****

****

Seminar Safety Part 4:

Protecting Yourself Online, Scams, Fraud, Cyber Security

Session Outline:

1. Introduction
2. Communication
3. What is the internet? How does it work?
4. Using technology to stay connected – the many devices
5. Social Media
6. Cyber Safety
7. Phishing
8. Scams, Fraud
9. Passwords
10. Protecting Yourself Online

Section 1 – Introduction:

Welcome everyone. I’d like to start off by saying that you should not fear using your devices, be bold, explore the features of your devices, and ask lots of questions. Your network of family, friends and neighbours may know how to do something you don’t, and why not learn from them too. In no time you’ll be confident in how to do things all on your own.

This topic is an important one for everyone of all ages. We’re going to be talking about the many ways we are often unsafe or vulnerable online and how we can protect ourselves. Our goal here today, is for you to explore some safer ways of using your devices and implement those tips into your routine use of technology.

Section 2 - Communication:

As we all know, people talk to each other for numerous reasons: sharing information can make our lives easier and gives us a sense of togetherness, talking helps us to grow social bonds with others, and being able to choose what we talk about is important to what it means to be ‘us’. Sometimes we talk to others to help others and be helpful. Making connections with other people has a tremendous impact on our happiness!

Section 3 – What is the internet? How does it work?:

The internet is a network that allows digital devices to talk to one another. It allows digital information to travel around the world. Let’s just say that this part can get really complicated, but it doesn’t have to be. Around the world there are networks of cables that run underground and that lay along sea floors, in the deep sea that carry data at the speed of light from country to country, so on and so forth. It’s this infrastructure that let’s us do the many things we enjoy doing online, like chatting with our friends and family, and learning new things online.

Section 4 – Using technology to stay connected / Devices:

In this section we will present to participants the many general ways we use technology to stay connected; keeping it brief and particularly simple. As the slides progress, we will go into more detail.

Speaking points – most people have mobile phones these days, and many people still have landlines, for their own reasons. For those of us who still have land lines it might be because we have poor cellular signal in our homes, because we don’t want a mobile phone because its expensive, or just maybe even a combination of the two! Some of us have computers, new and old. Some of us prefer tablets that have touch screens like iPad’s and Androids. In most cases, all of these devices [with the exception of a landline] are all smart devices and can do so much. Whatever devices you choose to have and use, remember, no device is the wrong device, it’s how you use it!

Section 5 – Social Media:

Here we will talk about social media best practices and the various types.

What is it? Social media is a program / application of sorts, that uses a device, which connects to the internet and let’s you socialize and stay connected with friends and family. Sometimes, it isn’t even staying connected with family and friends, it’s about following the latest news. Be careful with that one though, surrounding ourselves with a lot of bad news can add unnecessary stress to our lives. Some examples of these applications to name a few are:

* WhatsApp
* Facebook
* Instagram
* YouTube
* WeChat

Each of those have a different audience and are used for different reasons. Some are more for posting pictures, others for watching videos, and some for both! Usually when people think about social media, they think about staying in touch / connected with their family and friends, staying up-to-date. Whichever social media you choose to have, try not to have too many. It can be super overwhelming trying to manage all of these at the same time. Try and pick one to three to help minimize the amount of information that could cause screen fatigue. Try turning off notifications, or limiting them, by exploring the notification settings, and then simply checking the application when YOU WANT TO.

Section 6 – Cyber Safety (Calls, texts, emails):

Talking Point ONLY - Now that the internet has become an essential part of our everyday lives, understanding that using it comes with its own set of risks. We share more of our personal data online now than ever before, and keeping our information safe from fraudulent activity is vital. Let’s have a look at some of the cyber threats that are out there and how to protect ourselves against them. In the following slides we will look at examples of some of the scams going around.

Section 7 – Phishing:

Read off slide and then use the below sentence to further elaborate.

They knew that most users wouldn’t take the bait, but that a few likely would.

Section 8 – Identifying Scams & Fraud:

Email Example 1: Let’s all take a look at this email. Let’s see if we can figure out what’s wrong with it. Talk about the red flags of the email using the commentary below as a guide.

In the spots marked in yellow highlighter my name and email were there, so don’t worry about that. Talk about red flags, anyone see that wacky email address? Filled with letters and numbers, lowercase and uppercase, and super long! That’s a huge red flag that we don’t recognize the sender. How about the subject at the top? It says “Confirm your identity please!” Which is what convinced me to open it up in the first place, why would I need to confirm my identity? The answer, you do not. This is definitely something we need to be aware of. Then they let me know that I’m a winner, but in order to claim my prize, I should click on the blue “confirm identity” button and add in my personal details. Here’s the thing, the moment I click that button, they will likely ask me to enter my personal information like credit card or debit card to just pay for shipping and I will get the prize. But no prize will ever arrive at my door, and my personal information was just given away, not stolen. I would have been responsible for giving my own information. Let’s say you don’t want to receive these emails anymore, how about clicking that “U.n.s.u.bs.c.r.i.b.e” button? It’s spelled very incorrectly and irregularly, that’s a huge red flag.

If you see this type of email, don’t hesitate to delete it, mark it as spam/junk, or even ask a family member or friend if you aren’t sure to check its validity. Nowadays we receive email notifications from pharmacies saying our prescription is ‘ready for pickup’ – So let’s make sure that just because we receive a message that looks real, we understand that we don’t need to click on anything or reply, we can always pick up the phone and call the pharmacy ourselves!

After going through this email and identifying red flags in the email, move on to the following slides where more examples will be illustrated. Take the time to have participants become familiar with what a scam message looks like.

Section 9 - Passwords:

Review slides with participants. By the end of this section, participants should be encouraged to write down their passwords in a safe and secure location where they can retrieve this information whenever needed. They should also include their security questions etc. in case they ever get locked out of their account.

Section 10 – Protecting Yourself Online:

This section has been reserved for the review of everything learned but in bullet point form. Restate each point on the slides one at a time for participants to round up the presentation.

Review Points:

* Be suspicious of unknown phone numbers and emails
* Try choosing 1-3 social media platforms, it can be extremely overwhelming having too many sources of communication, even for professionals!
* Just because someone texts you, doesn’t mean you have to text too! Call them, use your technology, your way.
* If possible, turn off or minimize the alerts and notifications you receive. This will help you focus on matters most reduce the chances of screen fatigue you may experience.
	+ Example: You don’t need an email from Facebook saying that you have a message. Simply go check Facebook when you want to.
* Write down your passwords in a dedicated password notebook. Leave some extra space in case you have to change or update your passwords.
* Use a passphrase instead of a password.
* When you do go shopping, if a retailer asks you for your email, let them know you don’t want to receive any marketing or flyers to your email. If they want to send you the receipt, it has to be JUST THAT.
* If something in a text or email looks too good to be true, then it probably is! Delete it immediately.

|  |  |
| --- | --- |
| The Guardian – What is the Internet? | <https://www.theguardian.com/technology/2018/oct/22/what-is-the-internet-13-key-questions-answered> |
| CRTC FRAUD | <https://crtc.gc.ca/eng/phone/telemarketing/fraud.htm> |
| Scams | [Fightspam.gc.ca](https://www.Fightspam.gc.ca) |
| Scams | [Antifraudcentre.ca](https://www.Antifraudcentre.ca) |
| Phishing | [https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html#:~:text=The%20word%20phishing%20was%20coined,%22sea%22%20of%20Internet%20users.](https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html%23%3A~%3Atext%3DThe%20word%20phishing%20was%20coined%2C%22sea%22%20of%20Internet%20users.) |
| Phishing | <https://www.cleo.on.ca/en/publications/scams/what-are-some-common-telephone-and-internet-scams> |