KnowledgeFlow.org

HOW TO PROTECT YOUR PRIVACY AND SECURITY ONLINE

Combatting Cybercrime through Collaboration

DURHAM REGIONAL POLICE

Town of Ajax By the Lake

VICTIM SERVICES DURHAM REGION

KNOWLEDGEFLOW CYBERSAFETY FOUNDATION

Facilitated by:
Claudiu Popa
CISSP CIPP CRISC

How to be #UnHackable

Be Private

Be Secure

Be Skeptical

Be Positive

Be Private

How to be #UnHackable: **Be Private**

KnowledgeFlow.org

SHOULD THEY HAVE YOUR PRIVATE DATA?

Companies are not allowed to overcollect your personal info.

You can choose what data to share with businesses.

WHITE LIES

Provide 'fake info' and use the same fake info next time you are asked to verify it.

Use a password manager to keep track of the information you have given to each site.

WHAT CAN YOU "LIE" ABOUT? DATA THEY DON'T NEED SUCH AS:

- Your Name
- Your Date of Birth
- Images of Yourself
- Where you Live
- Your Occupation
- Your Age
- Your Gender
- Your Ethnicity

Be Private

How to be #UnHackable: **Be Private**

KnowledgeFlow.org

Skim a Privacy Policy: 4 Key Words

Use CTRL+F to find and read these sections:

Information

Review the personal info collected. Is it necessary for the purpose of the site/app? How will it be used? Will your data be shared with third-parties like 'partners' or 'affiliates'?

Delete/Retain

How long will your information be kept? Can you request that it be deleted? Does the company provide a contact to ask questions or access your own data?

Advertising

Is your data shared in order to target you with ads? Look for words like 'targeted advertising' or 'interest-based' content, 'personalize' or 'improve' the service.

Security

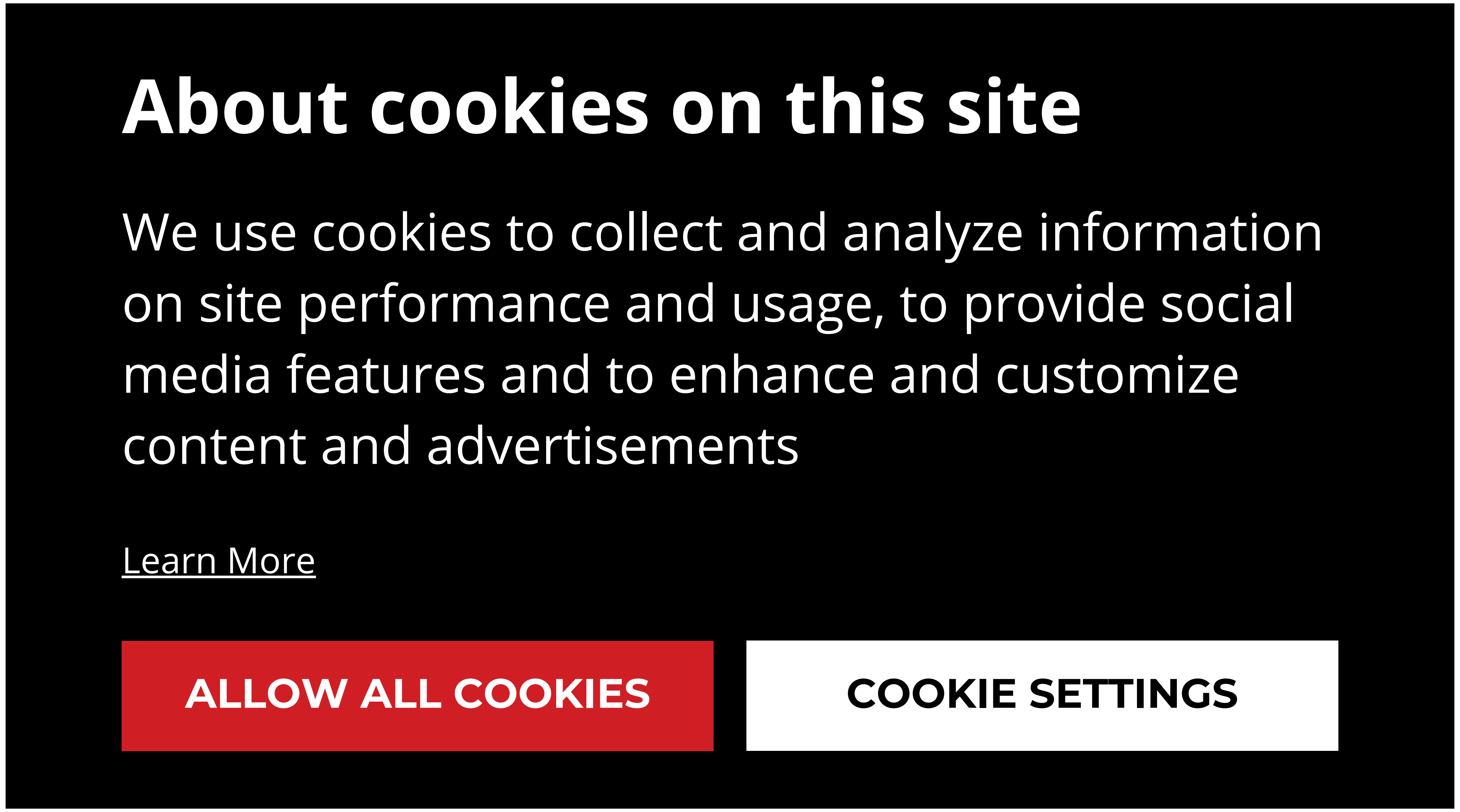
How will your information be protected? Will it be encrypted? Will it be stored outside of Canada? Does the company offer two-step verification or MFA to access the account?

Be Private

How to be #UnHackable: **Be Private**

KnowledgeFlow.org

- You do not have to accept cookies!
- Cyberattacks can hijack cookies and gain access to your browsing sessions



About cookies on this site

We use cookies to collect and analyze information on site performance and usage, to provide social media features and to enhance and customize content and advertisements

Be Private

How to be #UnHackable: **Be Skeptical**

- Use privacy tools that run in your Web browser:

Privacy Badger

ABP AdblockPlus

CleanBrowsing

Be Private

Be Skeptical

How to be #UnHackable: **Be Skeptical**

KnowledgeFlow.org

Caller ID Spoofing

You can **no longer trust** that a caller is legitimate based on caller ID

RCMP
1-833-541-3089
Ontario Provincial Police
905-841-5777
Remind Me
Message
slide to answer
Canada Revenue Agency
1-800-959-8281
Decline
Accept
Department of Finance Canada
1-833-712-2292

Scammers can fake any number and any organization!

The Fraud Department Call

IMPORTANT

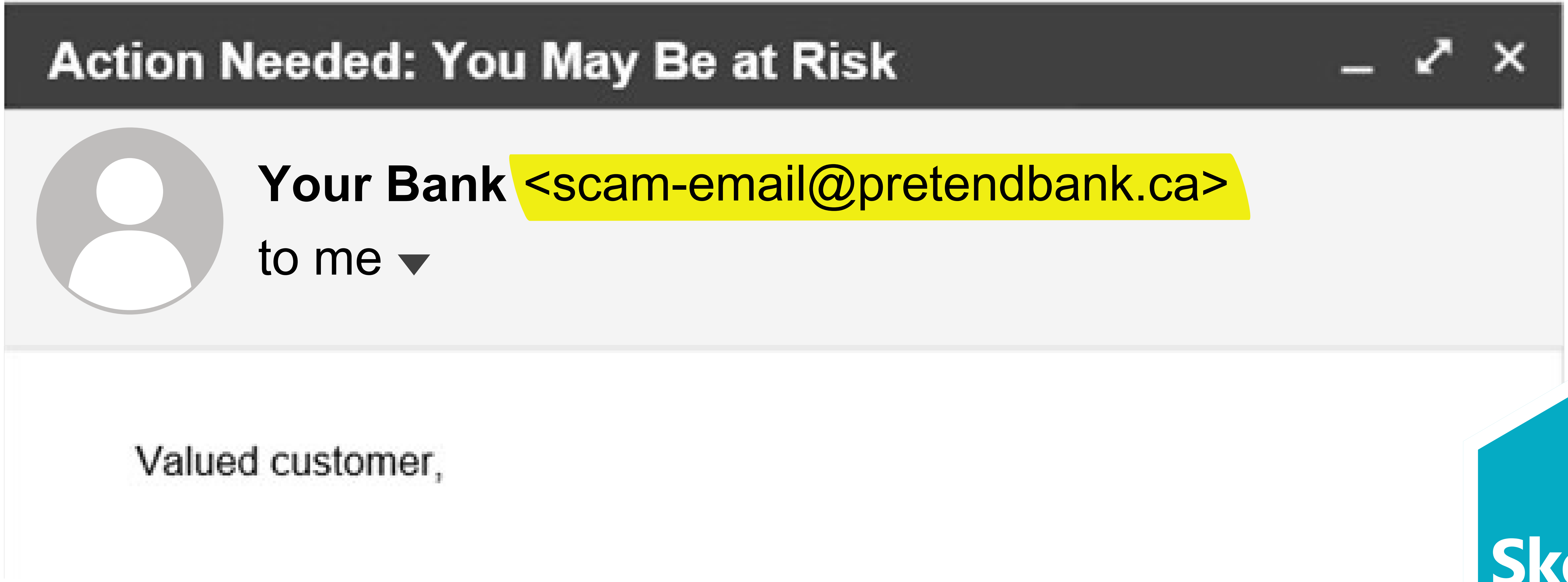
No fraud department should ever ask you to confirm your PIN

Be Skeptical

How to be #UnHackable: **Be Skeptical**

KnowledgeFlow.org

- Be suspicious of 'no-reply' email addresses
- Don't trust the 'email header'



Action Needed: You May Be at Risk

Your Bank <scam-email@pretendbank.ca>

to me ▾

Valued customer,

Be Skeptical

How to be #UnHackable: **Be Skeptical**

KnowledgeFlow.org

Scam Red Flags 🚩

1

Fear, Urgency, Secrecy

2

Authority or Legitimacy

3

Payment (in any form)

4

Personal Information

- Never feel pressured to pay urgently
- Watch for signs of fearmongering
- Ignore requests for secrecy, 'court gag orders', etc.
- Badge numbers, case numbers, employee numbers, logos, company names, department name - can all be made up
- Unexpected requests for payment, refunds, or to dispute charges are all the same - phishing
- Even if they already have some your info - like your name, address, phone number, SIN, health card number - they will want the rest
- Requests to provide or confirm your information are just as sketchy if you did not initiate the call.

Be Secure

How to be #UnHackable: **Be Secure**

KnowledgeFlow.org

Password Checklist

1

UNIQUE

Create a different password for each account

2

STRONG

Long, with capitals, numbers and characters

3

SECURE

Store in a password manager

4

COMPLEX

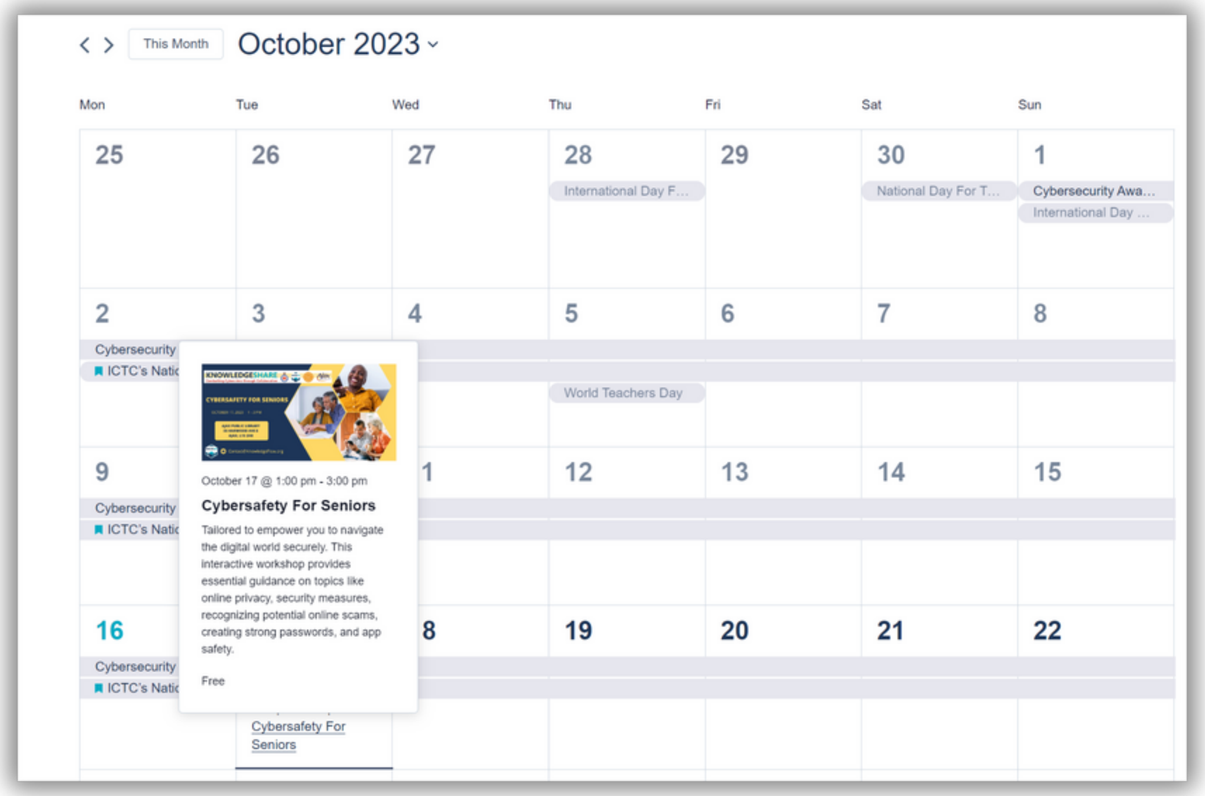
Enable multi-factor authentication

How to be #UnHackable: **Be Secure**

KnowledgeFlow.org

Device Security: 10 Steps To Secure Your Phone, Tablet Or Computer

- See your handout



‹ › This Month October 2023 ˅

Mon	Tue	Wed	Thu	Fri	Sat	Sun
25	26	27	28 International Day F…	29	30 National Day For T…	1 Cybersecurity Awa… International Day …
2 Cybersecurity ICTC's Natic	3	4	5 World Teachers Day	6	7	8
9 Cybersecurity ICTC's Natic		1	12	13	14	15
16 Cybersecurity ICTC's Natic	Cybersafety For Seniors	8	19	20	21	22

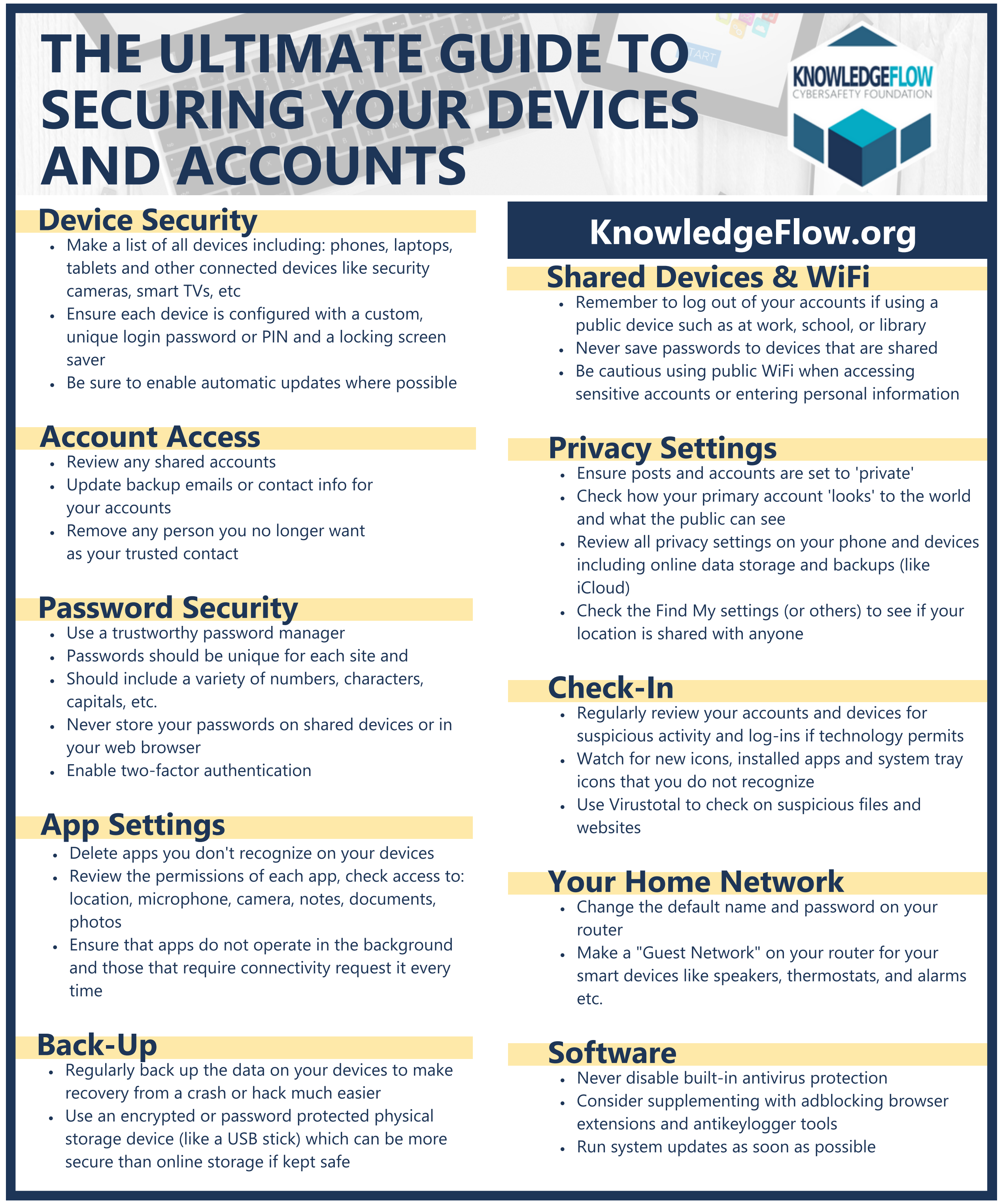
October 17 @ 1:00 pm - 3:00 pm

Cybersafety For Seniors

Tailored to empower you to navigate the digital world securely. This interactive workshop provides essential guidance on topics like online privacy, security measures, recognizing potential online scams, creating strong passwords, and app safety.

Free

KnowledgeFlow.org > Events



THE ULTIMATE GUIDE TO SECURING YOUR DEVICES AND ACCOUNTS

KNOWLEDGEFLOW CYBERSAFETY FOUNDATION

KnowledgeFlow.org

Device Security

- Make a list of all devices including: phones, laptops, tablets and other connected devices like security cameras, smart TVs, etc
- Ensure each device is configured with a custom, unique login password or PIN and a locking screen saver
- Be sure to enable automatic updates where possible

Account Access

- Review any shared accounts
- Update backup emails or contact info for your accounts
- Remove any person you no longer want as your trusted contact

Password Security

- Use a trustworthy password manager
- Passwords should be unique for each site and
- Should include a variety of numbers, characters, capitals, etc.
- Never store your passwords on shared devices or in your web browser
- Enable two-factor authentication

App Settings

- Delete apps you don't recognize on your devices
- Review the permissions of each app, check access to: location, microphone, camera, notes, documents, photos
- Ensure that apps do not operate in the background and those that require connectivity request it every time

Back-Up

- Regularly back up the data on your devices to make recovery from a crash or hack much easier
- Use an encrypted or password protected physical storage device (like a USB stick) which can be more secure than online storage if kept safe

Shared Devices & WiFi

- Remember to log out of your accounts if using a public device such as at work, school, or library
- Never save passwords to devices that are shared
- Be cautious using public WiFi when accessing sensitive accounts or entering personal information

Privacy Settings

- Ensure posts and accounts are set to 'private'
- Check how your primary account 'looks' to the world and what the public can see
- Review all privacy settings on your phone and devices including online data storage and backups (like iCloud)
- Check the Find My settings (or others) to see if your location is shared with anyone

Check-In

- Regularly review your accounts and devices for suspicious activity and log-ins if technology permits
- Watch for new icons, installed apps and system tray icons that you do not recognize
- Use Virustotal to check on suspicious files and websites

Your Home Network

- Change the default name and password on your router
- Make a "Guest Network" on your router for your smart devices like speakers, thermostats, and alarms etc.

Software

- Never disable built-in antivirus protection
- Consider supplementing with adblocking browser extensions and antikeylogger tools
- Run system updates as soon as possible

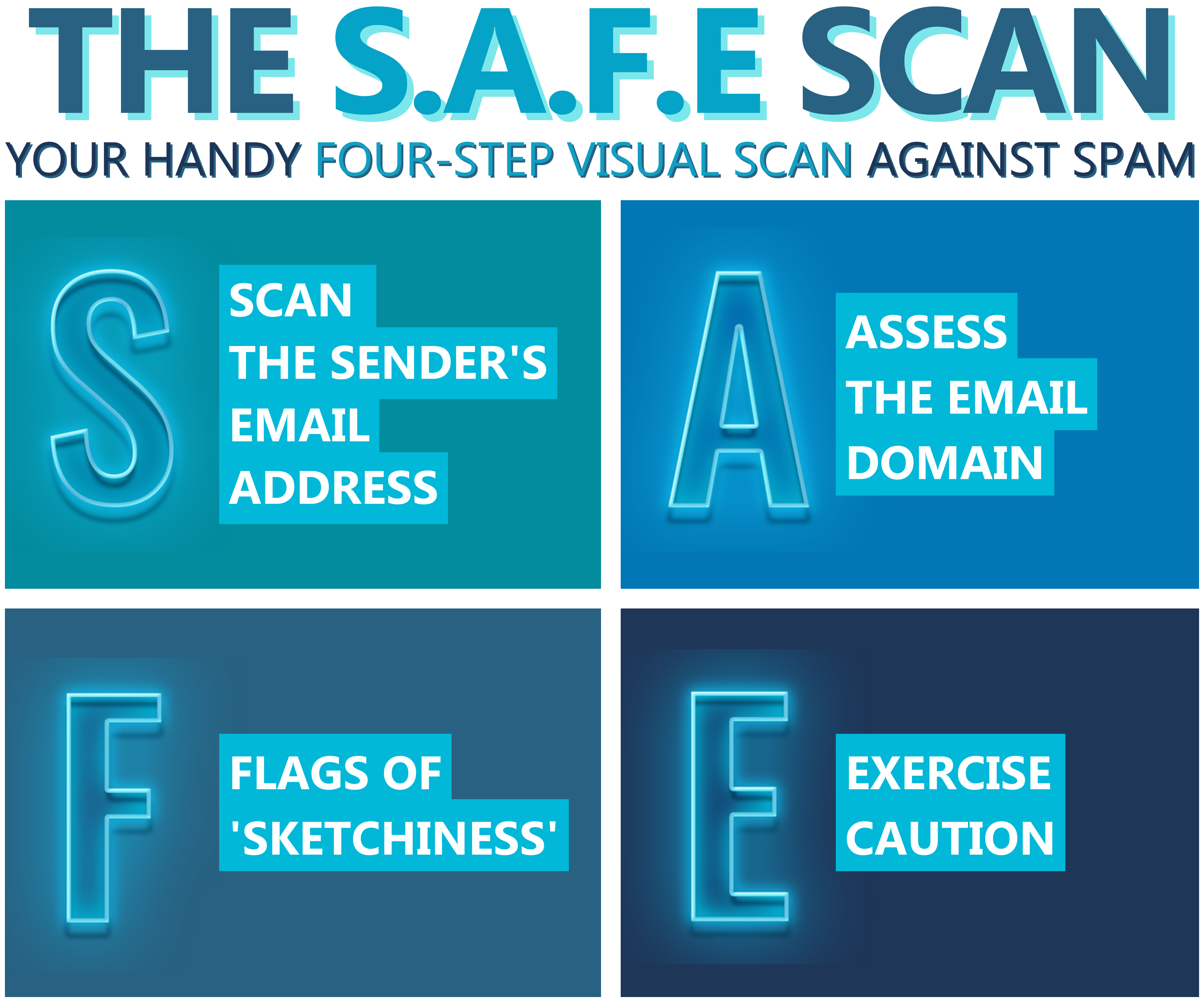
Combatting Cybercrime through Collaboration

Durham Regional Police · Town of Ajax By the Lake · Victim Services Durham Region · KnowledgeFlow

Be Secure

How to be #UnHackable: **Be Secure**

KnowledgeFlow.org



THE S.A.F.E SCAN

YOUR HANDY FOUR-STEP VISUAL SCAN AGAINST SPAM

S — SCAN THE SENDER'S EMAIL ADDRESS

A — ASSESS THE EMAIL DOMAIN

F — FLAGS OF 'SKETCHINESS'

E — EXERCISE CAUTION

Attachments

- There is no such thing as a safe file type! File extensions can be forged.

Be Secure

How to be #UnHackable: **Be Secure**

KnowledgeFlow.org

WHY YOU SHOULD BE USING AD-BLOCKING SOFTWARE

What is Ad-blocking Software? What Does it do?

Ad-blocking software is a tool that stops ads from appearing on your computer or phone. It makes browsing faster and more private, and can prevent you from encountering a malicious ad.

Why Should You be Using Ad-Blocking Software?

Ad-Blocking software is a great addition to your browsing experience. It can help with:

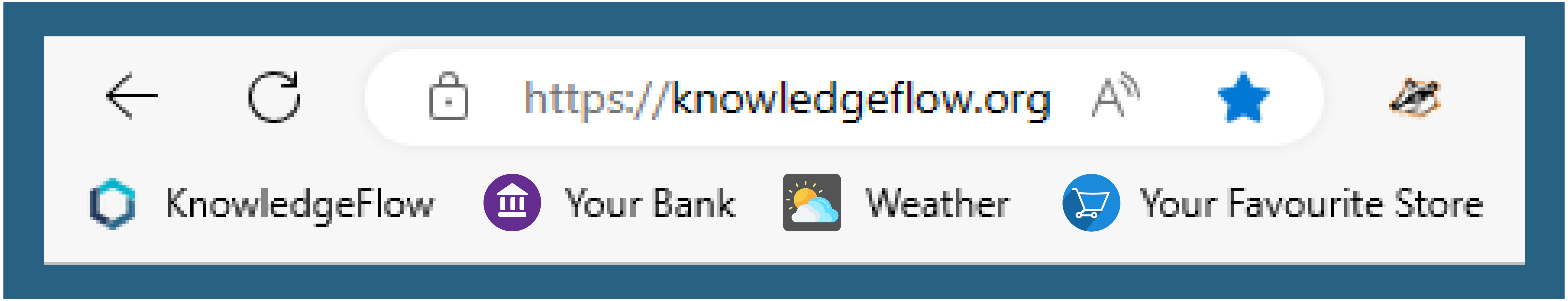
- Improved security by blocking third party trackers, malware, etc.
- Less chance of being affected by malicious ads
- Increased privacy
- Faster browsing

Scammers pay for browser search ads so that they appear before the legitimate ads in searches.

Be Secure

How to be #UnHackable: **Be Secure**

- Use Bookmarks!



https://knowledgeflow.org

KnowledgeFlow Your Bank Weather Your Favourite Store

- Do not trust links in emails.

✓ **Real URL**
KNOWLEDGEFLOW.ORG

✗ **Scam URL**
KN0WLEDGEFL0W.ORG

Be Secure

How to be #UnHackable: **Be Secure**

KnowledgeFlow.org

- Never allow strangers to remotely access your device.

- If you receive a pop-up notice, don't click on it - turn off your device

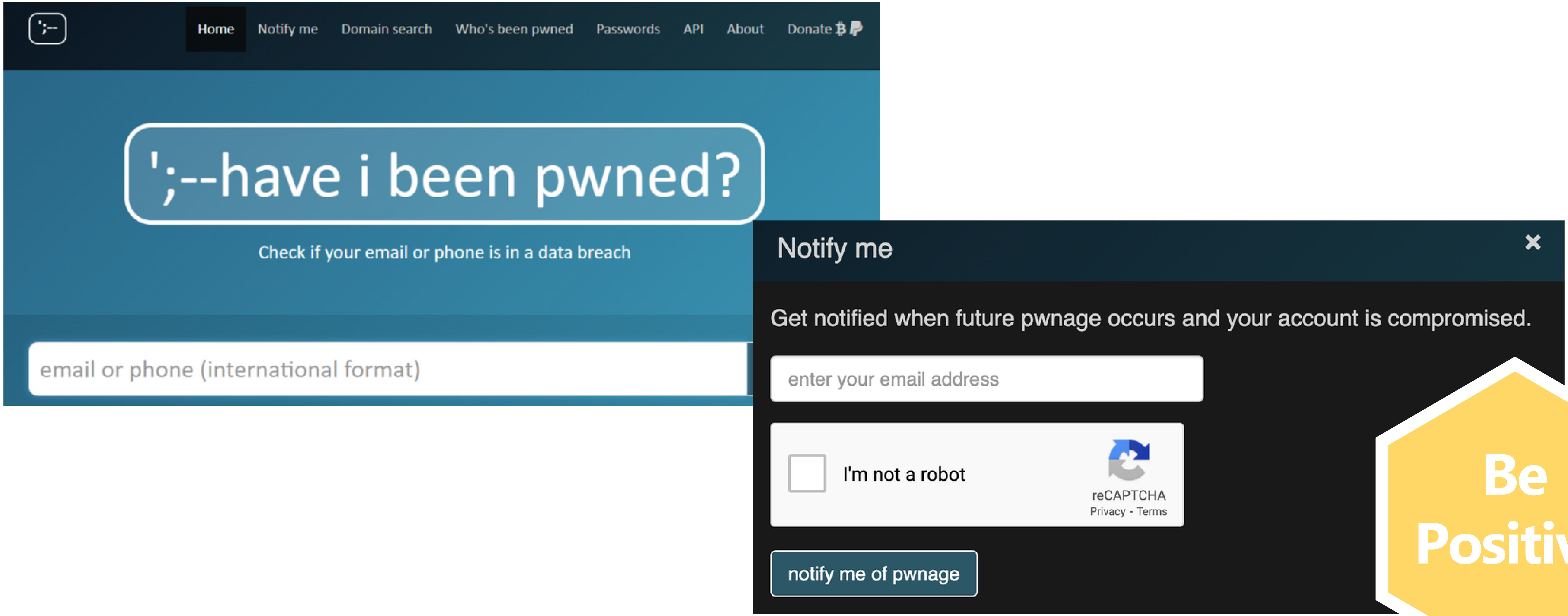
Be Secure

Be Positive

How to be #UnHackable: **Be Positive**

KnowledgeFlow.org

Get Notified 🔔



';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

Notify me ×

Get notified when future pwnage occurs and your account is compromised.

enter your email address

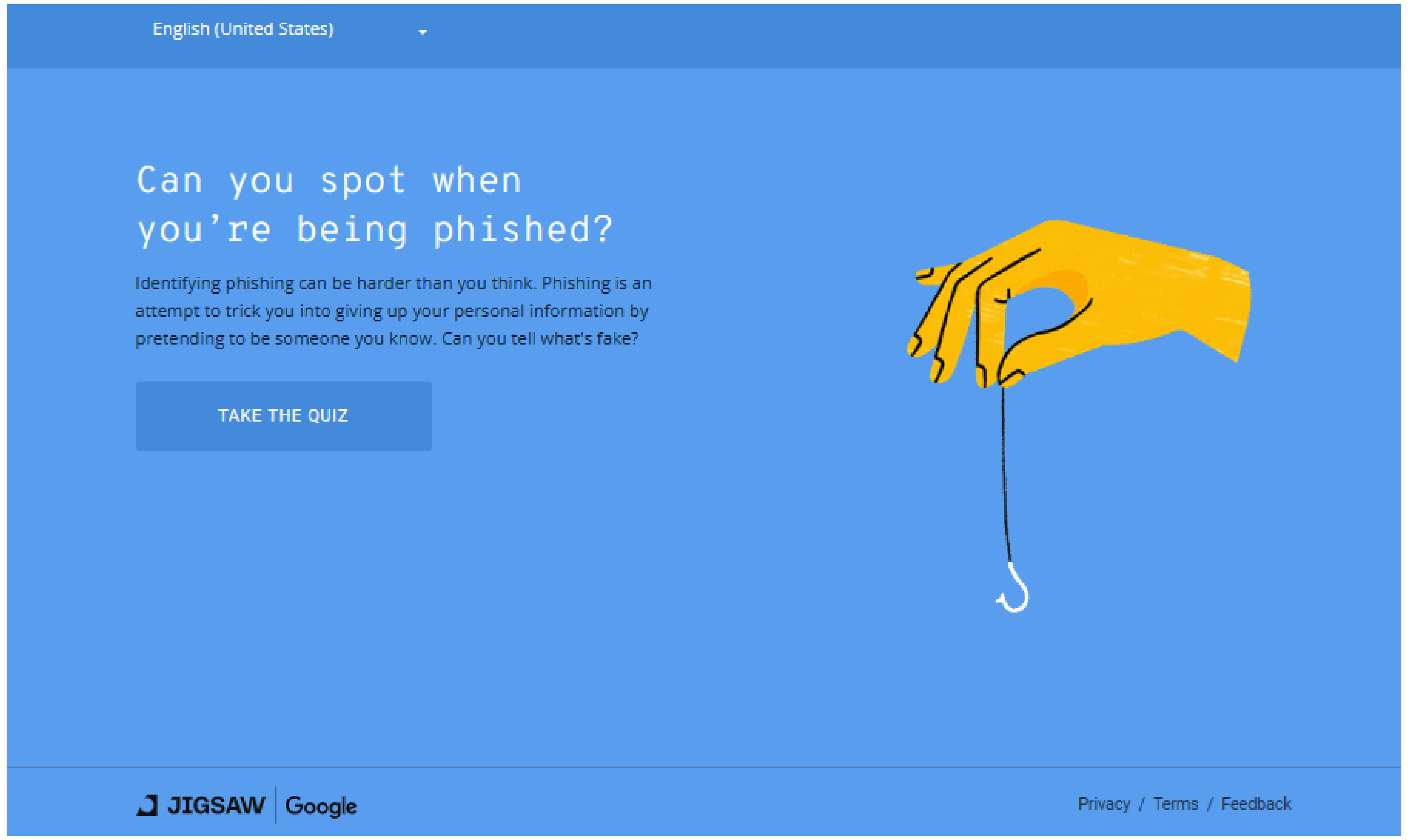
□ I'm not a robot

Be Positive

How to be #UnHackable: **Be Positive**

KnowledgeFlow.org

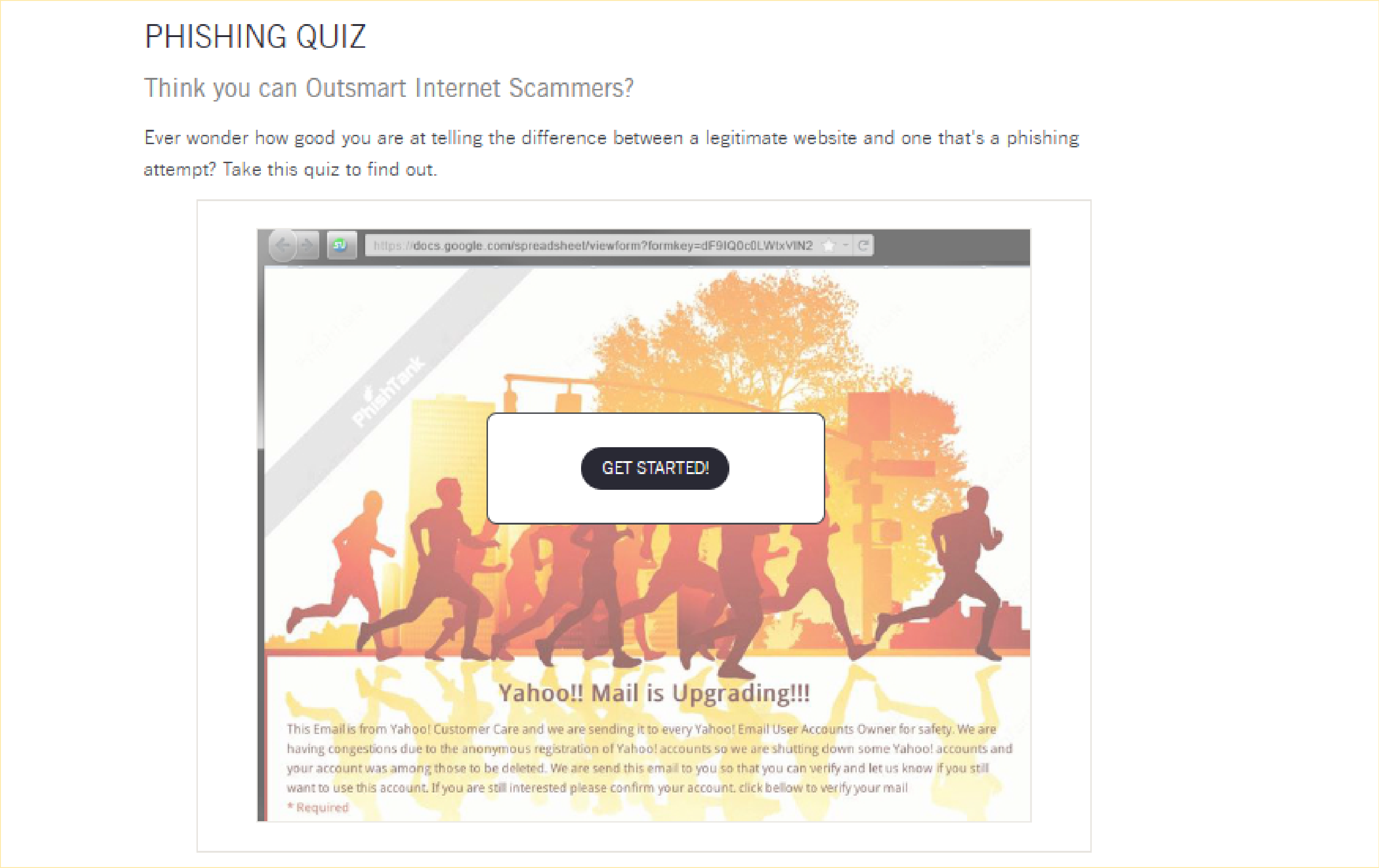
Test Yourself



Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

phishingquiz.withgoogle.com



PHISHING QUIZ

Think you can Outsmart Internet Scammers?

Ever wonder how good you are at telling the difference between a legitimate website and one that's a phishing attempt? Take this quiz to find out.

https://docs.google.com/spreadsheet/viewform?formkey=dF9IQ0c0LWIxVIN2
PhishTank
GET STARTED!

Yahoo!! Mail is Upgrading!!!

This Email is from Yahoo! Customer Care and we are sending it to every Yahoo! Email User Accounts Owner for safety. We are having congestions due to the anonymous registration of Yahoo! accounts so we are shutting down some Yahoo! accounts and your account was among those to be deleted. We are send this email to you so that you can verify and let us know if you still want to use this account. If you are still interested please confirm your account. click bellow to verify your mail

* Required

opendns.com/phishing-quiz

Be Positive

How to be #UnHackable: **Be Positive**

KnowledgeFlow.org

FREE

Protect Your Device

Cybersafety for Everyone

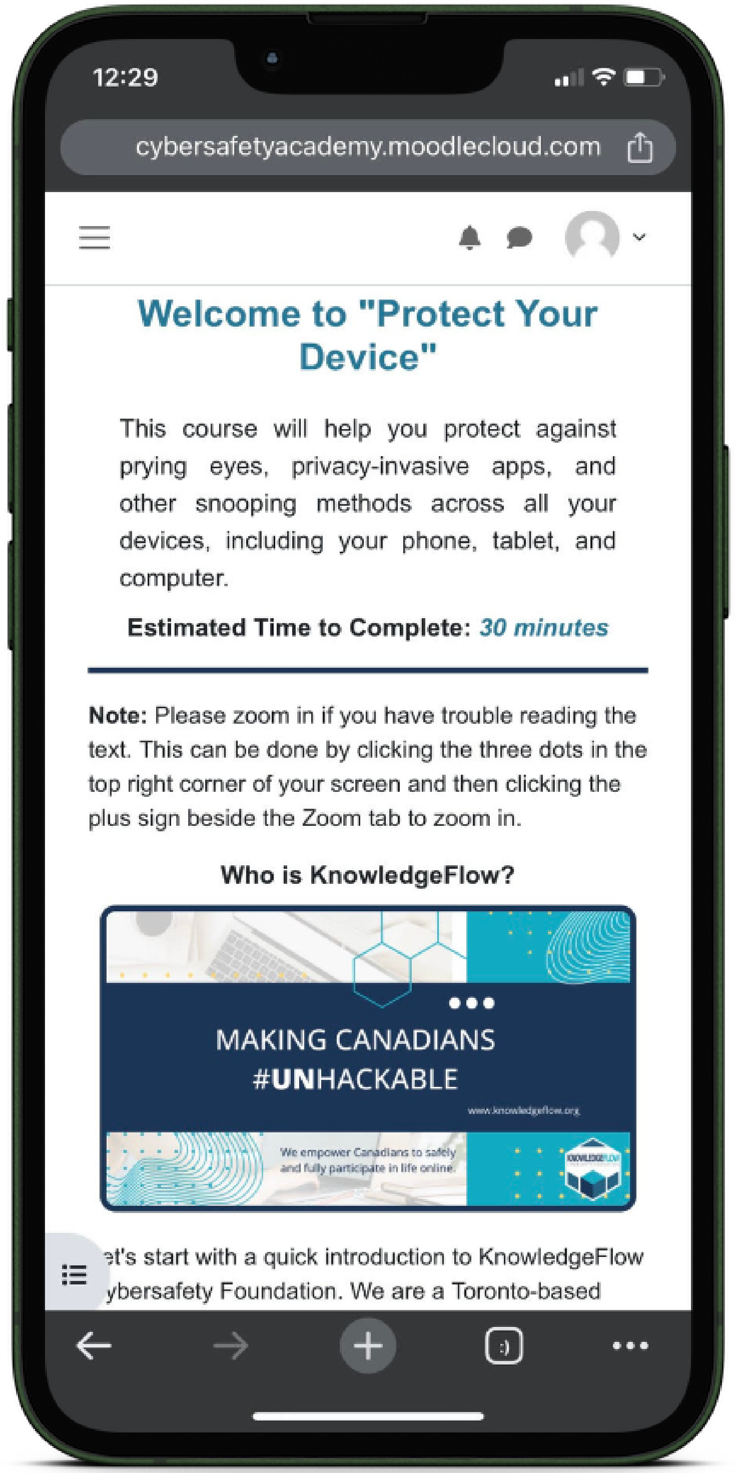
Protect Your Information

Cybersafety for Everyone

Scams: Spot Them and Stop Them

Cybersafety for Everyone

CybersafetyAcademy.ca



Welcome to "Protect Your Device"

This course will help you protect against prying eyes, privacy-invasive apps, and other snooping methods across all your devices, including your phone, tablet, and computer.

Estimated Time to Complete: *30 minutes*

Note: Please zoom in if you have trouble reading the text. This can be done by clicking the three dots in the top right corner of your screen and then clicking the plus sign beside the Zoom tab to zoom in.

Who is KnowledgeFlow?

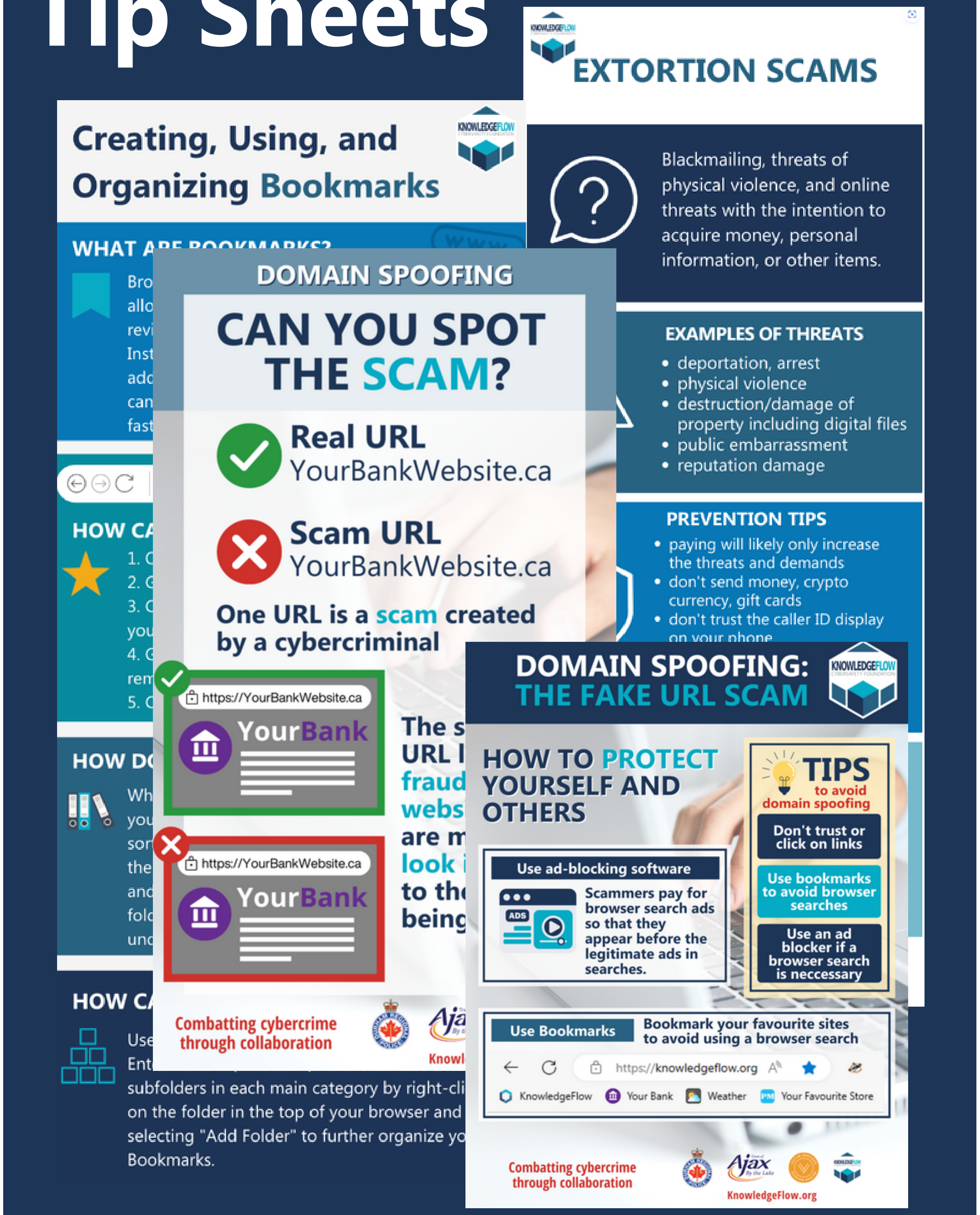
MAKING CANADIANS
#UNHACKABLE
www.knowledgeflow.org
We empower Canadians to safely and fully participate in life online.

et's start with a quick introduction to KnowledgeFlow ybersafety Foundation. We are a Toronto-based

How to be #UnHackable: **Be Positive**

KnowledgeFlow.org

Tip Sheets



EXTORTION SCAMS

Blackmailing, threats of physical violence, and online threats with the intention to acquire money, personal information, or other items.

EXAMPLES OF THREATS
- deportation, arrest
- physical violence
- destruction/damage of property including digital files
- public embarrassment
- reputation damage

PREVENTION TIPS
- paying will likely only increase the threats and demands
- don't send money, crypto currency, gift cards
- don't trust the caller ID display on your phone

Creating, Using, and Organizing Bookmarks

WHAT ARE BOOKMARKS?

HOW CA

HOW DO

HOW CA

subfolders in each main category by right-cli on the folder in the top of your browser and selecting "Add Folder" to further organize yo Bookmarks.

DOMAIN SPOOFING

CAN YOU SPOT THE SCAM?

Real URL YourBankWebsite.ca

Scam URL YourBankWebsite.ca

One URL is a scam created by a cybercriminal

https://YourBankWebsite.ca YourBank

https://YourBankWebsite.ca YourBank

Combatting cybercrime through collaboration

DOMAIN SPOOFING: THE FAKE URL SCAM

HOW TO PROTECT YOURSELF AND OTHERS

TIPS to avoid domain spoofing

Don't trust or click on links

Use bookmarks to avoid browser searches

Use an ad blocker if a browser search is neccessary

Use ad-blocking software

Scammers pay for browser search ads so that they appear before the legitimate ads in searches.

Use Bookmarks — Bookmark your favourite sites to avoid using a browser search

https://knowledgeflow.org

KnowledgeFlow · Your Bank · Weather · Your Favourite Store

Combatting cybercrime through collaboration

KnowledgeFlow.org

Visuals

SYNTHETIC IDENTITY THE

Visit our website for more information!

Represents 88.3% of all identity fraud events

Often targets children's SIN numbers

Is the fastest-growing financial crime

Combatting cybercrime through collaboration

KnowledgeFlow.org

Caller ID Spoofing

You can no longer trust that a caller is legitimate based on caller ID

RCMP 1-833-541-3089

Ontario Provincial Police 905-841-5777

Canada Revenue Agency 1-800-959-8281

Department of Finance Canada 1-833-712-2292

Scammers can fake any number and any organization!

The Fraud Department Call

You Receive a Call

The Scammer Provides In

"Rep" Claims Unusual Ac

They Send you a Code

IMPORTANT: No fraud department should ever ask you

KnowledgeFlow.org

Combatting cybercrime through collaboration

KnowledgeFlow.org

What's The Harm?

Reusing Passwords on Multiple Accounts

LOGIN ****

Tutorials

Scams And Fraud

Scams and Fraud: How to spot them and stop them. This video will help you protect yourself against all kinds of scams and fraud including online and digital scams. This video will demonstrate how to detect fraud in it's various forms, how to protect yourself against them and how to correct or respond to fraud attempts when they happen.

Scams and Fraud — Spot them and Stop them

Protect · Detect · Correct · #UnHackable

#CyberAMA ASK ME ANYTHING

Grades 1- Cybersafety Champion Program

"A rare treat!" "Do not miss your chance to engage with podcaster, educator, author and cyber security expert, Claudiu Popa.".

Managed Privacy

Cybersafety Champion #CyberAMA with KCF Co-Founder, Claudiu Popa, hosted by Markham Public Library

Knowledge Flow Cybersafety Foundation · Subscribe

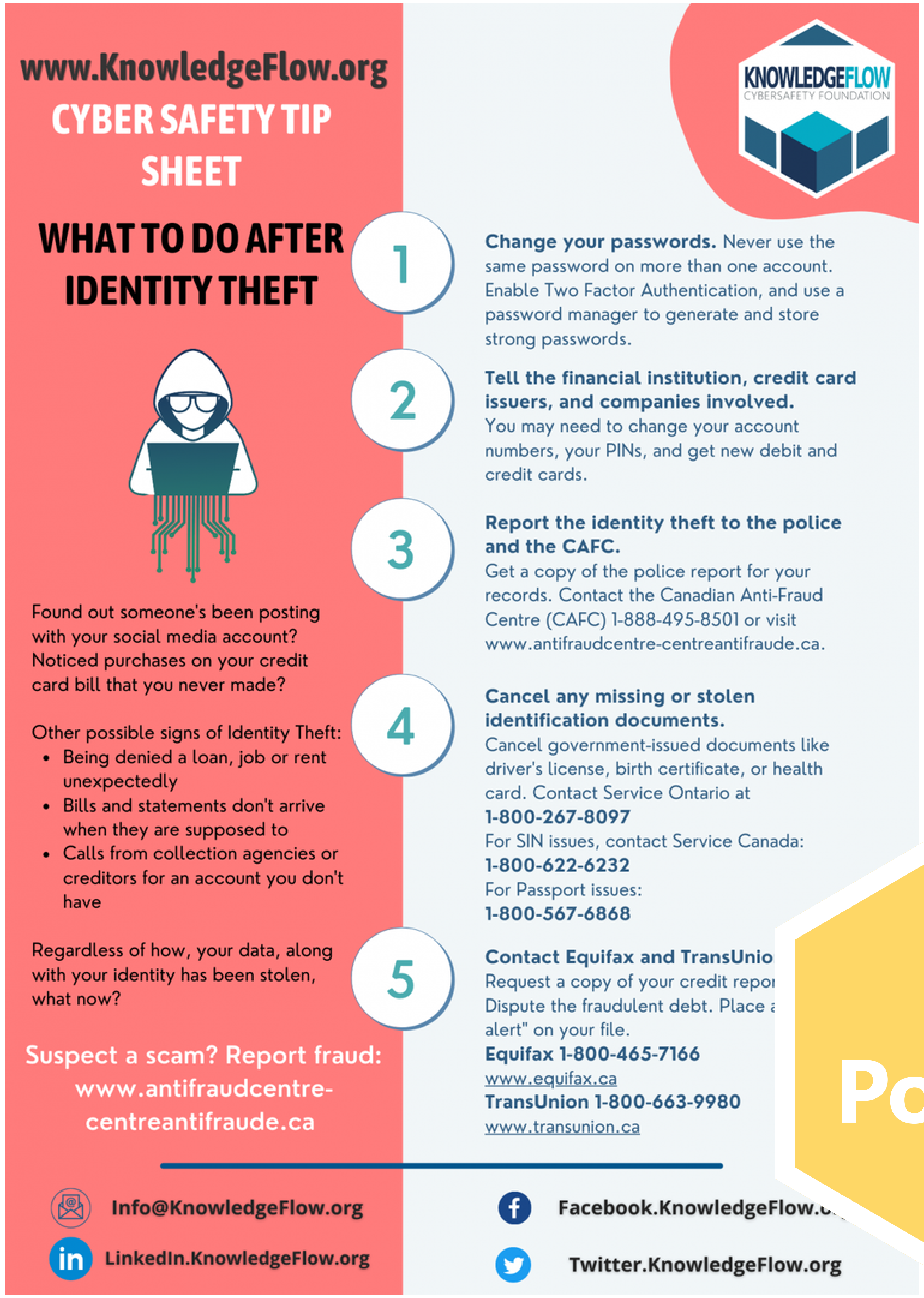
Be Positive

How to be #UnHackable: **Be Positive**

KnowledgeFlow.org

Report Concerns to:

- Canadian Anti-Fraud Centre
- Your bank & Credit Card Company
- Local police department
- Equifax and Transunion for credit alerts
- CRTC - regarding spam emails
- 7726 - forward spam texts
- Federal Privacy Commissioner
- Provincial Privacy Commissioner



www.KnowledgeFlow.org

CYBER SAFETY TIP SHEET

WHAT TO DO AFTER IDENTITY THEFT

KNOWLEDGEFLOW
CYBERSAFETY FOUNDATION

Found out someone's been posting with your social media account? Noticed purchases on your credit card bill that you never made?

Other possible signs of Identity Theft:
- Being denied a loan, job or rent unexpectedly
- Bills and statements don't arrive when they are supposed to
- Calls from collection agencies or creditors for an account you don't have

Regardless of how, your data, along with your identity has been stolen, what now?

Suspect a scam? Report fraud: www.antifraudcentre-centreantifraude.ca

1 **Change your passwords.** Never use the same password on more than one account. Enable Two Factor Authentication, and use a password manager to generate and store strong passwords.

2 **Tell the financial institution, credit card issuers, and companies involved.** You may need to change your account numbers, your PINs, and get new debit and credit cards.

3 **Report the identity theft to the police and the CAFC.** Get a copy of the police report for your records. Contact the Canadian Anti-Fraud Centre (CAFC) 1-888-495-8501 or visit www.antifraudcentre-centreantifraude.ca.

4 **Cancel any missing or stolen identification documents.** Cancel government-issued documents like driver's license, birth certificate, or health card. Contact Service Ontario at **1-800-267-8097** For SIN issues, contact Service Canada: **1-800-622-6232** For Passport issues: **1-800-567-6868**

5 **Contact Equifax and TransUnio** Request a copy of your credit repor Dispute the fraudulent debt. Place a alert" on your file. **Equifax 1-800-465-7166** www.equifax.ca **TransUnion 1-800-663-9980** www.transunion.ca

✉ Info@KnowledgeFlow.org

in LinkedIn.KnowledgeFlow.org

f Facebook.KnowledgeFlow.o

Twitter.KnowledgeFlow.org

Be Positive

Newcomers to Canada: Support Services

211 Ontario®

211 Ontario is a free and confidential service that connects people to social and community supports.

211ontario.ca

Call: 2-1-1

Get Cyber Safe

Get Cyber Safe is a national public awareness campaign about cybersecurity and how to protect yourself online.

www.getcybersafe.gc.ca

Free Newcomer Services

Find newcomer community support in your area. Get support with job searches, language classes, residence searching, and more.

ircc.canada.ca

Stay In Touch!

Thank You!

info@KnowledgeFlow.org

www.KnowledgeFlow.org

facebook.KnowledgeFlow.org

instagram.KnowledgeFlow.org

linkedin.KnowledgeFlow.org

twitter.KnowledgeFlow.org

youtube.KnowledgeFlow.org