



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

DATE: December 7, 2022 & January 4, 2023  
SUMMERSVILLE FAMILY HEALTH TEAM/PEEL SENIOR LINK

## 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



**How much money was lost in Canada in 2021 due to Cybersecurity Scams?**

- a. 380 million
- b. 98 million
- c. 500 million
- d. More then we want to mention



# ONLINE/SOCIAL ENGINEERING SCAMS

“Phishing Emails”





# QUESTION

# CYBERSECURITY



**Tell us what types of information a cybercriminal might try to steal from you?**

- a. Your banking information
- b. Your password
- c. Your name and phone number
- d. Your credit card information
- e. All of the above

# Phishing Attacks

# CYBERSECURITY



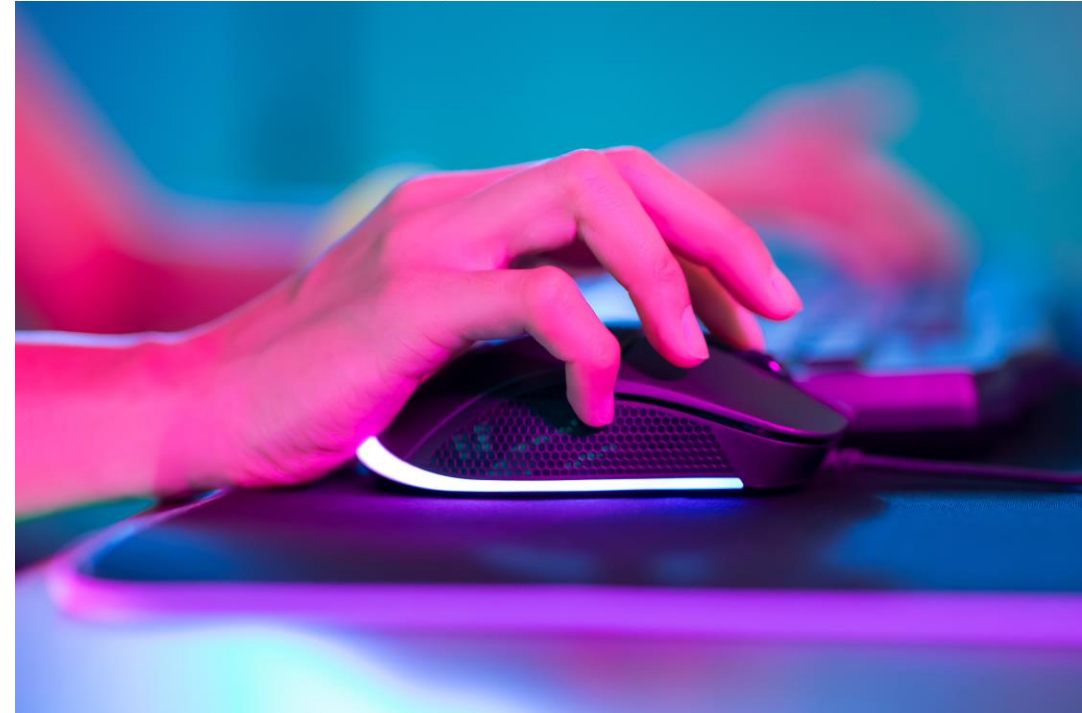
## What's changed?

- Cybercriminals are sending more targeted emails
- Emails are crafted using the recipients personal and professional characteristics and interests
- Emails require more effort but recipients more likely to respond
- Phishing attacks are effective because the emails look more legitimate these days
- More than 70% of phishing emails received are opened



# HOW HARD IS IT TO GET SCAMMED?

---






# Targeted 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.

# Targeted Phishing Attacks

## What are they and how to recognize them



### RECIPIENT INFORMATION

**From:** awaycourier.ca Auto Mail Delivery <[wedad@drbrunner.com](mailto:wedad@drbrunner.com)>  
**Sent:** Thursday, June 25, 2020 11:53 AM  
**To:** Executive Director <[execdir@fakeorg.ca](mailto:execdir@fakeorg.ca)>  
**Subject:** Password Expiration Request ID: 42312 Created for [execdir@fakeorgcourier.ca](mailto:execdir@fakeorgcourier.ca)  
**Importance:** High

**HOVER YOUR CURSOR OVER THE LINK**

**Bit.ly or Ow.ly**

Dear: [execdir@fakeorg.ca](mailto:execdir@fakeorg.ca),

Kindly be inform that your password to [execdir@fakeorg.ca](mailto:execdir@fakeorg.ca) Expires today.

**Date and Time :** Thursday, June 25, 2020 7:53:00 AM

**Severity:** High

**A high-extremity alert has been triggered**

**Proceed To Keep Same Password**

This email was sent to [execdir@fakeorg.ca](mailto:execdir@fakeorg.ca).

[Microsoft](#) | [Support](#) | [Privacy Policy](#)

Copyright © 2020 Microsoft Inc. All rights reserved.

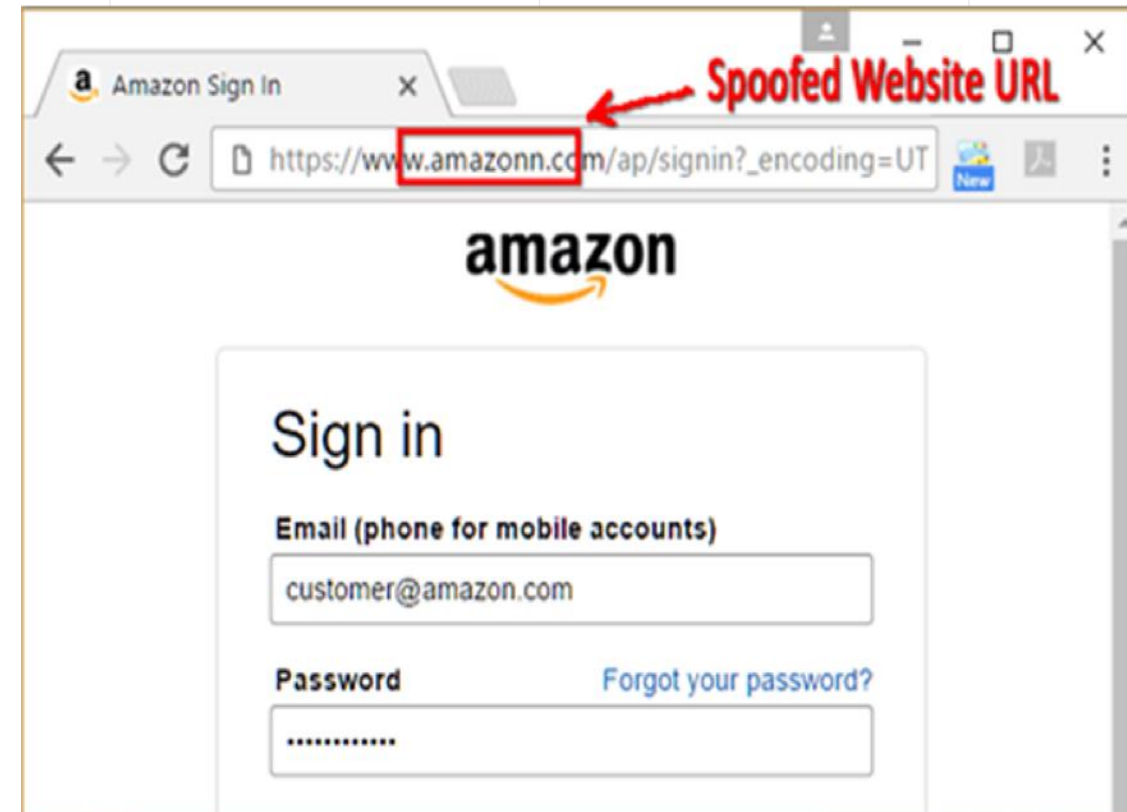


# Targeted Phishing Attacks

What are they and how to recognize them

Email Phishing – con't

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





# TARGETED PHISHING EMAILS

## How to keep yourself safe

---

### TIPS

1. If an offer seems **to good to be true**, then it probably is
2. Do NOT open emails from **untrusted sources** and do NOT click on links
3. **Never send** personal or financial information by email
4. Be **skeptical**. Verify the identity of any person making a request
5. **Slow down**
6. Check your **Anti-Virus software** and keep it up to date at all times
7. **Report scam emails** if you are able and Delete it

# QUESTION

# CYBERSECURITY



**What is the absolute most important thing to do when you receive an email that has an embedded hyper(LINK) inside it?**

- a. Respond to the email
- b. Click on the link to see if the website looks suspicious
- c. Hover your mouse over the link and without clicking the link pay full attention to see what the actual URL web address is
- d. Review who the email is for and from by clicking on the email address information



# Online/Social Engineering SCAMS

“SMiShING”

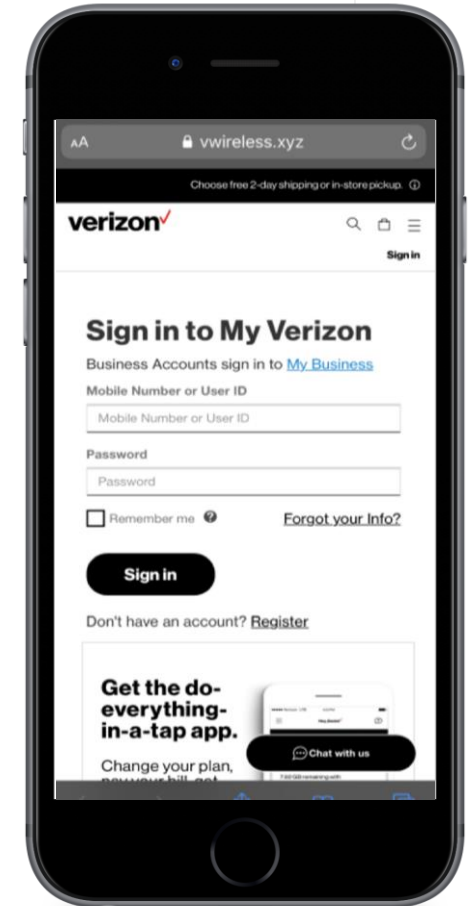
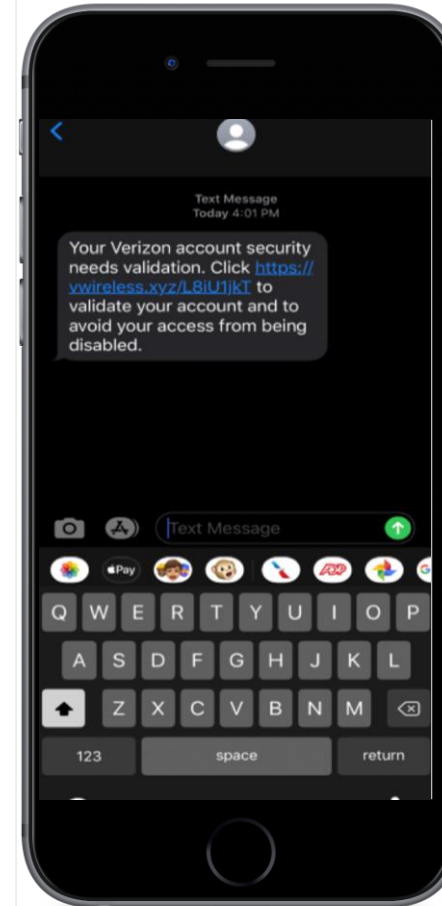


# SOCIAL ENGINEERING SCAMS

## What are they and how to recognize them

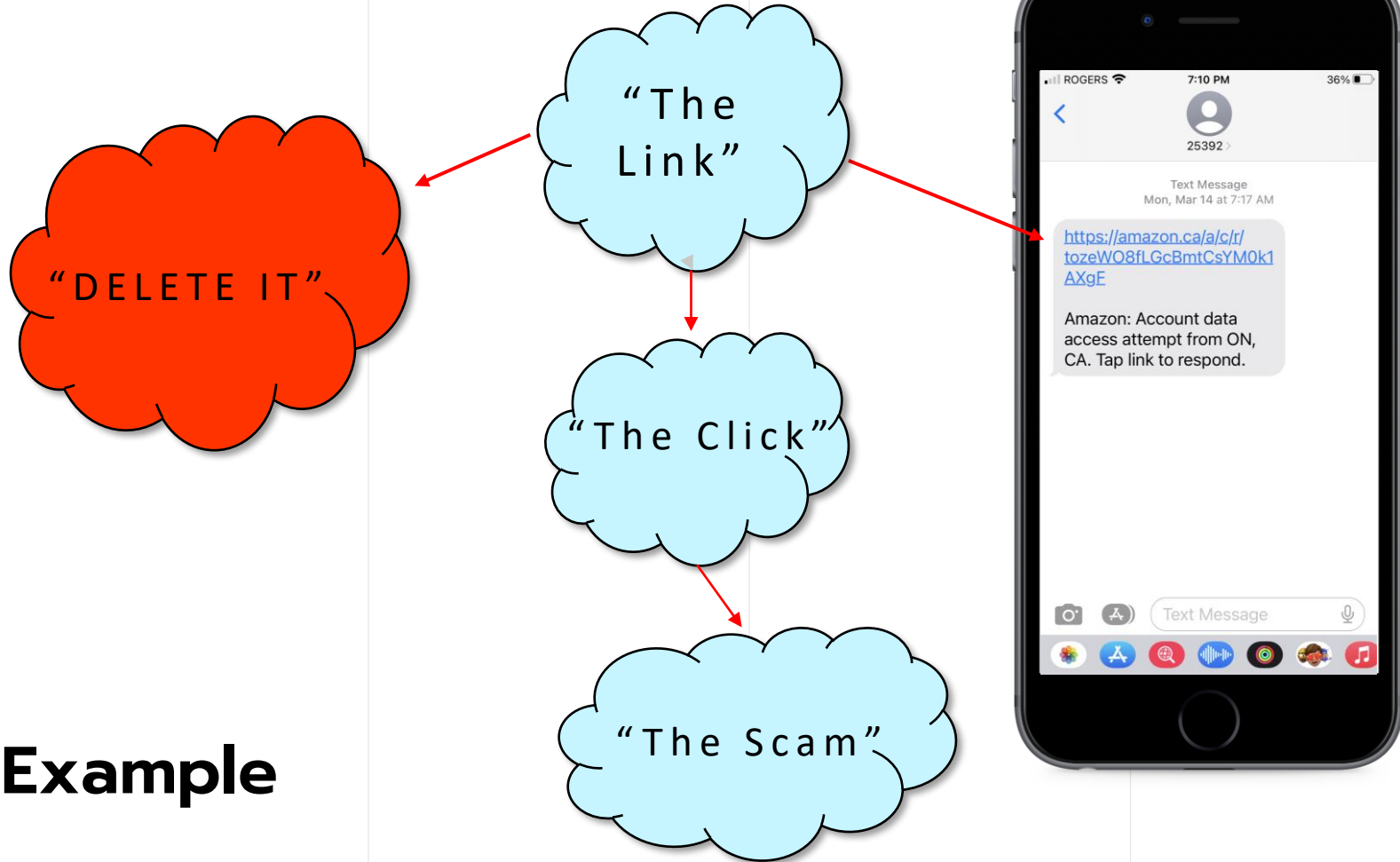
---

### SMiShing Example

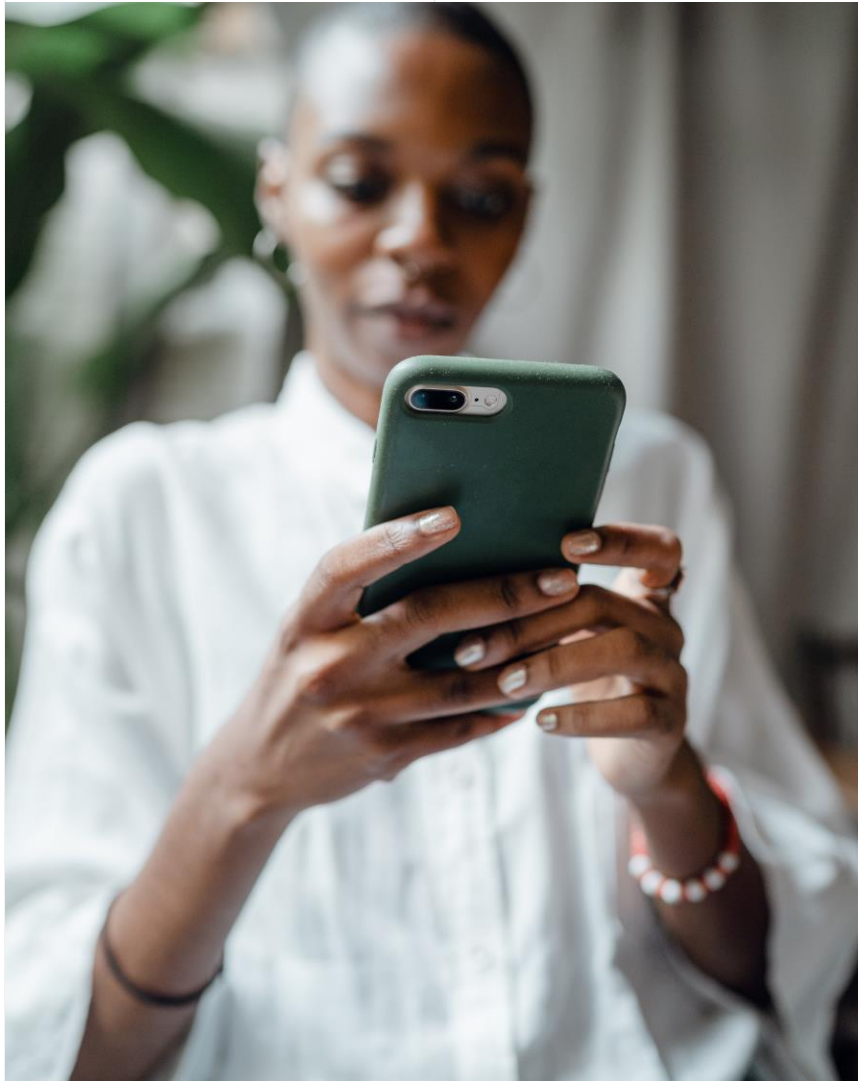


# SOCIAL ENGINEERING SCAMS

What are they and how to recognize them



## SMiShing Example



# SOCIAL ENGINEERING SCAMS

## What are they and how to recognize them

---

### New in SMiShing attacks

- “Urgent messages about your credit card or bank account
- Notifications that you’ve won something
- Fake survey links
- Fake messages from trusted brands

### Tips

- Delete text messages right away, Do NOT reply, Do NOT respond in short codes and Do NOT click on any links.
- Requesting YOUR personal information through a text message is not standard procedure. A clear sign of suspicious activity.



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

DATE: December 7, 2022 & January 4, 2023  
SUMMERVILLE FAMILY HEALTH TEAM/PEEL SENIOR LINK





# 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



**In 2021, where did Canada rank in the world related to Cybersecurity attacks; for example, the USA was ranked the 6th most attacked country in the world?**

- a. 10th
- b. 30th
- c. 3rd
- d. None of the above

# Online/Social Engineering SCAMS

“Vishing”



# QUESTION

# CYBERSECURITY



**Vishing is a form of Social Engineering, what can a cybercriminal do to scam you?**

- a. Use fraudulent phone numbers
- b. Use voice altering software
- c. Use social engineering tactics
- d. Spoof the caller ID to look like it's coming from legitimate companies and institutions
- e. All of the above





# SOCIAL ENGINEERING SCAMS

What are they and how to recognize them

---

## Vishing

### What is Vishing or voice phishing?

- The telephone version of phishing.
- Same concepts apply to a vishing attack.
- They use social engineering tactics to entice you into divulging personal and confidential information like account numbers or passwords.
- They really are banking on the fact that we may just trust a human voice rather than an email.





# SOCIAL ENGINEERING SCAMS

## What are they and how to recognize them

---

### New in Vishing attacks

- Hybrid form - "Callback phishing" includes an email
- More advanced forms like creating fake phone numbers and spoofing the caller ID
- VoIP technology is now easier to automate hundreds of scam calls over the internet making it hard to trace

### Tips

- Someone asks for sensitive information be suspicious
- If you don't recognize the number let it go to voicemail. Don't be curious!!
- Watch for calls with poor audio quality – Hang up
- Don't press buttons or respond to prompts
- Verify the caller's identity

# PASSWORD PROTECTION



# QUESTION

# CYBERSECURITY



**Which password would be considered the most secure?**

- a. johnny@345!
- b. Ja&der3\*8
- c. Desk+truck-pup^hello22
- d. None of the above

# 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

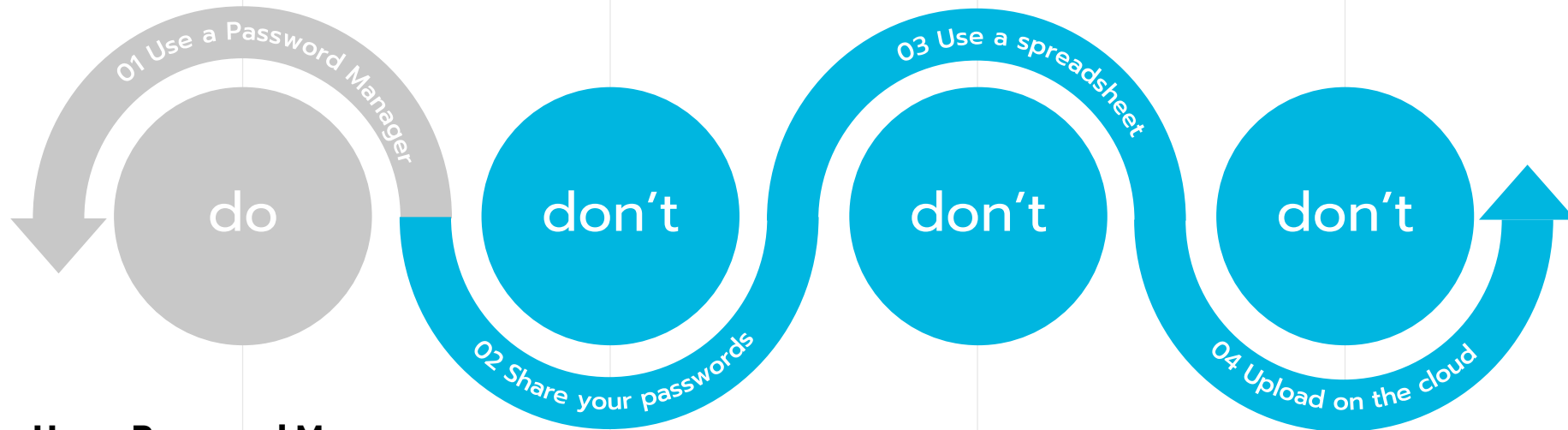
Use unique passwords

## 05. Unrelated

Group unrelated words together to create passphrases

# KEEPING YOUR PASSWORDS SAFE

#PASSWORDS



**Use a Password Manager  
And update every 6 months**

**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

Twitter, Facebook, Instagram, Snapchat





# QUESTION

# CYBERSECURITY



## Why shouldn't you reveal too much about yourself on Social Media?

- a. Cyber attackers use personal information to trick you into believing they are a legitimate company or relative (social engineering)
- b. People use personal information as passwords ie pet's names
- c. People can impersonate you
- d. All of the above

# SOCIAL MEDIA SCAMS

## Think before you post

---

Cybercrime has breached social medial networks, due to increased users and increased use.

Cybercriminals use opportunities to gain access to people's accounts, personal or financial information. HOW?

Using suspicious links or downloads

- Are being used to deliver phishing scams.
- Focuses on exploiting a person's inclination to trust
- Once you click "Post", "Publish" or "Send"





# SOCIAL MEDIA SCAMS

Think before you post

## TIPS

1. Privacy settings – be comfortable with your privacy settings
2. Do not overshare
3. Know the audience
4. Control your public profile
5. Control your data
6. Understand the security of your platform



# SOCIAL MEDIA SCAMS

Think before you post

## TIPS

7. Use strong passwords and change it regularly
8. Don't click on links, coupons and answer surveys
9. Avoid giving out your location
10. Stick to people you know
11. Never add personal or financial information
12. Report abuse or if you think you have been hacked
13. Know fact from fiction



# PRIVACY 101



# QUESTION

# CYBERSECURITY



**Tell us the best way(s) to protect your online privacy?**

- a. Use a unique and complex password/passphrase for each account
- b. Enable multi-factor authentication where you can
- c. Use a Password Manager
- d. Beware of suspicious behaviour
- e. Share information cautiously



# PRIVACY 101

## How to keep your personal information safe

---

**The internet is used for many different things today. It will be up to us to protect our online security**

Online privacy is about protecting your rights to keep private information to yourself.

Internet privacy and internet security are different but closely related.

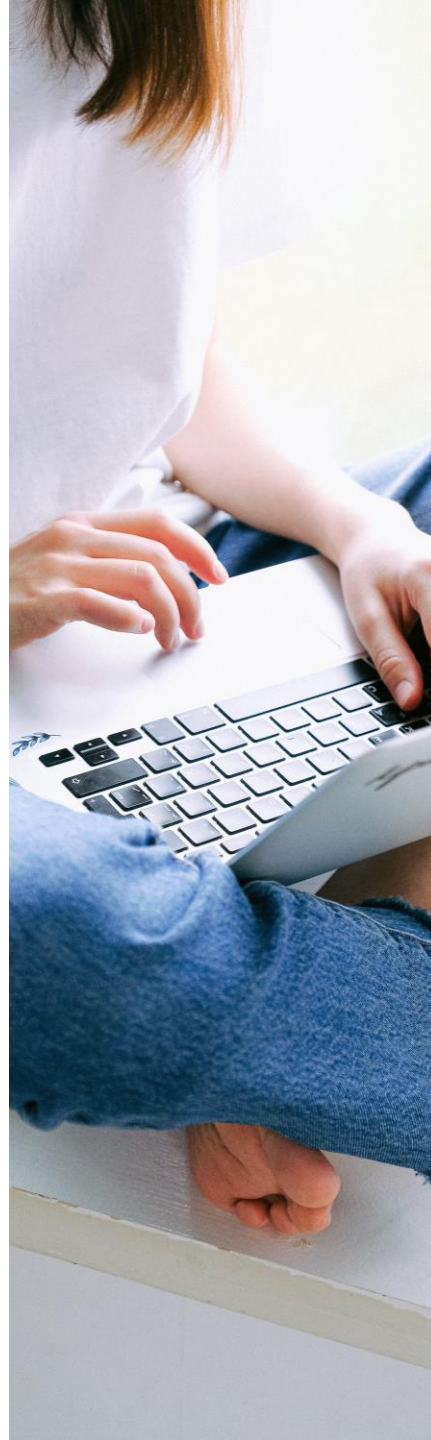
### Privacy vs Cybersecurity

Good security enhances privacy, and enhanced privacy helps maintain good security.



# Privacy 101

# CYBERSECURITY



## How to keep your personal information safe

### A few simple steps to think about:

1. Commit to sharing less online
2. Use strong, unique passwords, and two-factor authentication when possible
3. Tighten privacy settings for your online accounts
4. Purge unused mobile apps
5. Don't ignore any software updates
6. Disable ad and data tracking
7. Use encryption to keep data private (chats)
8. Revoke unnecessary third-party app connections





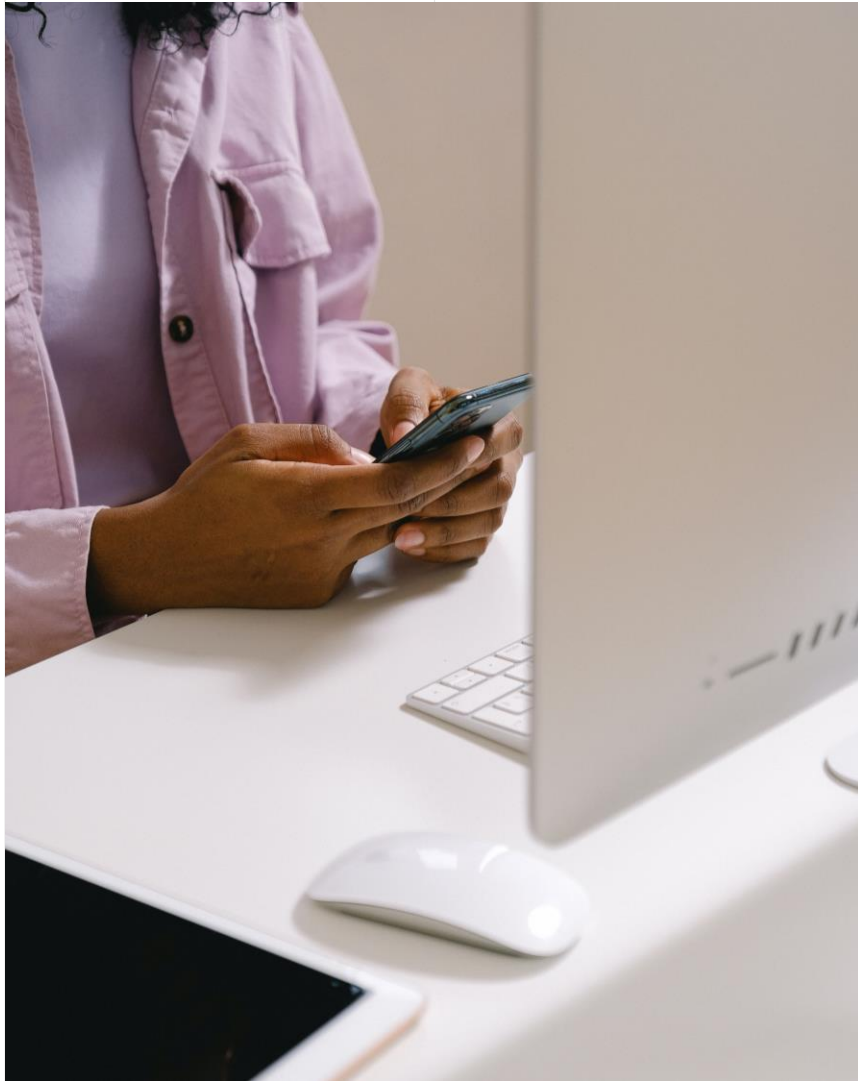
# PRIVACY 101

## 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





# RESOURCES

<https://gizmodo.com/google-bing-fbi-ad-blocker-scam-ads-1849923478>

Here are a couple of recommendations to consider:

## Password Managers

### **For PC**

Passhub - <https://passhub.net/login.php?>

Keepass - [https://keepass.info/news/n160611\\_2.34.html](https://keepass.info/news/n160611_2.34.html)

## **Mobile Device Apps**

Dashlane

LastPass

## Adblockers for Smartphones

### **For Androids**

uBlock Origin

### **For iOS devices**

Adblock Plus

A website that checks to see where your email has been exposed to a security breach

<https://haveibeenpwned.com/>

# QUESTIONS?





**THANK  
YOU FOR  
YOUR TIME**

