LIT/ CLB 1

LESSON

ISSofBC

Digital Literacy Curriculum Resource

Module 7
Safety and Security

THE UNIVERSITY OF BRITISH COLUMBIA
Learning Exchange

Funded by:
Immigration, Refugees and Citizenship Canada

Financé par :
Immigration, Réfugiés et Citoyenneté Canada

Learning Objectives

1. Understand the concept of 'phishing'
2. Understand how cyber criminals "catch" people
3. Identify hyperlinks
4. Recognize possible 'phishing' emails and text messages and understand how to respond (optional)

Pre-requisite Skills

- **Mouse skills**: hold the mouse, left click, double click, scroll, different shapes of cursor
- **Navigation**: move the mouse around the screen to position the cursor in correct location
- **Keyboarding**: type words, numbers, symbols; use Shift and Enter keys
- **Online skills**: open a web browser, use the address bar, search for a website
- **Email skills**: open an email message
- **Mobile phone skills**: open the "messages" app

Preparation

- Set up a room with computers or laptops for each student
- Read through the lesson outline and notes for the teacher
- Print the handouts for students
- Turn on the projector or interactive whiteboard (Smartboard)

Information for the teacher

The most important takeaway for students from this lesson is that they should never give out personal information online, by text message or over the phone, nor should they click on a link in an email or text message. Understanding the language in the message is not the focus, nor is it important to teach that language.

Materials

- Computers or laptops with access to the internet
- Handouts of the lesson activities
- Projector or interactive whiteboard. If these are not available demonstrate by having students gather around teacher's computer

Visuals

- Module 7-Lit/CLB 1-Introduction-Visual

Handouts

- Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout A Fishing
- Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout B Phishing
- Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout C Stealing Personal Information
- Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout A Catching Victims
- Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout B Catching Victims
- Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout C Catching Victims
- Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout D Catching Victims
- Module 7-Lit/CLB 1-Digital Skill 3-Learn Handout A Hyperlink Styles
- Module 7-Lit/CLB 1-Digital Skill 3-Learn Handout B Identify Hyperlinks
- Module 7-Lit/CLB 1-Digital Skill 4-Learn Handout A Recognizing Phishing Emails
- Module 7-Lit/CLB 1-Digital Skill 4-Learn Handout B Phishing Emails – Dos and Don'ts

LESSON

Introduction to the Module

Maximum 10 minutes

Elicit from students the idea of personal information (e.g. name, address, bank account number, etc.)

If students have trouble offering examples of personal information, you can tell students:

- Personal information is:
  - *name*
  - *birthday / date of birth*
  - *address*
  - *Social Insurance Number*
  - *bank card P.I.N.*
  - *bank account number*
  - *credit card number*
  - *passwords*
  - *driver's license*
  - *passport number*
  - *and more...*

Show **Module 7-Lit/CLB 1-Introduction-Visual** on Smartboard, project on screen in room, or hand out printed copies for students.

Point to woman with phone. Point to man with laptop. Ask students:

Is it OK to give personal information to strangers?

Explain to students that it is important to keep their personal information safe. Tell them not to give personal information to people they don't know.

DIGITAL SKILL 1

Approximate time: 30-45 min

Understand the concept of phishing

Information for the teacher:

It is critical that the students understand the importance of protecting their personal information and that there are people out there who want to steal it.

Objective

Students will be able to:

- understand the concept of phishing

Vocabulary

- **phishing** – an email, text message or phone scam used to steal ("fish for" or "catch") your personal information

Learn

Approximate time 20-30 mins

Elicit from students what they know about the sport fishing.

Show **Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout A Fishing** on Smartboard, project on screen in room, or hand out printed copies for students.

Ask students:

What is this? (point to picture of the fish) Answer: fish

What is he doing? (point to picture of man fishing) Answer: fishing

Do you like fishing?

Do you go fishing?

Teach the words "catch" and "hook" (point to hook in first picture). Tell students:

The man wants to catch a fish. He uses a hook to catch the fish.

(Have students practice these words)

Explain to students that sometimes words with different spelling have the same pronunciation (e.g. "two" and "to" and "too"). Write the word "phishing" on the board or project on a screen. Explain that this word has the same sound as "fishing".

Teach the word "criminal".

Show **Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout B Phishing** on Smartboard, project on screen in room, or hand out printed copies for students. Be sure that students understand the images. Teach the word "criminal". Elicit from students what is happening in both pictures.

Explain to students:

People go fishing to catch fish.
Criminals go phishing to catch your personal information.

Elicit from students:

What do criminals want?

Show **Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout C Stealing Personal Information** on Smartboard, project on screen in room, or hand out printed copies for students.

Important: You should not try to teach all this vocabulary! The only thing that is important is that students understand that criminals can try to steal personal information, money, etc. from them, and that students need to learn to protect themselves.

Use your own discretion to explain to students:

Criminals want to steal (take) your...

- *email address*
- *personal data*
- *email messages*
- *computer login information (username and password)*
- *identity*
- *money*
- *information stored on the cloud*
- *information saved to your phone*
- *bank card or credit card information*

Tell students:

Today, we learn to be safe on your computer and phone.

Practice

Approximate time: 10-15 min

Place students in pairs or small groups and using **Module 7-Lit/CLB 1-Introduction-Visual** and **Module 7-Lit/CLB 1-Digital Skill 1-Learn Handout C Stealing Personal Information**, have students practice saying:

Be safe on the computer and phone.
Do not give personal information!

LIT/ CLB 1

DIGITAL SKILL 2

Understand how cyber criminals "catch" people

Approximate time: 30-45 min

Information for the teacher: It is very important that students understand the concepts of "being afraid or scared" and "being surprised by something unexpected" before teaching this digital skill.

Objective

Students will be able to:

- understand the two main ways cyber criminals "catch" their victims

Learn

Approximate time: 20-30 min

Show Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout A Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

Criminals want you to feel afraid or scared. Criminals:
– send an email
– send a text message
– call you
Criminals tell you about a problem. The problem is with:
– your bank account
– your taxes / the government
– your mobile phone account
– your computer
– or something else
The problem is not true (not real)!

Show Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout B Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

You are afraid. What do you do?
Do not give money or personal information!

Show Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout C Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

Criminals want you to feel surprised or excited. Criminals:
– send an email
– send a text message
– call you
Criminals tell you about a surprise:
– Government tax refund
– money transfer
– package or parcel delivery
– free vacation or prize
– or something else
The surprise is not true (not real)!

Show Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout D: Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:
- You are surprised or excited.
- What do you do?
- Do not give money or personal information!

Practice

Approximate time: 10-15 min

Place students in pairs or small groups and using **Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout B Catching Victims** and **Module 7-Lit/CLB 1-Digital Skill 2-Learn Handout D Catching Victims**, have students practice saying:

The problem is not real OR the surprise is not real.
Do not give money or personal information.

DIGITAL SKILL 3

Approximate time: 30-45 min

Identify hyperlinks

Information for the teacher: Understanding the language in a phishing email or text message is not the focus. You should not attempt to teach that language! It is crucial that students understand that they should never click on a link in an email or text message.

Objective

Students will be able to:
- Identify hyperlinks

Vocabulary

- **click** – to press a button on a mouse or touchpad
- **hyperlink** (also: **link**) – a word or picture in a document or Web page that you can click on with a computer mouse to go to another place in the same or a different document or Web page

Learn

Approximate time: 20-30 min

Be sure that students remember the word ***click***. They would have learned this in Module 1: Mouse and Navigation.

Teach students about hyperlinks. It is not important for students to know or memorize this word. It is only important that students can recognize what a hyperlink is.

Tell students:

Sometimes, an email message (or text message) has
- *different coloured words or numbers (not black)*
- *underlined words or numbers*
- *a box (coloured)*

Show **Module 7-Lit/CLB 1-Digital Skill 3-Learn Handout A Hyperlink Styles** on Smartboard, project on screen in room, or hand out printed copies for students.

Point to the three circled areas on the graphic and ask:

What is this? (Answer: box)
What is this? (Answer: different colour / underlined)
What is this? (Answer: different colour / underlined)

Tell students:

These are hyperlinks.
Hyperlinks take you to another page or website.
Do not click on hyperlinks. Some hyperlinks are bad.

Practice

Approximate time: 10-15 min

Show **Module 7-Lit/CLB 1-Digital Skill 3-Learn Handout B Identify Hyperlinks** on Smartboard, project on screen in room, or hand out printed copies for students.

Place students in pairs or small groups and have them find the hyperlinks in the text message and email examples. Students can circle the hyperlinks on copies of the handouts or as a group activity on the Smartboard if projected in the classroom. Remember, the goal is to have students identify a hyperlink, not understand the words in the messages.

DIGITAL SKILL 4

Approximate time: 30-45 min

Recognize possible phishing emails and text messages and understand how to respond

Information for the teacher: The "Learn" section of this digital skill is optional. Consider the level of the students you are teaching before deciding whether to teach this. If you choose not to teach it, you can skip to the practice activity for this digital skill which helps summarize the Dos and Don'ts when receiving a phishing email or text message. Understanding the language in a phishing email or text message is not the focus. You should not attempt to teach that language! It is crucial that students understand that they should never click on a link in an email or text message.

Objective

Students will be able to

- recognize possible phishing emails and text messages and understand how to respond

Learn

Approximate time: 20-30 min

Now that students have learned how to identify hyperlinks, it is important that they begin to recognize phishing emails and text messages. Review Digital Skill 2 if necessary. Remind students that criminals want to scare or surprise them to steal money or personal information.

Show **Module 7-Lit/CLB 1-Digital Skill 4-Learn Handout A Recognizing Phishing Emails** on Smartboard, project on screen in room, or hand out printed copies for students.

Focus on the first graphic. Tell students that it looks like a real email from online shopping site Amazon. Point out:

- the logo
- the "Order Details"
- the "Hello Customer" greeting, and the closing from Amazon.com
- the "small print" legal info that is often found at the bottom of this type of email

Now show the second graphic. Explain how to recognize a phishing email using the info on the graphic.

- It's not from an Amazon email address.
- Companies never ask you to update personal or financial email through a link in an email or text message.
- You do not remember buying something for this amount. You are not expecting a delivery.

Tell students what to do if they think they have received a phishing email or text message that looks like it came from a bank, post office or business, etc:

- *Do not click on a hyperlink.*
- *Go to your bank or post office.*
- *Log in to your account (in a separate tab). Check information.*
- *Ask yourself: did I buy something?*
- *Do not reply to (answer) the email.*

Practice
Approximate time: 10-15 min

Show **Module 7-Lit/CLB 1-Digital Skill 4-Learn Handout B Phishing Emails – Dos and Don'ts** on Smartboard, project on screen in room, or hand out printed copies for students.

Have students practice telling each other what to do and what not to do if they think that they have received a phishing email or text message.

Closing

What have you learned today?

Review the skills learned and practiced in this workshop. Ask concept-check questions. For example:

Do you give personal information to strangers?
Do you click on hyperlinks?
Do you reply to a phishing email (or text message)?

What are you going to do to practice on your own?

Have students say what they will do to for independent practice before the next session, e.g.

Do the Extra Practice Activity online