Healthy Aging Education Series
"Introduction to Cybersecurity"

SUMMERVILLE FAMILY HEALTH TEAM / PEEL SENIOR LINK

DATE: MAY 5, 2021

Asurtec
Managed IT Solutions

Who am I?

My name is Cathy Timlin

- Retired Executive Director
- Training and Organizational Development Coordinator with Asurtec Technology Solutions

Asurtec
Managed IT Solutions

Introduction

Throughout our discussion I will;

- Discuss the types of cybersecurity risks facing individuals today,
- Showcase examples of potential cybersecurity risks
- Give you tips on identifying and responding to these threats

Any Questions?

Asurtec
Managed IT Solutions

Today's Topics

- Dealing with Scam emails, texts and phone calls
- Passwords – Creating strong passwords and Keeping yourself Safe
- Social Media – Think before you post
- Privacy 101 – online shopping, banking and other financial transactions

Asurtec
Managed IT Solutions

What is Cybersecurity?

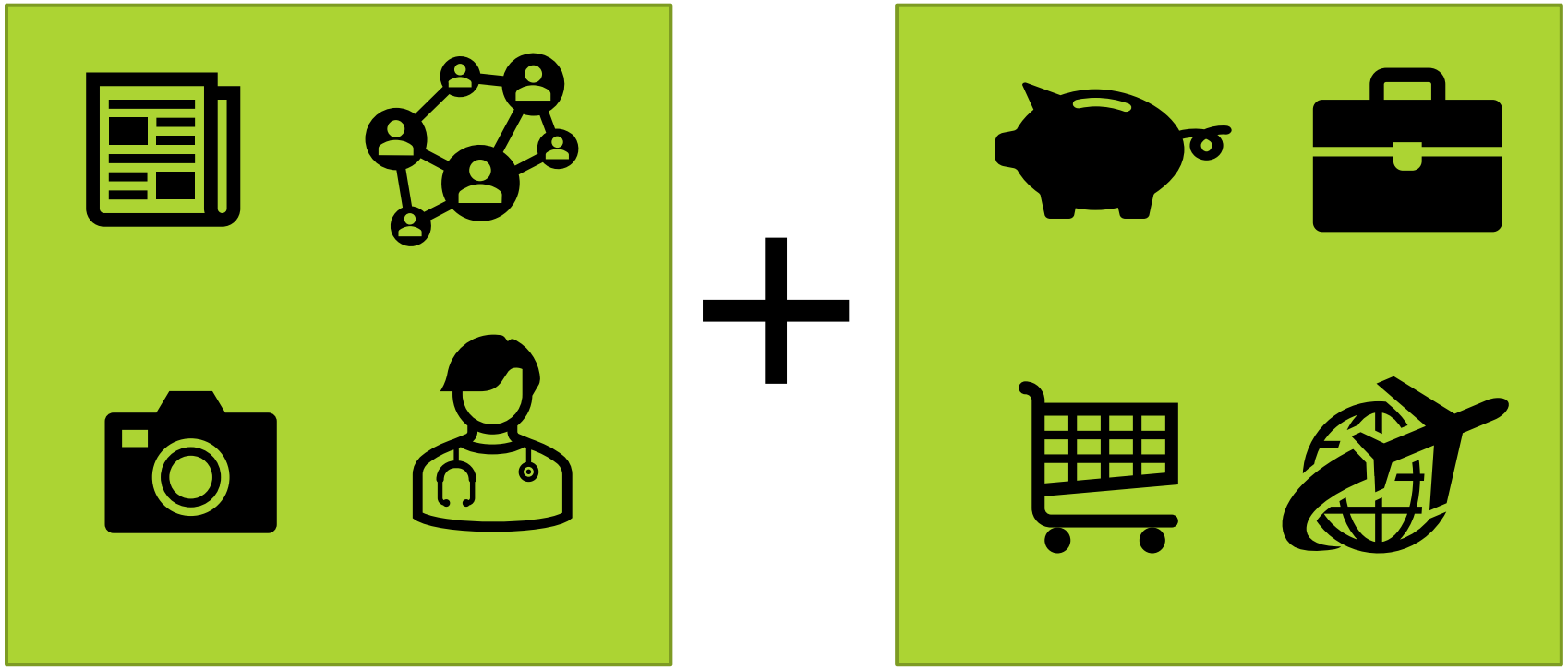
- **Definition of *cybersecurity***

: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Source: https://www.merriam-webster.com/dictionary/cybersecurity

Asurtec
Managed IT Solutions

Why do seniors go online?



Asurtec
Managed IT Solutions

Seniors Online

- While technology can provide many positive and powerful tools, there can be risks involved with online use
- Learning how to manage these risks really is key to safe and enjoyable online use
- Following some simple rules can go a long way to keep you, your family and friends safe

Asurtec
Managed IT Solutions

Seniors Online

Don’t be hacked by a Human!!

- There are many different types of online scams
- Online scams have recently become far more sophisticated
- They exploit a person’s inclination to trust in order to manipulate them into handing over specific information

The fundamentals of these online scams they have one common element DECEPTION!!

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

What is the one thing everyone here today has that a scammer or cybercriminal wants from you?

- It would be considered the most valuable asset you have
  - **YOUR PASSWORD**
- It should be considered just as important as your banking information.

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Scams can come in different forms.

The most common are -

- Email Phishing
- SMiShing
- Vishing

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

What is Email Phishing/Scam Emails?

- Receive an email that look like they are coming from a trustworthy source i.e. a business, family member, the bank, a government agency and;
- May look like its coming from someone that you frequently interact with

What is the goal is they are trying to achieve?

- Gaining access to your personal information
- Installing malware on your computer or mobile device

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam Emails – con't

- Fool you into clicking an embedded link that would take you to a fake/ or look alike website where you subsequently log in using your password

Should you click on any of these and log in

You have just delivered them your log in information. It's as easy as that!!

- Passwords are like GOLD to a cybercriminal

Reminder – you should always ask yourself – Should I be entering my login information on this site?

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails – con't

How can you spot a potential email scams

- Someone sends an information request. Is the information request legit?
- Is there a sense of urgency attached to the email?
- Does the sender email look suspicious?
- Does the email contain a suspicious link or an attachment that you were not expecting?

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails – con't

TIPS

- Attach importance to your password as you would your debit card, or your visa card or your purse/wallet for that matter
- If you are provided with an offer seems to good to be true, then it probably is – don't fall for it
- Do NOT open emails from untrusted sources and do NOT click on links
- Never send personal and/or financial information by email

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails

TIPS – con't

- Be skeptical. Verify the identity of any person making a request
- Always verify whether or not the person is authorized to make such a request
- Check your Anti-Virus software and keep it up to date at all times
- If you do receive an email scam – Report it if you are able and Delete it

Reminder - Don't implicitly trust others without proper verification

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails

Office 365

Dear: execdir@fakeorg.ca,

Kindly be inform that your password to 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.

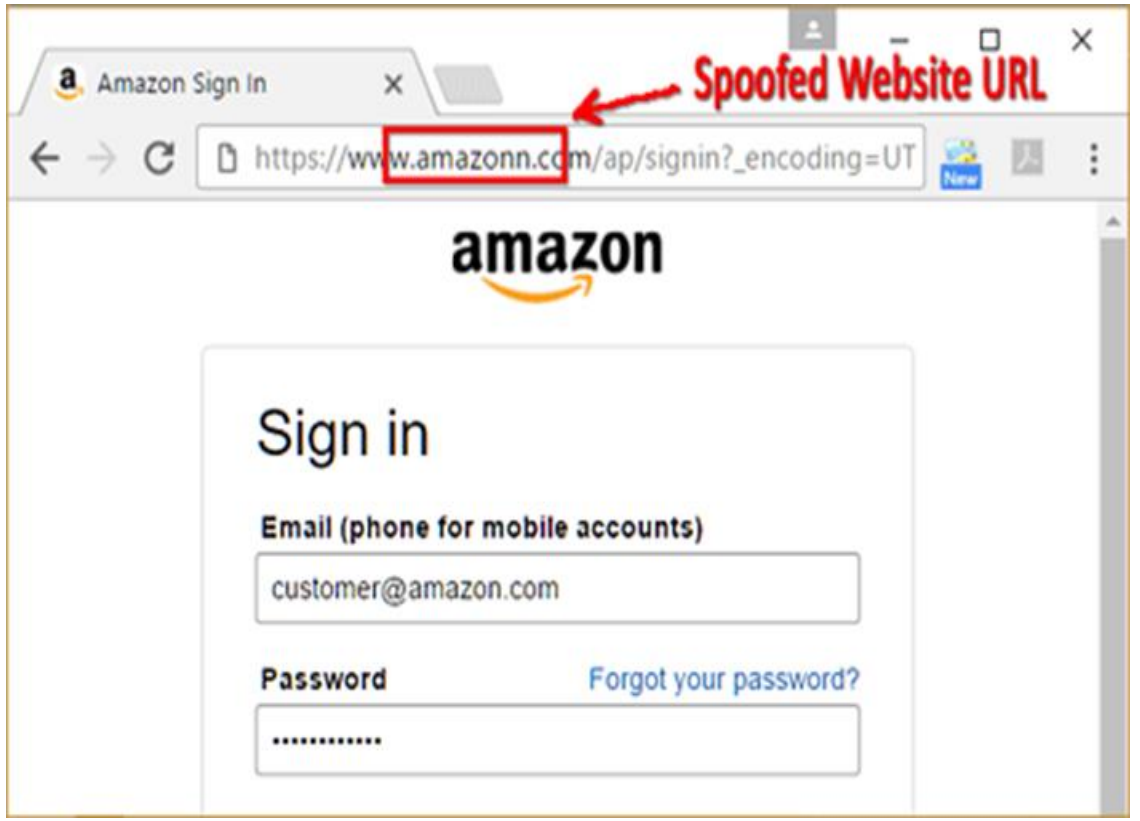
Microsoft | Support | Privacy Policy

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails

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



Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

Email Phishing/Scam emails related to COVID 19

- Many new scams have risen throughout the pandemic
- They offer fake online stores and treatments
- As we become more reliant on digital devices to communicate, work remotely and continue our day to day activities

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts, and phone calls

Email Phishing/Scam emails related to COVID 19

- It could look like this

Public Notice

Toronto, Ontario. All employees will receive (mandatory) paid leave to avoid the spread of the COVID-19 novel coronavirus starting from March 14, 2020.

Offices will resume after 2 weeks of the mandatory closure.

Check the link to see if your company is listed:

http://bit.ly/MandatoryPaidLeave

Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

SMiShing – What the heck is SMiShing?

- SMiShing takes on a different approach to email phishing. Smishing is a phishing attack carried out over mobile text messaging
- An attacker uses text messages to exploit their victim, and are deceived into giving out sensitive information. Just like email phishing cybercriminals use malware or fraudulent websites to gain access to account and password information
- This is definitely an emerging trend but don't be fooled by trusting a text message vs an email.

Asurtec
Managed IT Solutions

Dealing with scam emails, texts and phone calls

Types of SMiShing attacks

- Receive a text prompting you to respond by typing “yes”, or by spelling out “reply”
- Clicking a link included in the text to verify your information
- Prompted to download an app that looks legitimate

TIPS

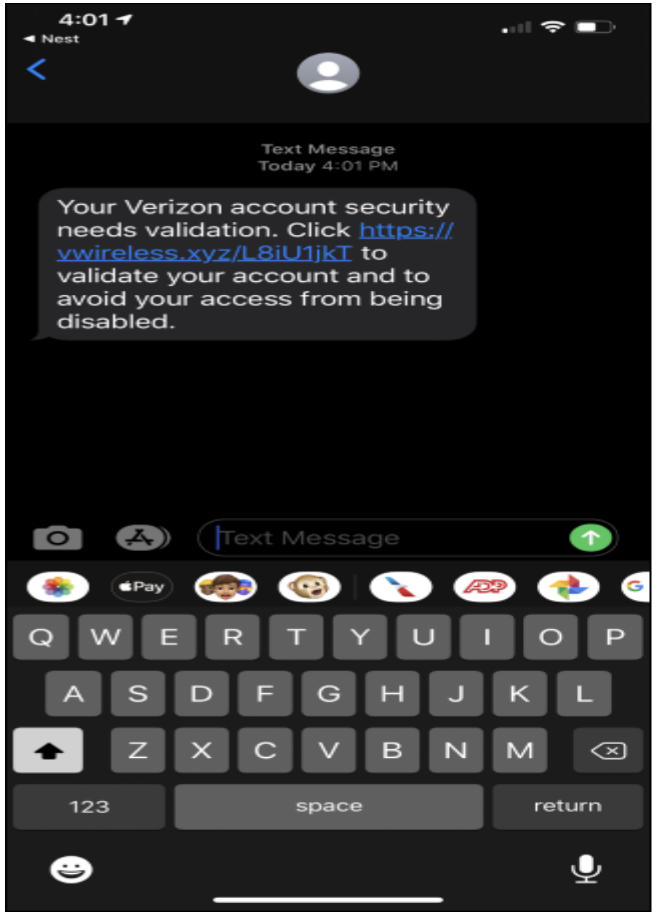
- Delete these text messages right away, Do NOT reply, Do NOT respond to short codes and Do NOT click on any links
- Requesting your personal information through a text message is not a standard procedure, this is a clear sign of suspicious activity

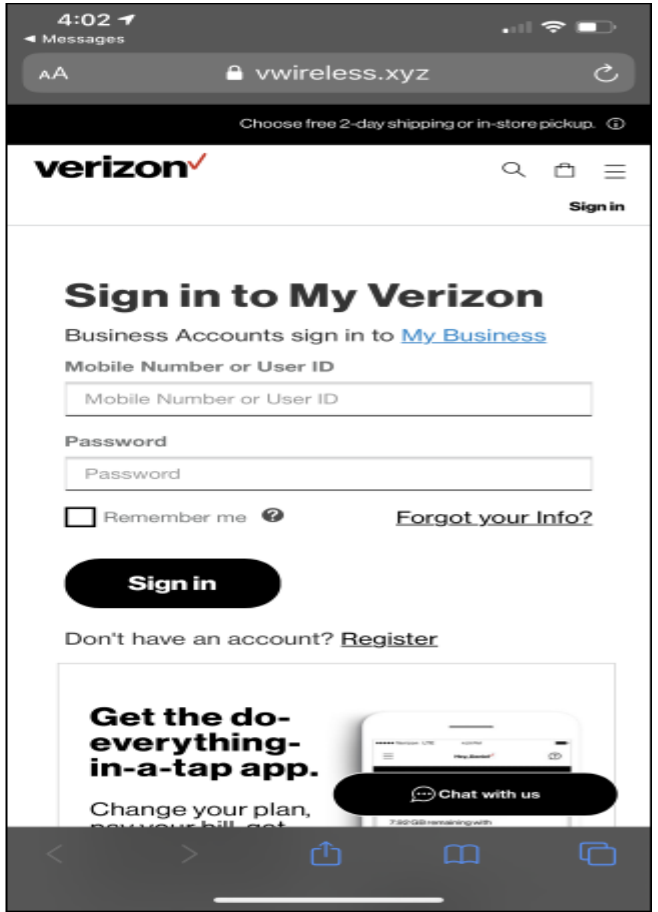
Asurtec
Managed IT Solutions

Dealing with Scam emails, texts and phone calls

SMiShing – con't

- Example





Asurtec
Managed IT Solutions

Dealing with Scam emails, text and phone calls

Vishing/Robocalls – What is Vishing?

- This is the telephone version of phishing.
- The same concepts of phishing apply to a vishing attack.
- Appear to be from a trusted source.
- Attempt to deceive you into handing over confidential information.
- Many times they are now using spoofed numbers of more than a dozen federal government agencies and police departments

Asurtec
Managed IT Solutions

Dealing with Scam emails, text and phone calls

Vishing/Robocalls/Phone scams – con't

Some common phone scams

- A phone call from Microsoft saying your computer is infected or compromised in some way.
- A phone call Visa/Bank with either a pre-recorded or a person on the line stating there is an issue with your account or a payment you made.
- A phone call from a government agency telling people that their social insurance numbers have been compromised
- They really are banking on the fact that we may just trust a human voice rather than an email.

Asurtec
Managed IT Solutions

Dealing with Scam emails, text and phone calls

Vishing/Robocalls/Phone scams – con't

TIPS -

- Join the "National Do Not Call Registry – Canada.ca"
- Don't answer the phone. Simply let the call go to voice mail.
- Hang up
- Don't press buttons or respond to prompts
- Verify the caller's identity

Asurtec
Managed IT Solutions

CREATING STRONG PASSWORDS

Our recommendation is to create long, complex passwords and applies to all internet uses – social media, financial transactions, email accounts etc.

Some tips to consider

- Create passwords that are at least 8 characters long
- Use all keys on the keyboard
- Avoid dictionary words
- Avoid commonly used password patterns
- Use unique passwords
- Update your passwords about every 6 months

Asurtec
Managed IT Solutions

KEEPING YOUR PASSWORDS SAFE

Who knows the first rule of thumb for keeping your passwords safe?

- Do not any share your passwords with anyone
- Do not save your passwords on a spreadsheet
- Do not upload them on the cloud
- Use a Password Manager

Asurtec
Managed IT Solutions

Social Media – Think before you post

Whether you post a picture, comment or a video, you want to ensure that whatever you post is a reflection on you.

You want to feel good about the information you share online. Don't share anything that you wouldn't want shared with the world.

Remember

- Even with privacy setting to limit your audience there is always that chance that the information you share can be copied and shared by others.

Asurtec
Managed IT Solutions

Social Media – Think before you post

TIPS -

- Always check your privacy settings
- Don't click on links, coupons, or answer survey's
- Use strong, long password
- Avoid giving out your current location

Asurtec
Managed IT Solutions

Social Media – Think before you post

TIPS - con't:

- Stick to people you know
- Never add personal or financial information to a social media site
- Report abuse from anyone
- Know fact from fiction

Asurtec
Managed IT Solutions

Privacy 101 – Online shopping, banking and other financial transactions

The internet has had a tremendous impact on the way we do many things these days

Online today we can -

- Do our shopping
- Do our banking and make investment purchases
- Pay our taxes
- Make our travel plans
- Book appts, receive medical information

Asurtec
Managed IT Solutions

Privacy 101 – Online shopping, banking and other financial transactions

TIPS –

- Only shop at reputable online merchants
- When shopping or banking look for secure websites/mobile apps
- Use a credit care where possible, or a debit cards or paypal

Asurtec
Managed IT Solutions

Privacy 101 – Online shopping, banking and other financial transactions

TIPS –

- Be careful before you click - carefully review all transactions before confirming them
- Mistakes can happen – contact the company right away
- Use the cancelation feature
- Read and understand **return policies**

Asurtec
Managed IT Solutions

INTRODUCTION TO CYBERSECURITY

QUESTIONS??

Asurtec
Managed IT Solutions

INTRODUCTION TO CYBERSECURITY

THANK YOU FOR YOUR TIME!!

Asurtec
Managed IT Solutions

INTRODUCTION TO CYBERSECURITY

Seminar Resources

- ***Statistics Canada – Seniors Online*** ***https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2019024-eng.htm***
- ***Seniors and technology during Covid-19: the latest insights*** ***https://www.ericsson.com/en/blog/2021/1/seniors-and-technology-during-covid***
- ***How can older adults safely use Social Media*** ***https://www.homecareassistancewinnipeg.ca/how-can-seniors-use-social-media-safely/***

Asurtec
Managed IT Solutions

INTRODUCTION TO CYBERSECURITY

Contact Information - If you are looking for more information on our Services or Training please contact:

inquiries@asurtec.com or 1.844.asurtec (1.844.278.7832) ext. 204

Asurtec
Managed IT Solutions