- ❑ Individually encrypt sensitive files with a long password
- ❑ For long-term documents, print them, store securely, then delete the electronic versions
- ❑ Never store your key identifiers, driver’s license number, social insurance number, etc., on your computer or phone
- ❑ Use a shredding tool, for paper and for data on drives and phones
- ❑ Erase your digital footprint on your device
  - ❑ Use a cleaning tool that is stronger than deleting your browsing history, like Disk Cleanup or CCleaner, to delete temp and cache files

Save this **checklist** for later.

Browsing

- ❑ Decline data sharing, restrict cookies
  - A more "personalized" browsing experience is a poor trade-off for your identity
- ❑ Resist saving credit card information and auto-fill information in your browser
- ❑ Don’t overshare on social media
- ❑ Limit information in “About Me” in your social media profiles

Save this **checklist** for later.

Online Identity Protection: Awareness

- ❑ Consider where you give your email address, or personally identifiable information
- ❑ Is your personal email address your business email?
  - Create a second email address for social media, news sites, games, etc. Save your primary for personal communications, banking, etc.
- ❑ Be careful with out-of-office messages
- ❑ Even if you are not going to use a specific social media service, consider creating a profile to consume the use of your email address. Watch it for postings
- ❑ Encrypt your email
  - Office 365 at certain license levels offers this
  - Extensions are available for Gmail to encrypt

Save this **checklist** for later.

Online Identity Protection: Awareness

☐ Save this **checklist** for later.

- ❑ Be careful what apps you download, especially free apps
- ❑ Google Security Check will show you what apps are pulling what from you. Apple will show you what apps have your ID, what is active
- ❑ Only buy online from reputable sites
- ❑ Post nothing that is Personally Identifiable Information (PII) on social media, consider setting your accounts to private
- ❑ Understand your Terms of Service and watch policy changes
- ❑ Use different screen names and images
- ❑ You can blur your house on Street View!

Back