Healthy Aging Education Series
"Cyber Security (Part 1)"

DATE: November 1, 2023 & December 6, 2023
SUMMERVILLE FAMILY HEALTH TEAM/PEEL SENIOR LINK

Asurtec

Asurtec Team Members

Cathy Timlin

Quality Assurance, Training and Organizational Development Director with Asurtec Technology Solutions

Bill LeBlanc

Chief Operations Officer with Asurtec Technology Solutions

OUR TOPICS

Part 1: Protecting Yourself from Online Scams

01. **Online Scams/Social Engineering**
Email Phishing and SMiShing

Part 2: Protecting Your Privacy against Cybercriminals

02. **Social Engineering Scams**
Vishing

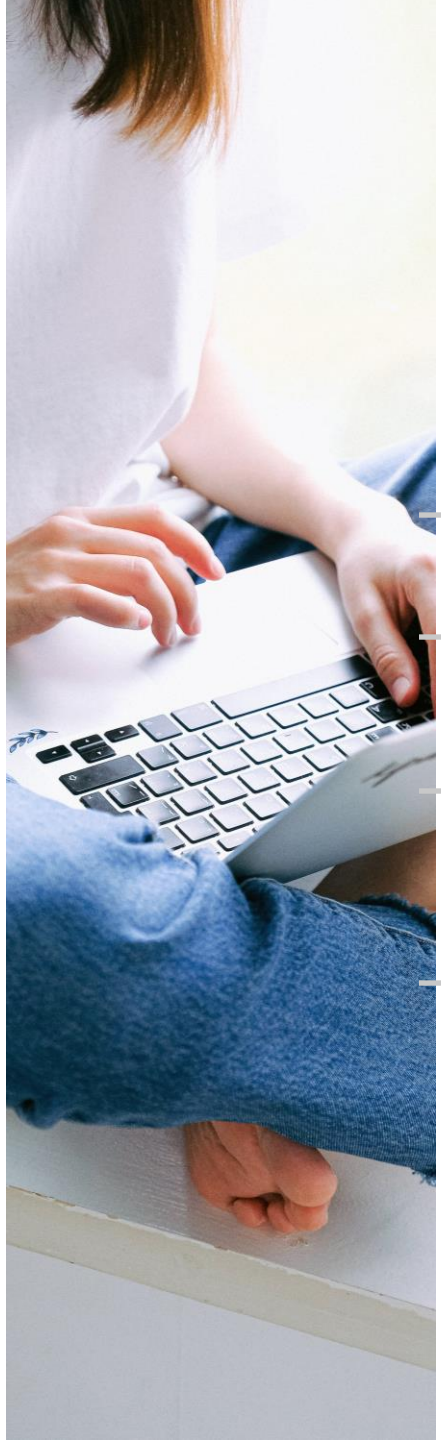
03. **Password Protection**

04. **Social Media**

05. **Privacy 101**

INTRODUCTION QUESTION

CYBERSECURITY



What is the importance of cybersecurity training and how can it enhance your online safety?

a. Cyber training varies depending on an individual's preferences and needs.

b. Cyber training is overrated because modern technology is designed to be user-friendly and secure, so users don't need specialized knowledge

c. The significance of cyber training is a matter of personal interpretation. Whether it enhances online safety is open to debate and depends on various factors

d. Training is crucial in today's digital age to help users understand and mitigate online risks

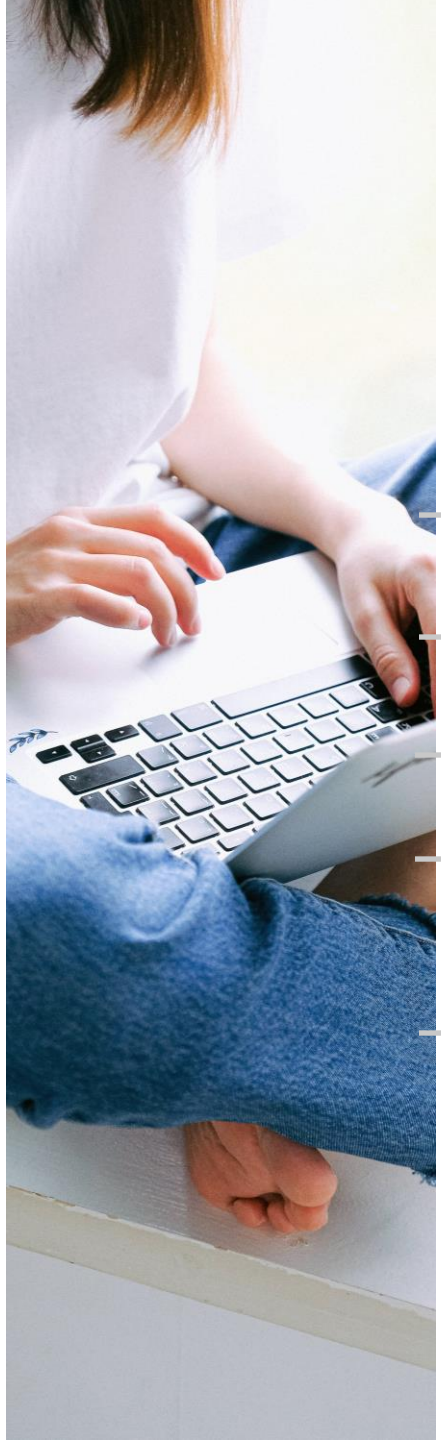
ONLINE/SOCIAL ENGINEERING SCAMS

"Phishing Emails"

Asurtec

QUESTION

CYBERSECURITY



What is Social Engineering?

a. It is a method of connecting with new friends and acquaintances on social media

b. It is a way to strengthen our social skills and adapt to the digital age.

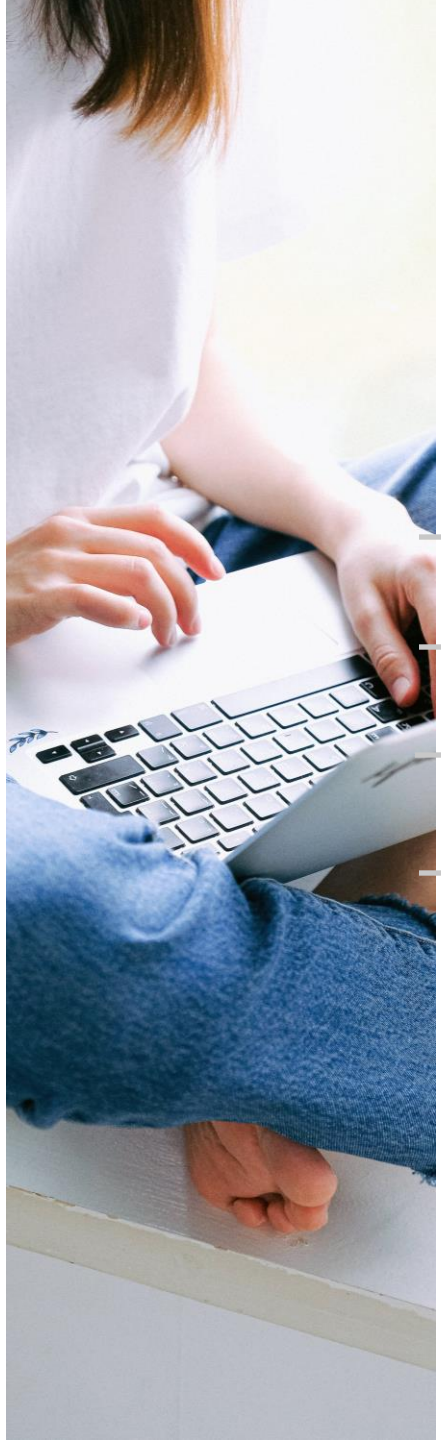
c. It is a tactic used by cybercriminals to manipulate individuals into revealing confidential information.

d. It is an art form where people should engage with telemarketers and provide them with personal information to practice our communication skills.

e. It is an advanced online dating technique for people.

INTRODUCTION QUESTION

CYBERSECURITY



What are some practical steps you can take to protect against social engineering and online scams?

a. Education and Awareness

b. Use reputable websites

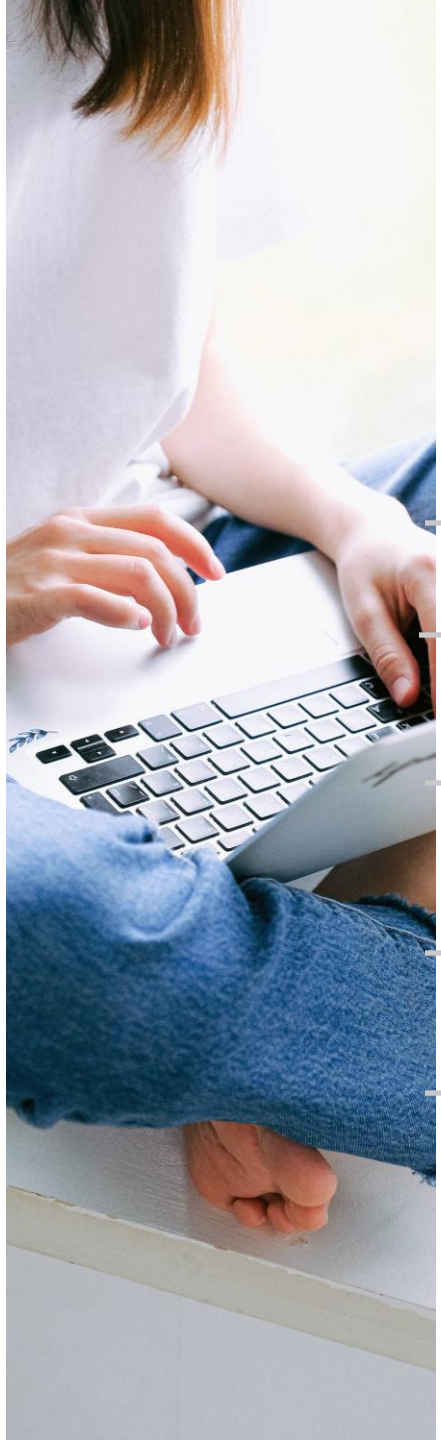
c. Avoid sharing personal information

d. All of the above

Asurtec

Phishing Attacks

CYBERSECURITY



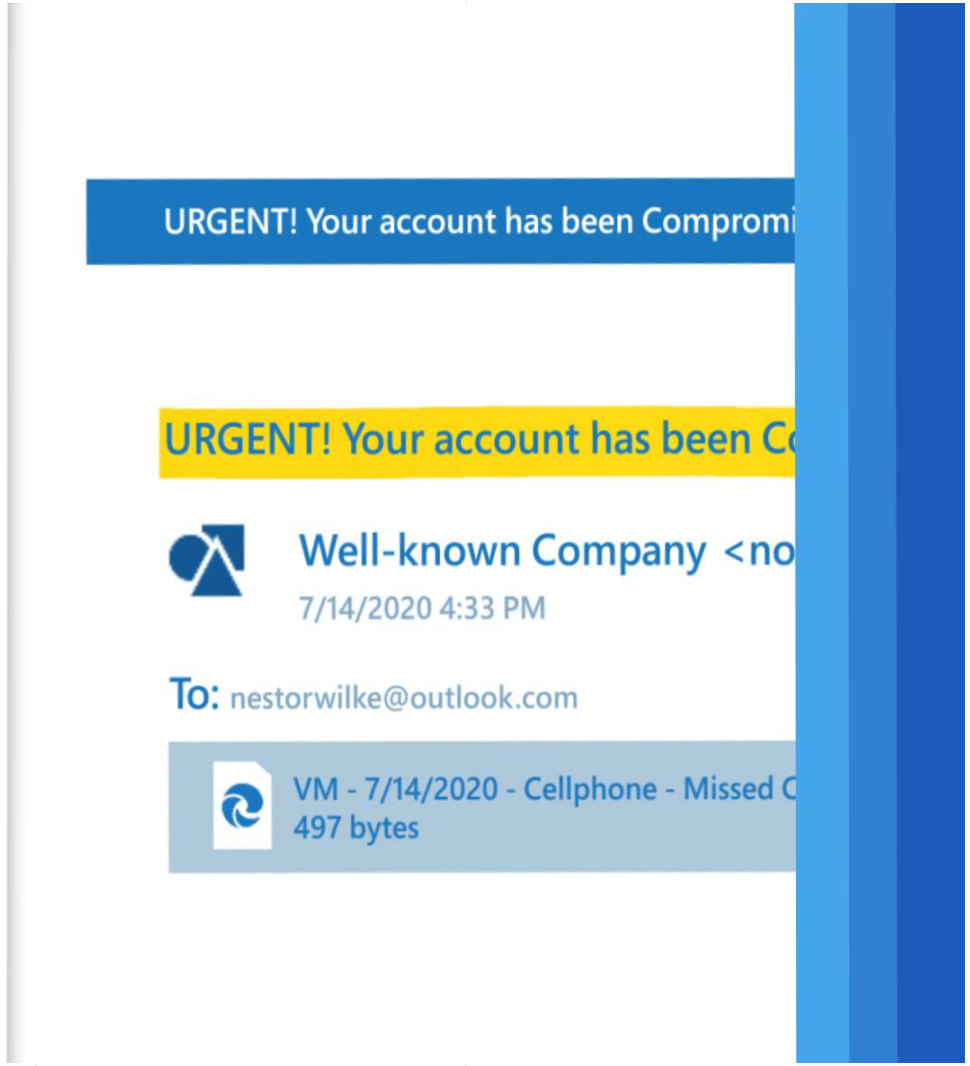
What's changed?

- Cybercriminals are leveraging the popularity of legitimate brands to impersonate those companies i.e. Microsoft
- Emails are crafted using urgency from trusted brands and as a result its enough to trick users into giving up their credentials
- Impersonation is likely to become worse with the increase in reliance on Artificial Intelligence like CHAT GPT and other AI tools
- Phishing attacks are effective because the emails look more legitimate, and they continue to find new subjects for phishing emails i.e. QR codes
- The most commonly used words in phishing emails are: important, attention, urgent, and important updates

Social Engineering Scams

What are they, how to recognize them

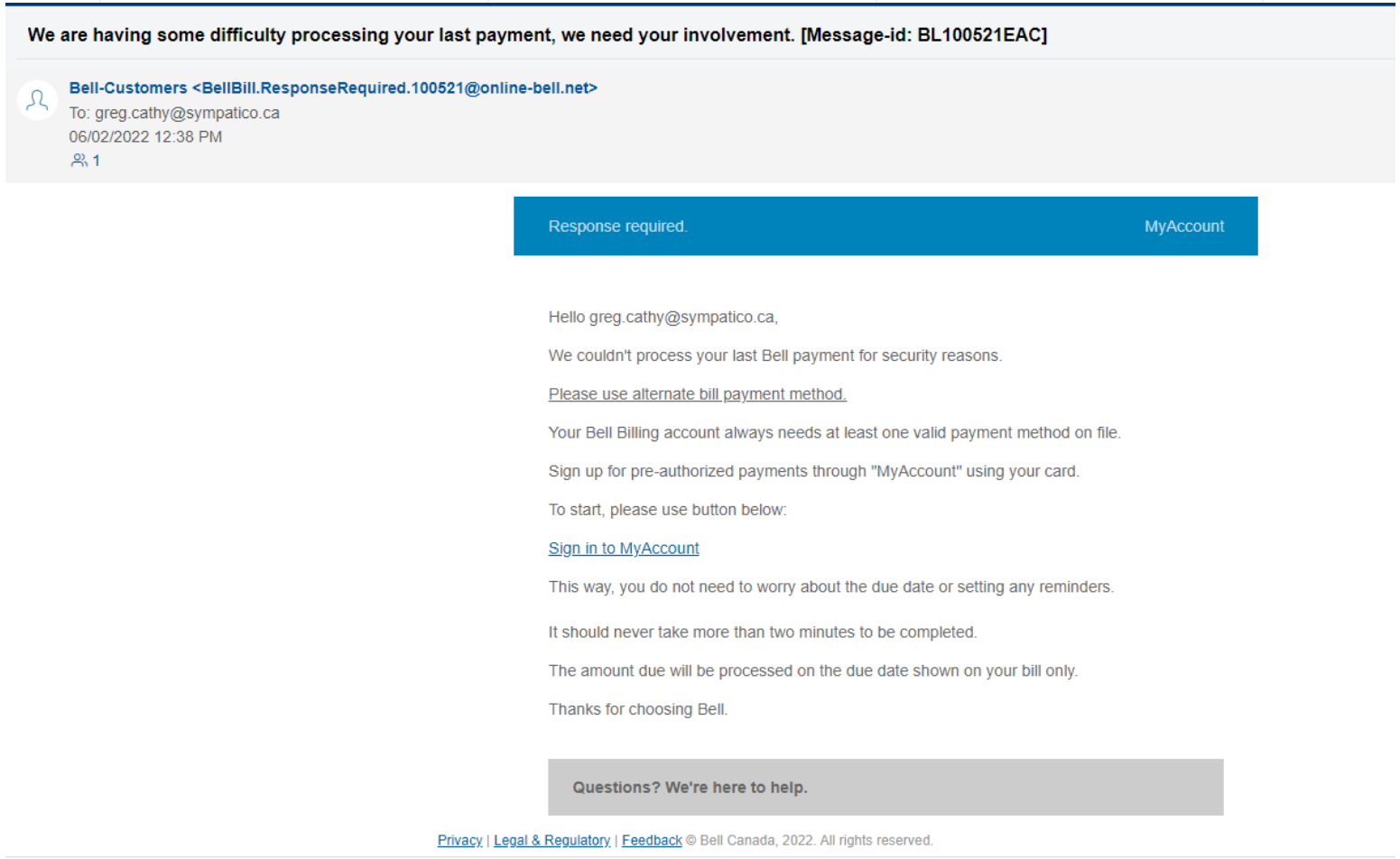
What is phishing?



Email Phishing Attacks

What are they and how to recognize them

Phishing Email Example



We are having some difficulty processing your last payment, we need your involvement. [Message-id: BL100521EAC]

Bell-Customers <BellBill.ResponseRequired.100521@online-bell.net>
To: greg.cathy@sympatico.ca
06/02/2022 12:38 PM
1

Response required. MyAccount

Hello greg.cathy@sympatico.ca,

We couldn't process your last Bell payment for security reasons.

Please use alternate bill payment method.

Your Bell Billing account always needs at least one valid payment method on file.

Sign up for pre-authorized payments through "MyAccount" using your card.

To start, please use button below:

Sign in to MyAccount

This way, you do not need to worry about the due date or setting any reminders.

It should never take more than two minutes to be completed.

The amount due will be processed on the due date shown on your bill only.

Thanks for choosing Bell.

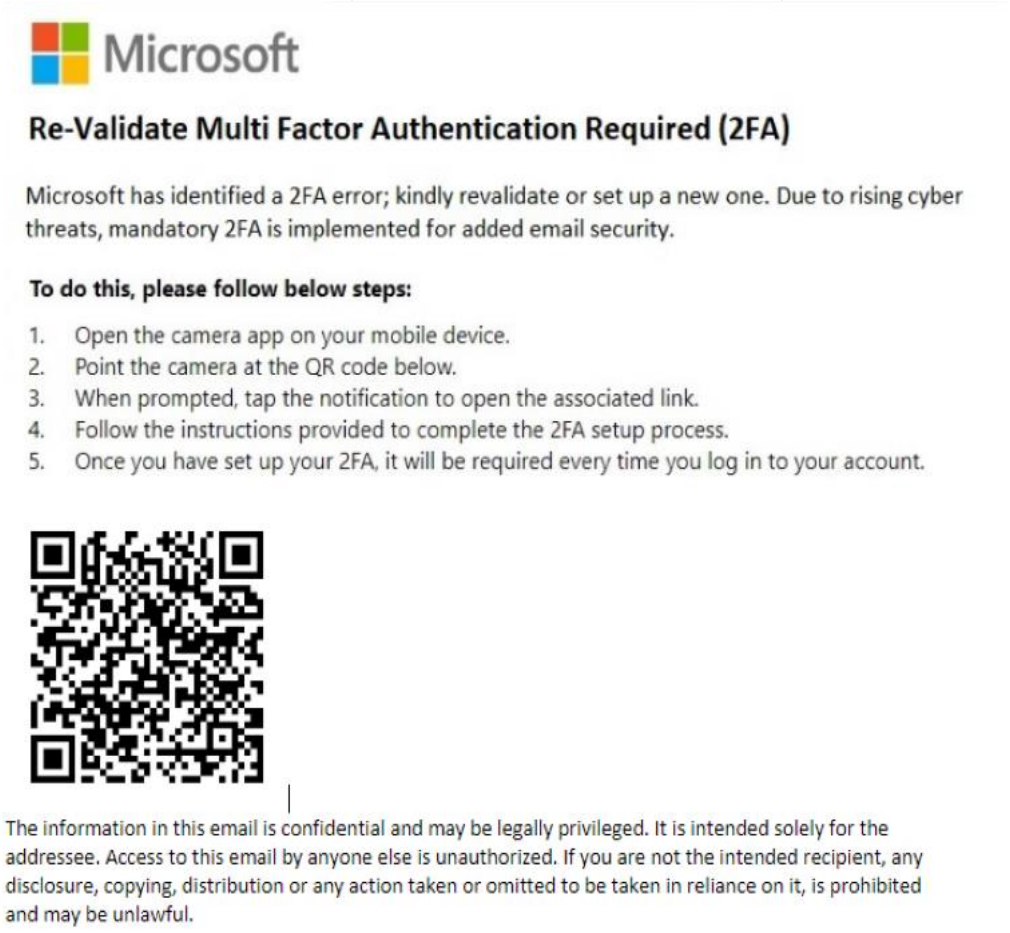
Questions? We're here to help.

Privacy | Legal & Regulatory | Feedback © Bell Canada, 2022. All rights reserved.

Email Phishing Attacks

What are they and how to recognize them

Phishing Email Example



Microsoft

Re-Validate Multi Factor Authentication Required (2FA)

Microsoft has identified a 2FA error; kindly revalidate or set up a new one. Due to rising cyber threats, mandatory 2FA is implemented for added email security.

To do this, please follow below steps:

1. Open the camera app on your mobile device.
2. Point the camera at the QR code below.
3. When prompted, tap the notification to open the associated link.
4. Follow the instructions provided to complete the 2FA setup process.
5. Once you have set up your 2FA, it will be required every time you log in to your account.

The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.

Asurtec

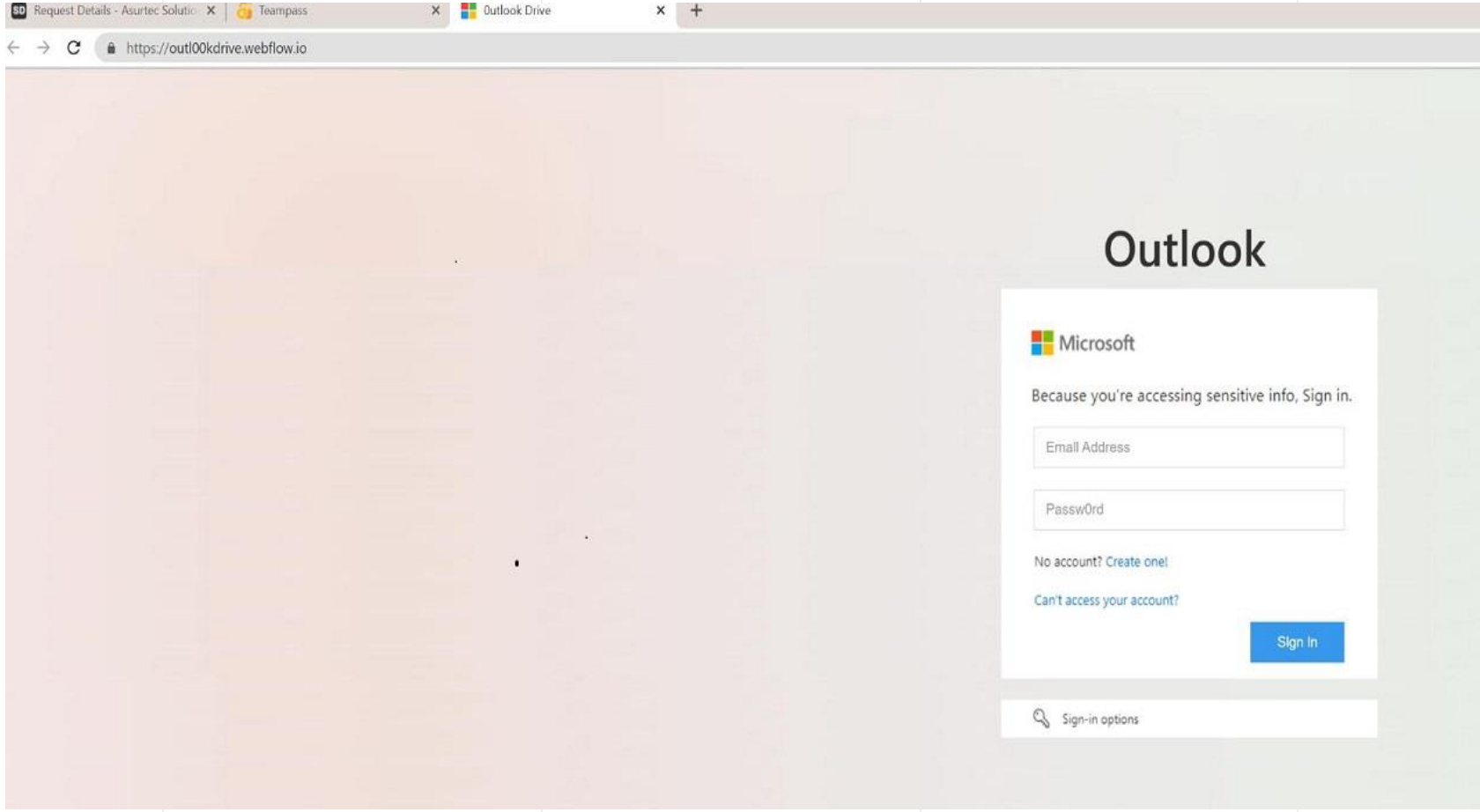
Email Phishing

What are they and how to recognize them

- TIP – always hover over the URL address to ensure it looks authentic

  Web address:

  https://outl00kdrive.webflow.io

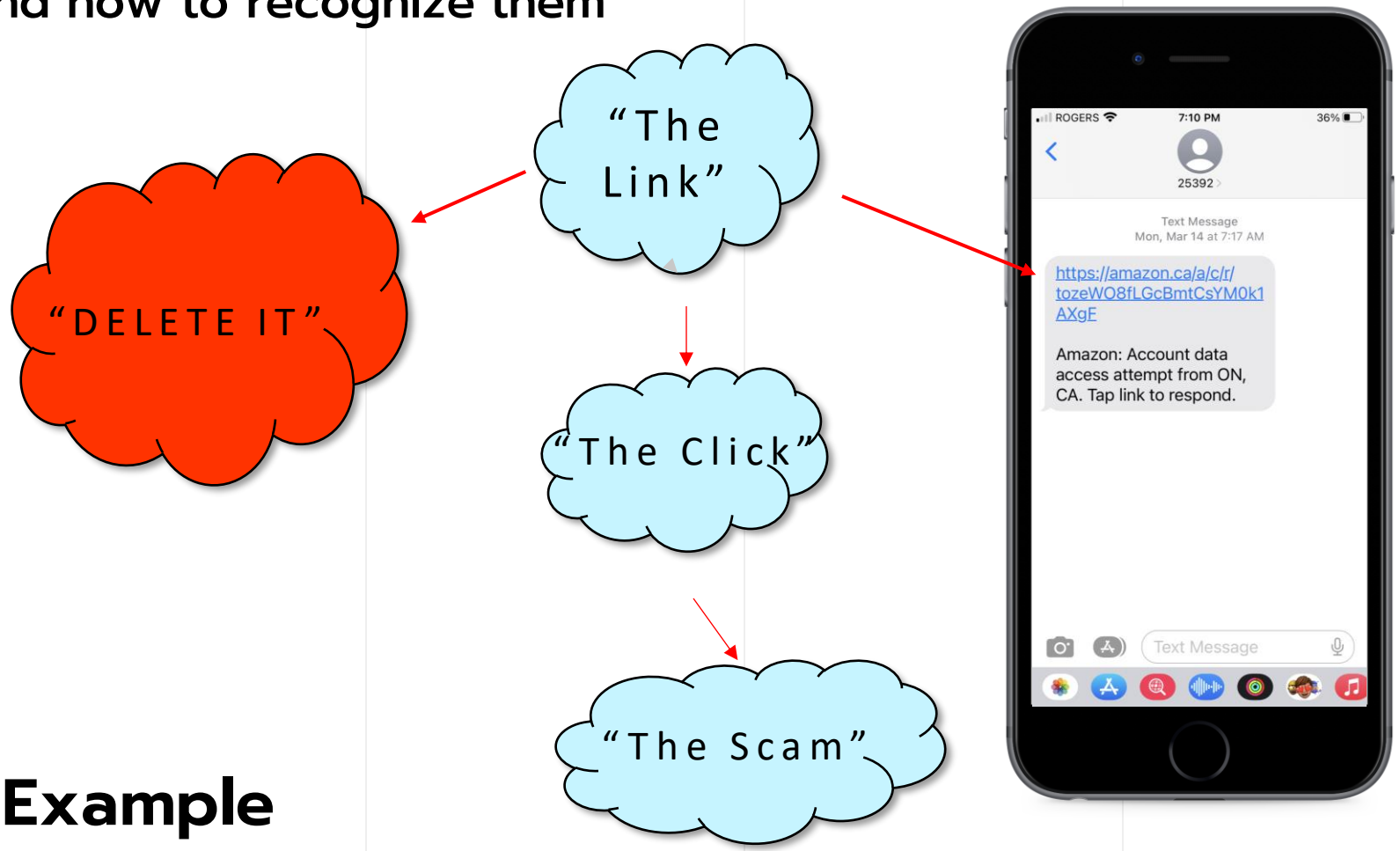


Online/Social Engineering SCAMS

"SMiShING"

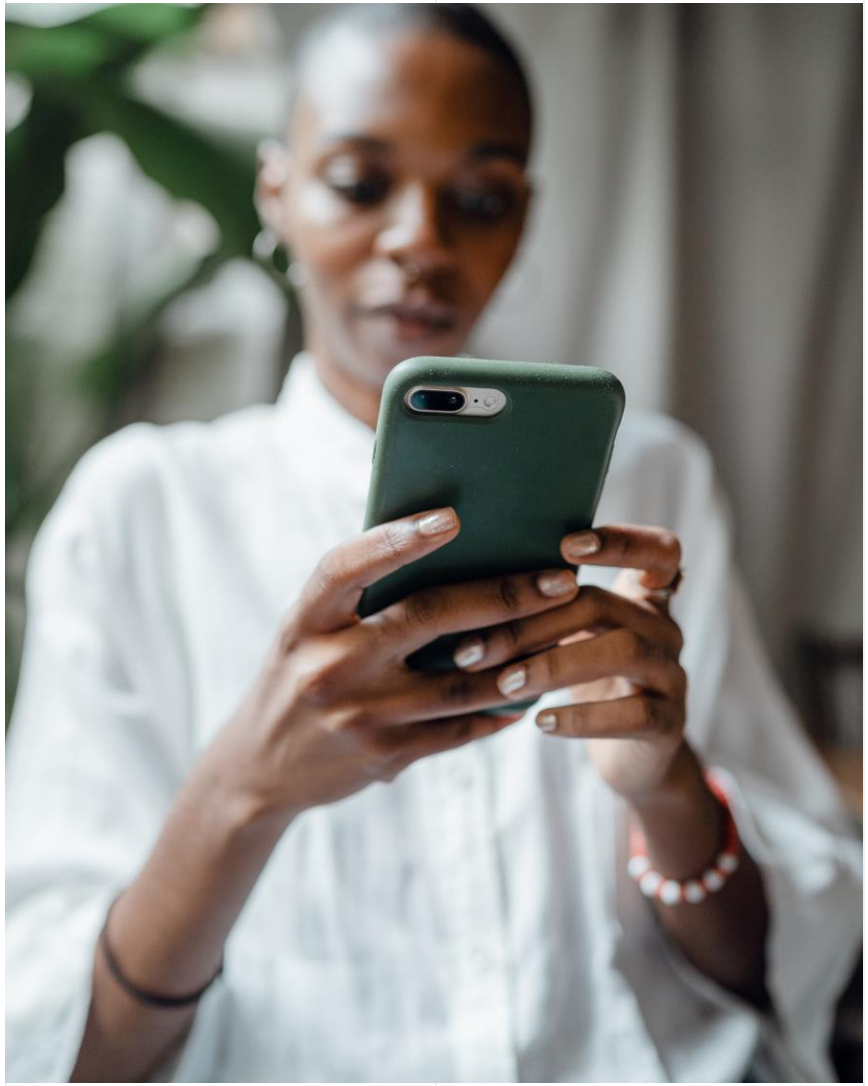
SOCIAL ENGINEERING SCAMS

What are they and how to recognize them



SMiShing Example

SOCIAL ENGINEERING SCAMS
What are they and how to recognize them



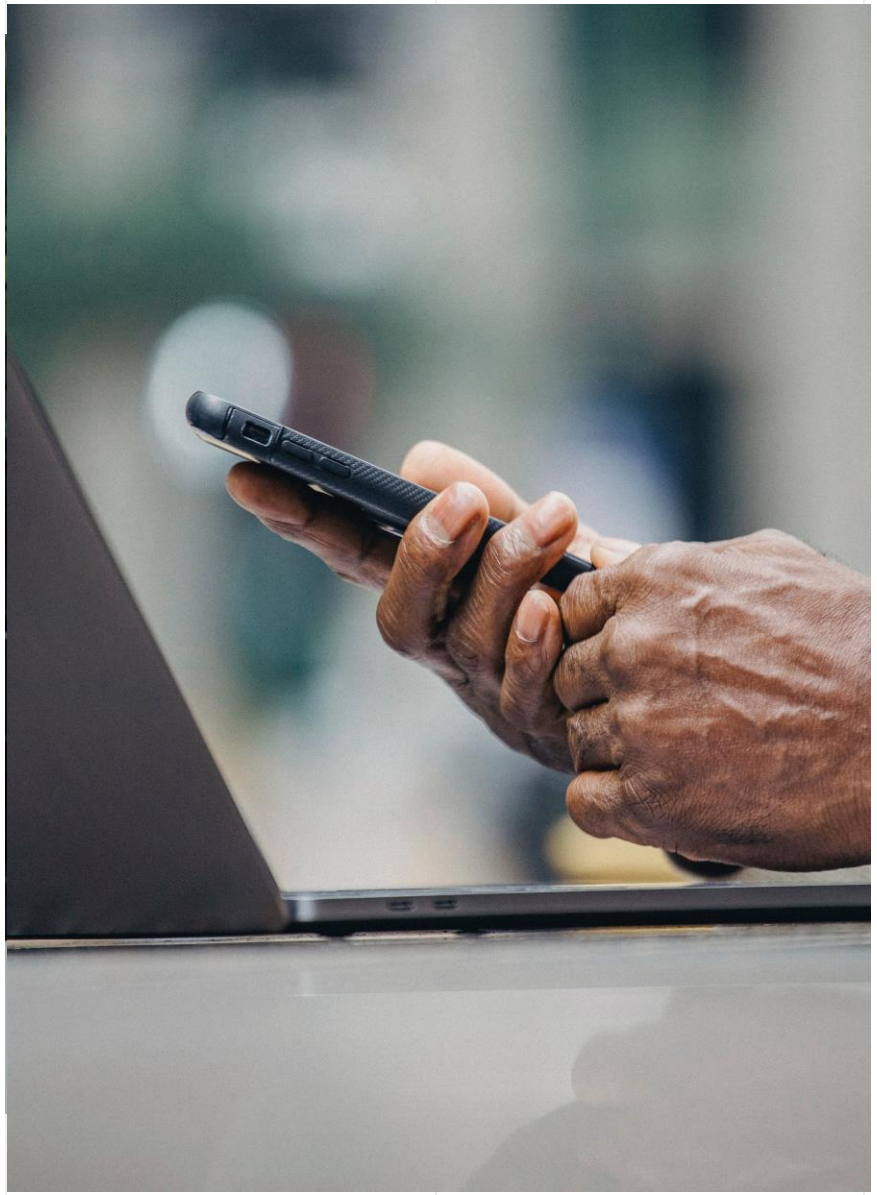
New in SMiShing attacks

- Cybercriminals are using technology to generate numbers automatically
- The landscape remains the same
- Many spam texts are scams

Tips

- Never reply
- Delete text messages right away
- Do NOT click on any links
- Do NOT disclose personal information
- Visit a company website directly
- Report and block the phone number

CYBERSECURITY BEST PRACTICES



Fundamental practices:

- Use strong, unique passwords
- Use 2 factor authentication (2FA)
- Regularly update all software & operating systems
- Be cautious about phishing
- Secure your Wi-Fi network
- Install reliable security software
- Use data encryption wherever possible i.e. cloud storage
- Backup your data regularly
- Review privacy settings
- Educate yourself
- Secure your mobile devices

QUESTIONS?

Healthy Aging Education Series "Cyber Security (Part 2)"

DATE: November 1, 2023 & December 6, 2023
SUMMERVILLE FAMILY HEALTH TEAM/PEEL SENIOR LINK

Asurtec

Asurtec Team Members

Cathy Timlin

Quality Assurance, Training and Organizational Development Director with Asurtec Technology Solutions

Bill LeBlanc

Chief Operations Officer with Asurtec Technology Solutions

TODAY'S TOPICS

Part 2: Protecting Your Privacy against Cybercriminals

01. **Social Engineering Scams**
Vishing

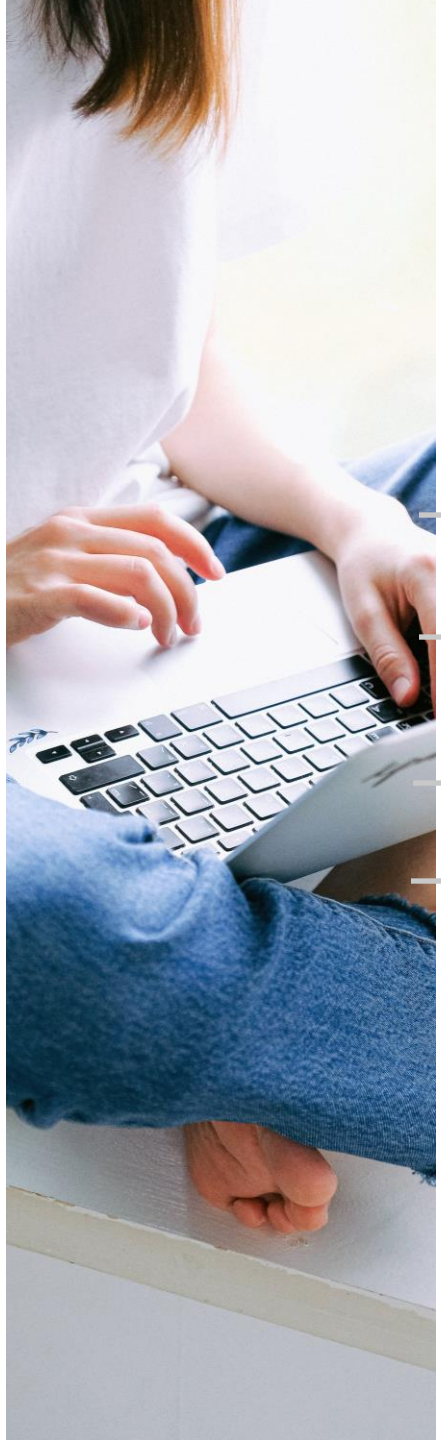
02. **Password Protection**

03. **Social Media**

04. **Privacy 101**

QUESTION

CYBERSECURITY



Which two activities can protect you r privacy when online?

a. Secure browsing

b. Disabling all cookies and tracking

c. Sharing only a small amount of personal information

d. Downloading files from unknown sources

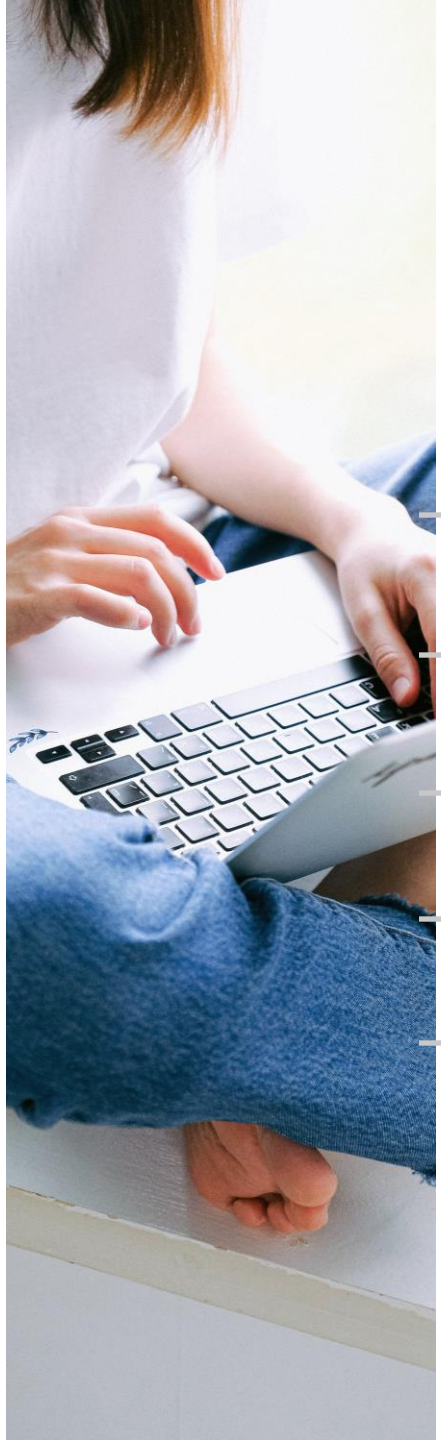
Asurtec

Online/Social Engineering SCAMS

“Vishing”

QUESTION

CYBERSECURITY



How might you sense that you have a person that is "vishing" you on the phone?

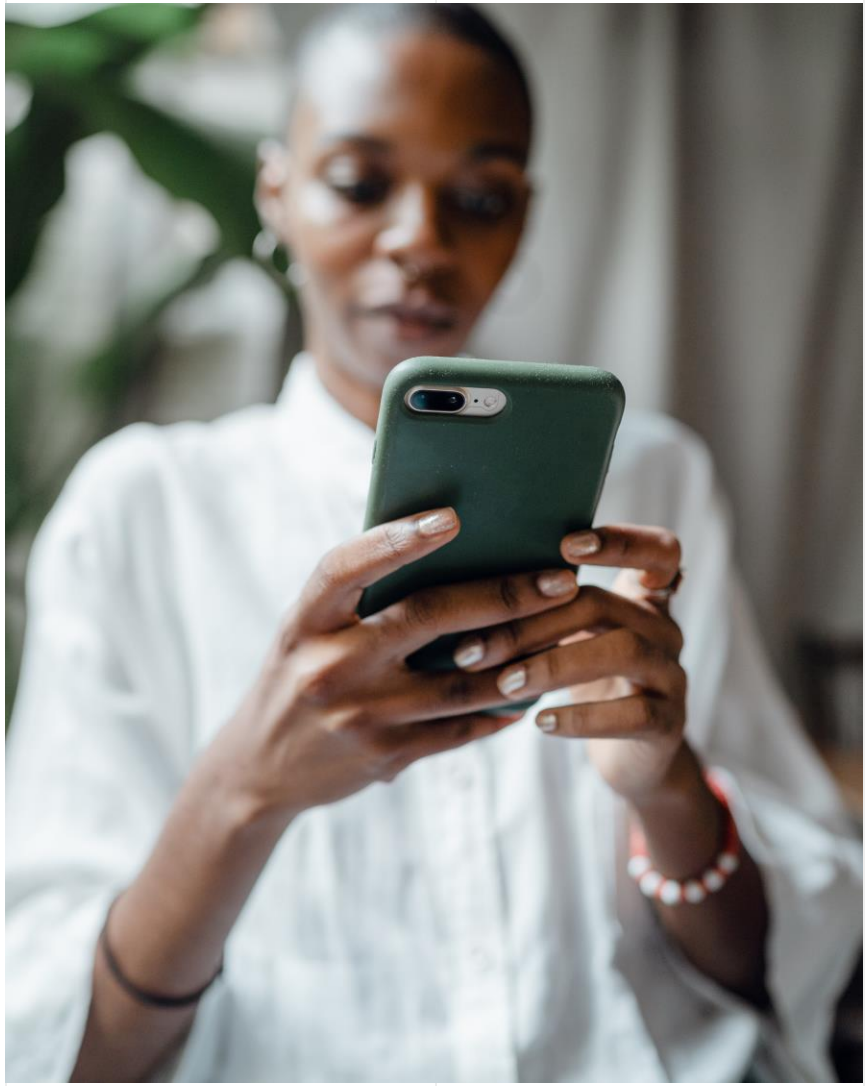
a. A caller insists on immediate action or threatens negative action

b. The caller asks for social insurance number, credit card information or your password

c. If a caller presents an unsolicited offer that is too good to be true

d. If something feels off or if the caller is offering inconsistent or vague information

e. All of the above



SOCIAL ENGINEERING SCAMS

What are they and how to recognize them

What is Vishing?

- This is the telephone version of phishing

How vishing works

- Thru data collection
- Voice manipulation
- Fraudulent calls

Tips

- Someone asks for sensitive information or scares, threatens
- Don't recognize the number let it go to voicemail.
- Watch for calls with poor audio quality – Hang up
- Don't press buttons or respond to prompts
- Verify the caller's identity

PASSWORD PROTECTION

CREATING STRONG PASSWORDS/PASSPHRASES

#PASSWORDS

Here are some tips for you to consider

01. **8 Characters**

Create passwords that are at least 8 characters long/12 is even better

02. **All keys**

Use all keys on the keyboard

03. **Avoid**

Avoid dictionary words and commonly used password patterns

04. **Unique**

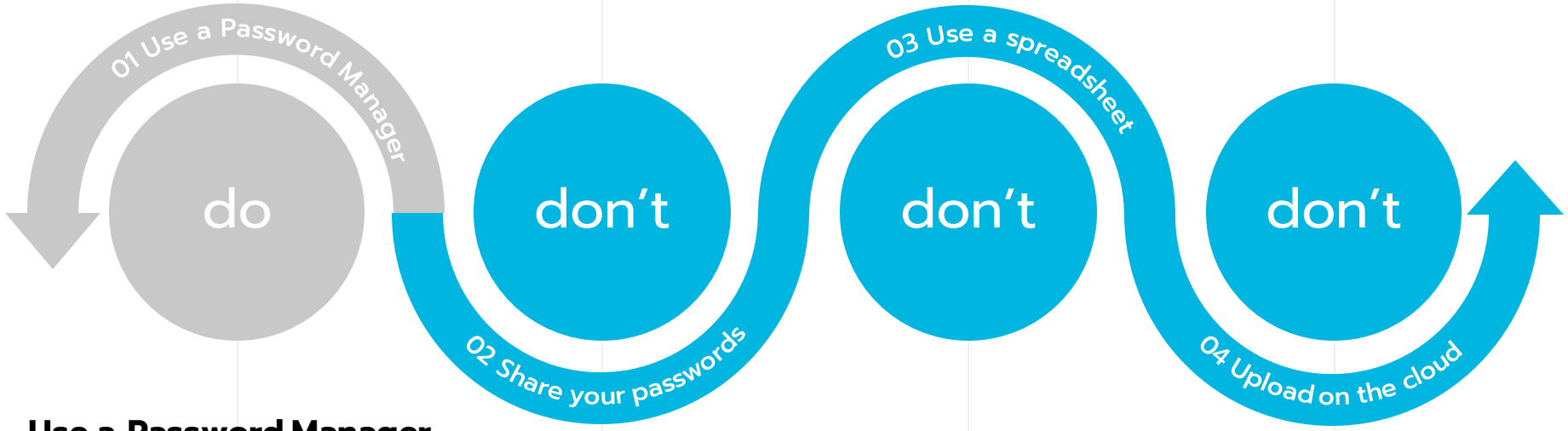
Use unique passwords

05. **Unrelated**

Group unrelated words together to create passphrases

KEEPING YOUR PASSWORDS SAFE

#PASSWORDS



Use a Password Manager
Update every 6 months
Use MFA

Do not any share your passwords with anyone

Do not save your passwords on a spreadsheet

Do not upload them on the cloud

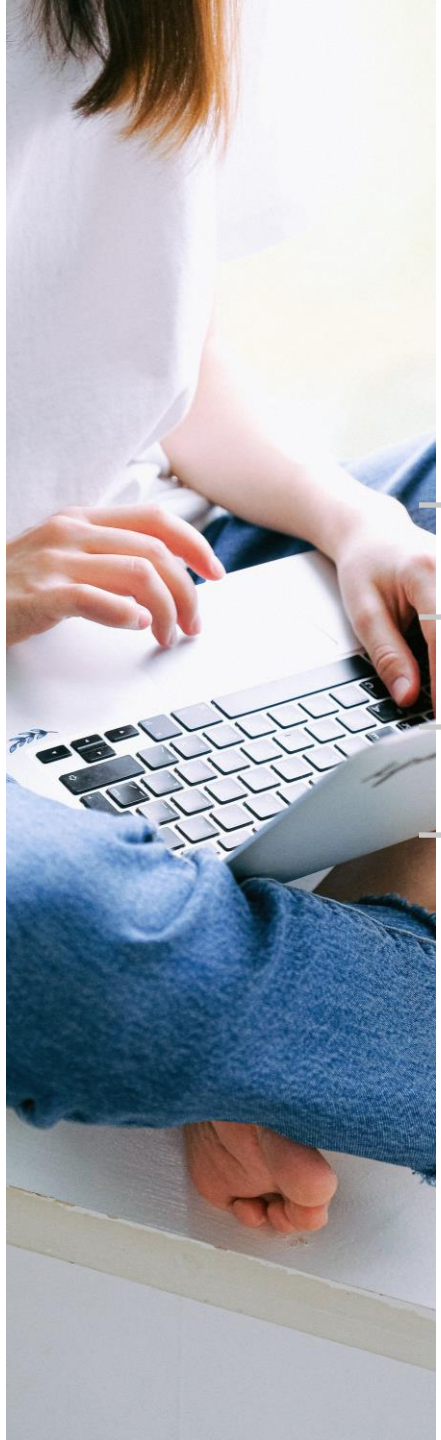
SOCIAL MEDIA

Facebook

Asurtec

QUESTION

CYBERSECURITY



What can cause a data breach to occur on a social media platform?

a. Phishing attacks

b. Adequate privacy settings

c. Encryption enabled by a company

d. Lack of multi-factor authentication

SOCIAL MEDIA SCAMS

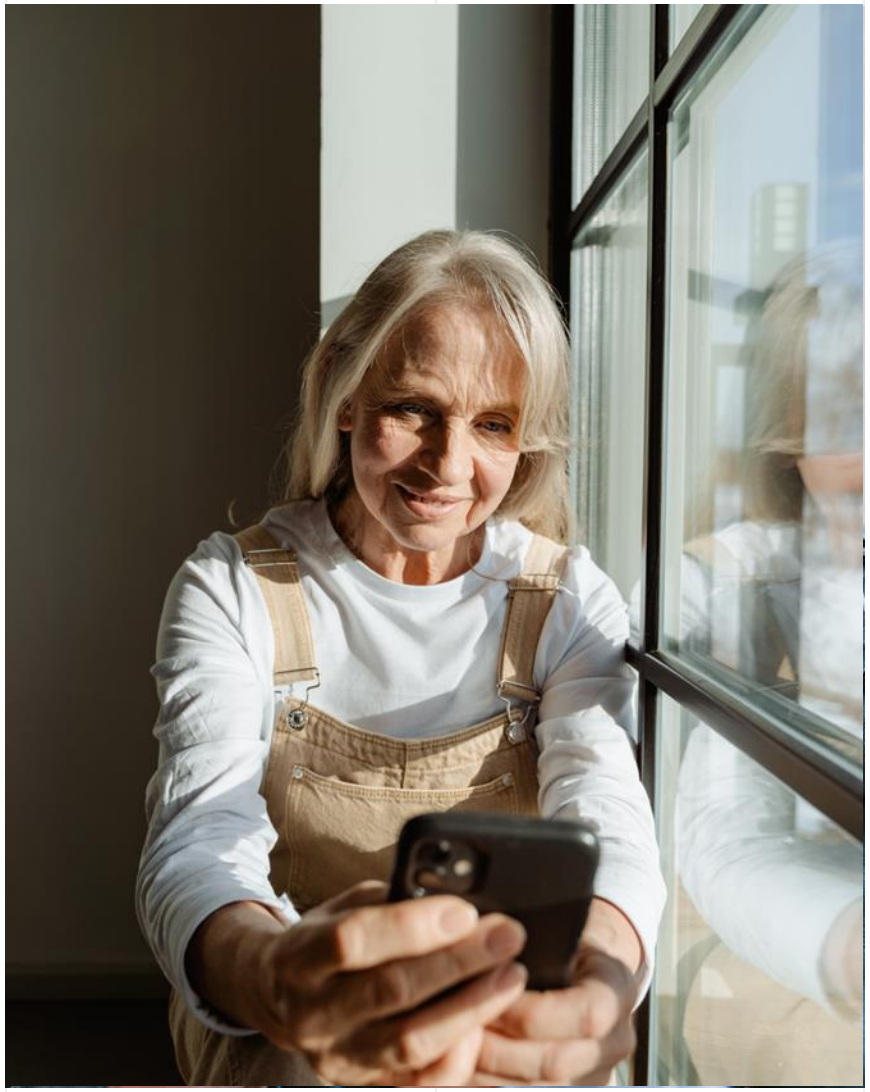
Keeping yourself safe on Facebook

Cyber criminals are taking advantage of many Facebook users. If you do receive unsolicited correspondence or someone who wants to interact and you don't know them consider these tips:

- The profile picture
- Personal details
- Followers/Friends
- Mutual friends

Remember it's not a good idea to respond or engage with messages from people you don't know.

Asurtec



SOCIAL MEDIA SCAMS

Keeping yourself safe on Facebook

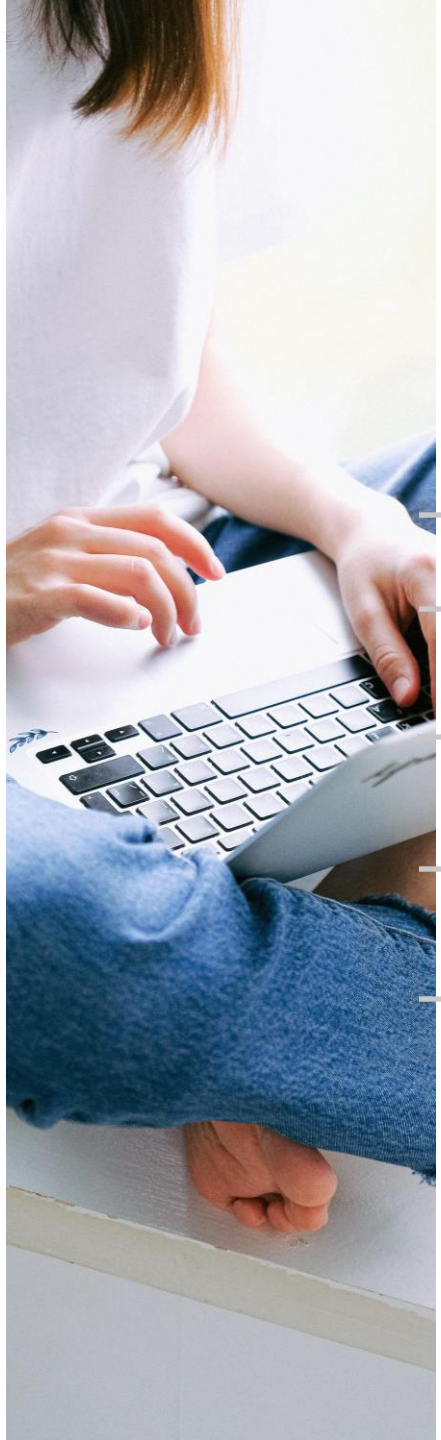
TIPS

1. Don't engage with people you don't know
2. If you receive a strange message. Delete it
3. Contact your friend via a different method
4. If you have been informed that they've received a message from you
5. Go to www.facebook.com/hacked

PRIVACY 101

QUESTION

CYBERSECURITY



PRIVACY 101

What are the factors to be aware of with identity theft?

a. Exposure of personal information

b. Use of deceptive emails, fake websites or social engineering

c. Weak cybersecurity practices that create vulnerabilities

d. Financial fraud by using stolen information in a victim's name

e. All of the above

Asurtec

PRIVACY 101

Identity Theft

Identity Theft is when someone uses another person's personal information to impersonate or defraud them

How does this happen?

1. Phishing scams
2. Malicious software – pop up windows on websites – use Alt + F4 to close
3. Data breaches
4. Oversharing

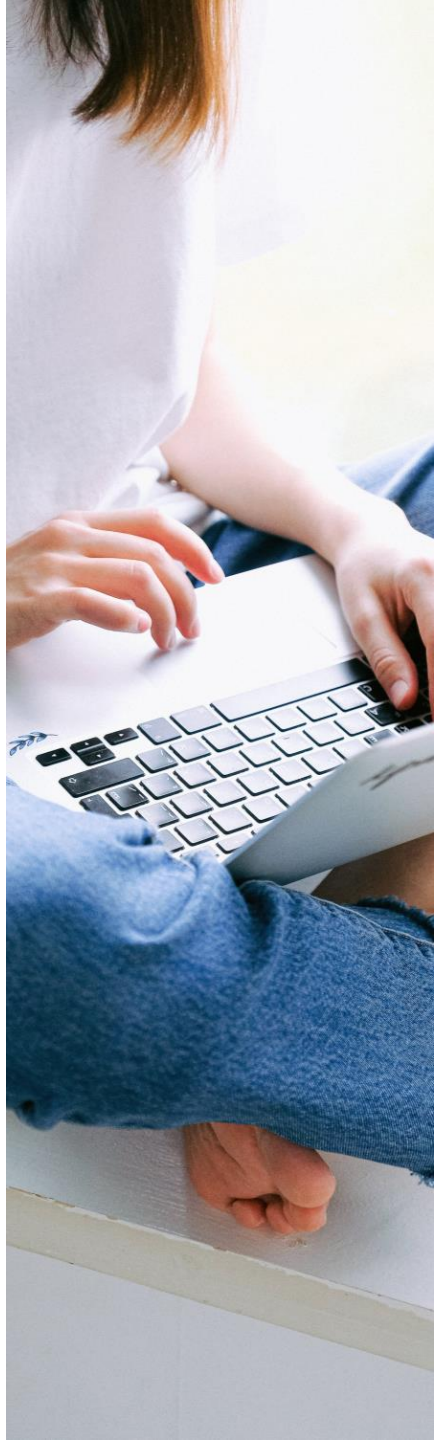
4 simple ways to protect yourself

1. Be defensive with your personal information
2. Create strong passwords and keep them secret
3. Protect your accounts and your credit
4. Boost your computer security

Asurtec

Privacy 101

CYBERSECURITY

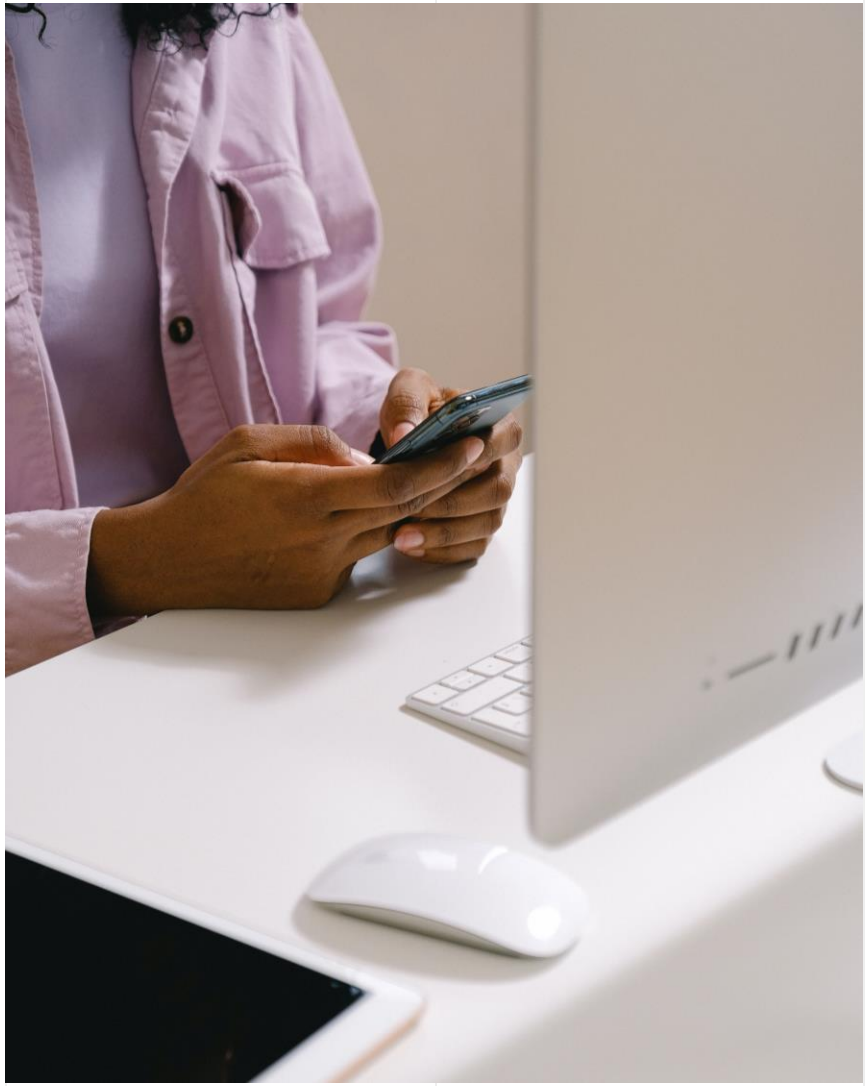


Identity Theft

What can you do if someone steals your identity

1. Act immediately
2. Change your passwords
3. File a police report
4. Have a fraud alert put on your credit report
5. Close accounts accessed or opened fraudulently
6. Report to the Canadian Anti-Fraud Center

Asurtec



RESOURCES

https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/

https://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7

Here are a couple of recommendations to consider:

Password Managers

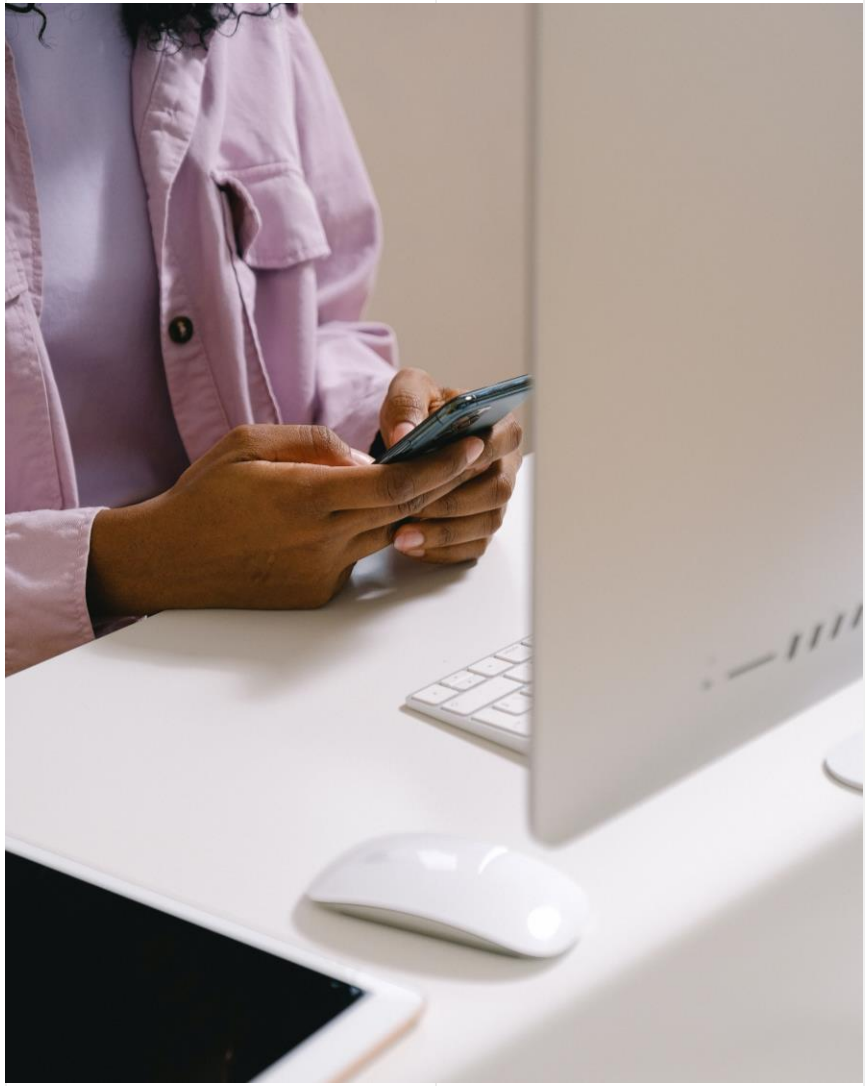
For PC
Passhub - https://passhub.net/login.php?
KeyPass - https://keepass.info/news/n160611_2.34.html

Mobile Device Apps
Dashlane
LastPass

Adblockers for Smartphones

For Androids	For iOS devices
uBlock Origin	Adblock Plus

A website that checks to see where your email has been exposed to a security breach
https://haveibeenpwned.com/



RESOURCES

More recommendations based on questions:

Spyware Software - Windows Defender - https://www.microsoft.com/en-ca/microsoft-365/microsoft-defender-for-individuals-b

Trend Micro - https://www.trendmicro.com/en_ca/forHome.html

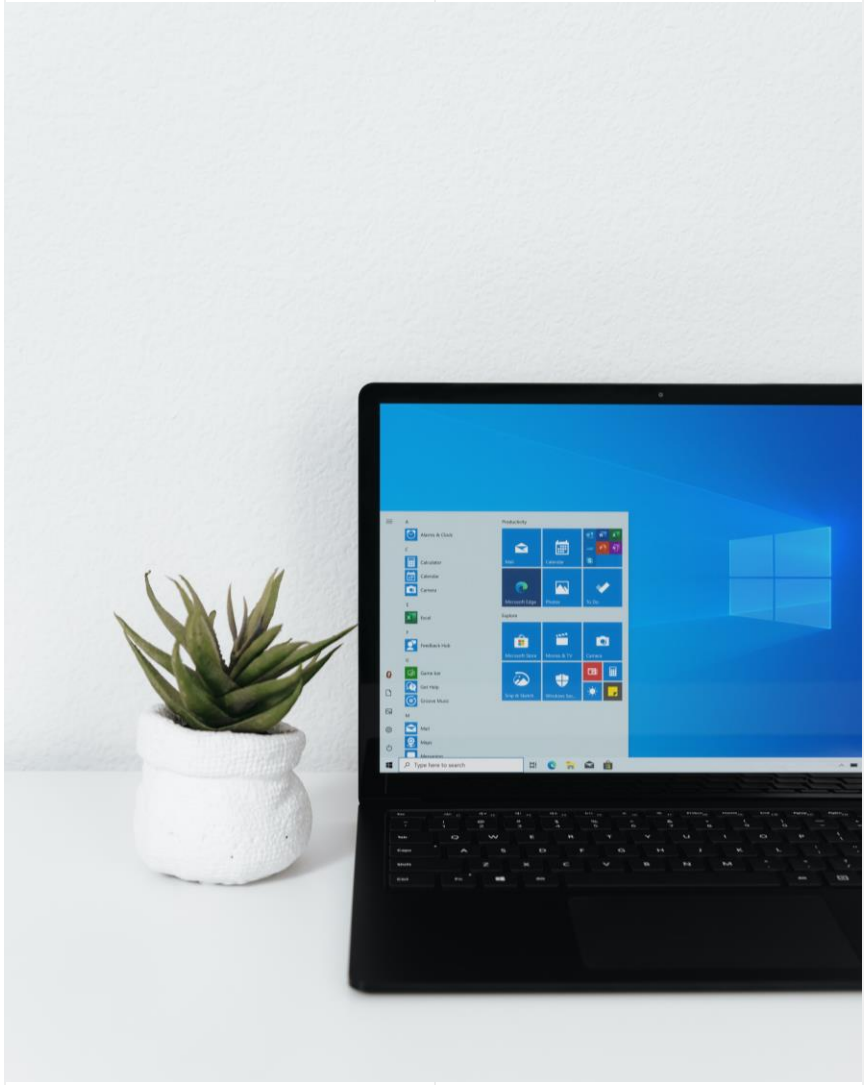
What's App hack question – This does depend on the type of hack has occurred. Some hacks are designed to take over the phone. Some to just spam contacts. Recommendation – Do not log out of What's App, Change your pin and verify the email address in your settings

Bit Defender question - immediately asks them to open a "Safe Pay" page if they are trying to do online banking. Is this safe? Yes, SafePay is a locked down browser made by Bit Defender. It will apparently stop keyloggers, trojans malware etc. From accessing the site. Now, nothing is foolproof these days so do your due diligence.

To report suspected or actual fraud please contact the -
Canadian Anti-Fraud Center - https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

QUESTIONS?

THANK YOU FOR YOUR TIME



PRIVACY 101

How to keep your personal information safe

Top Tips for Online Shopping

- Shop at reputable online merchants
- When shopping or banking use secure websites/mobile apps
- Use credit/debit cards or paypal where possible
- Be careful before you click – carefully review all transactions before confirming them
- Mistakes can happen – contact the company right away and use the cancellation feature