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

Module 7: Safety and Security • *TEACHER NOTES*

CLB 5•6

Learning Objectives

1. Understand weak vs. strong passwords
2. Create a strong password
3. Change your email password
4. Identify phishing emails and text messages and how to respond to them
5. Choose a suitable antivirus for your computer and phone

Pre-requisite Skills

- **Mouse skills**: hold the mouse, left click, double click, scroll, different shapes of cursor, hover over objects and links
- **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 information on a website, navigate websites
- **Email skills**: log in to account, open an email message
- **Mobile phone skills**: open the "messages" app and other messaging apps

Preparation

- Set up 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-CLB 5/6-Digital Skill 5-Learn Visual Antivirus icon

Handouts

- Module 7-CLB 5/6-Digital Skill 1-Learn-Handout Are these strong passwords?
- Module 7-CLB 5/6-Digital Skill 1-Practice-Handout True or False?
- Module 7-CLB 5/6-Digital Skill 2-Your Turn-Handout Strong Password Checklist
- Module 7-CLB 5/6-Digital Skill 3-Learn-Handouts A, B or C
- Module 7-CLB 5/6-Digital Skill 4-Learn Handout A Stealing Personal Information
- Module 7-CLB 5/6-Digital Skill 4-Learn Handout B Catching Victims
- Module 7-CLB 5/6-Digital Skill 4-Learn Handout C Catching Victims
- Module 7-CLB 5/6-Digital Skill 4-Learn Handout D Hyperlink Styles
- Module 7-CLB 5/6-Digital Skill 4-Practice Handouts A, B and C Phishing Clues
- Module 7-CLB 5/6-Digital Skill 5-Practice Handout Comparison of Free Antivirus

LESSON

Introduction to the Module

Maximum 5 minutes

Ask students:

What if someone stole our house key? What could that person do? Steal our things. In the online world, criminals can also steal from us. They steal our personal information.

Elicit from students some examples of personal information. Examples are:

- *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…*

What can criminals do if they have our personal information? They can open new bank accounts, get credit cards and loans, make purchases, get a passport, get government support… get government support… ruin our credit and our lives.

How do we keep our personal information safe? Today, we will learn ways to be safe on the internet.

DIGITAL SKILL 1

Approximate time: 30-50 min

Understand weak vs. strong passwords

Information for the teacher: The first vital step to online security is having a strong password for online accounts. However, many people do not understand the importance of having a strong password.

Objective

Students will be able to:

- understand what weak passwords are and the need to create strong passwords

Vocabulary

- **criminal** – a person who commits a crime (does an illegal act)
- **character** – a letter, number, or other mark or sign used in writing or printing
- **crack** – to get into someone else's computer system without permission and get information or do something illegal
- **hacker** – a person who gets into someone else's computer system without permission in order to find out information or do something illegal

Learn

Approximate time 15-20 mins

Ask students:

Do you remember the password of your email address? Is it easy to remember? Just like a house lock and key protect the belongings in your house, passwords protect your online accounts.

Tell students that in today's online world, hackers use computers to crack passwords. Give an example of a common password: batman. Ask:

> *How long do you think it will take for a computer to crack this password?*

Show the results on https://howsecureismypassword.net/. Alternatively, if the students have access to computers, ask them to type the password on the above website and they can find out for themselves. The answer is: instantly.

Show Module 7-CLB 5/6-Digital Skill 1-Learn-Handout Are these strong passwords? on Smartboard, project on screen in room, or hand out printed copies for students. Discuss as a class, if the passwords in the scenarios are strong passwords.

Use password: batman. Show how making a password longer by adding numbers, symbols, using a combination of upper case and lower case letters, makes it more complicated and longer to crack.

Practice
Approximate time: 10-15 min

Distribute Module 7-CLB 5/6-Digital Skill 1-Practice-Handout True or False?

Ask students to try the quiz. Go through the answers.

DIGITAL SKILL 2

Approximate time: 40-55 min

Create a strong password

Information for the teacher: At the time of writing, the following YouTube video is available. It explains in a very clear way, how to create a strong password using a passphrase.

Watch 1:17 – 1:40

https://www.youtube.com/watch?v=25G4tLVH1JE

Objective

Students will be able to:

- Create strong passwords

Vocabulary

- **passphrase** – a phrase or sentence that is easy to remember

Learn

Approximate time: 15-20 min

Design a strong password

Say:

> *Weak passwords are easier to remember but unsafe. But how can we remember complicated passwords? One for every online account we have? Not all of us have such a good memory. Let's look at two ways to design strong passwords.*

1) Design a passphrase

Tell students that they can use a passphrase. A passphrase is a phrase or sentence that is easy to remember.

For example:

- My friend Alan just found a teller job in December at Scotiabank.

Take the first letters of the sentence.

- MfAjfatjiDaS

Replace some letters with numbers or symbols.

- MfAjfatji12@S

Say:

> *Check these 2 passwords on the website:*
> https://howsecureismypassword.net/.
> *How long will it take a computer to crack these passwords?*

2) Use a combination of random words

- VanillaPineHeaterDock becomes V@n!ll@P!n3H3@t3rD0ck
- Check this password on the website: https://howsecureismypassword.net/. How long will it take a computer to crack this password?

Reiterate/Review:

Elicit from students: So what makes for a strong password?

- Has at least 8 characters. The longer, the better.
- Uses a combination of upper and lower case letters
- Uses numbers and symbols...

Practice

Approximate time: 15-20 min

Design a strong password

Divide the class into four teams. Ask the teams to come up with two passwords each: using a passphrase and another, using random words.

Write the passwords on the board. Vote which are the strongest passwords.

Check on https://howsecureismypassword.net to see which team wins.

Your turn

Approximate time: 10-15 min

Based on what they've learned, ask the students to reflect if they think the password of their email account is strong.

Give out Module 7-CLB 5/6-Digital Skill 2 -Your Turn-Handout Strong Password Checklist. Ask students to design a strong password for their own email account based on the checklist.

DIGITAL SKILL 3

Approximate time: 40-55 min

Change the password on your email account

Note to teacher: Students need to log in to their email accounts. Teacher should use a new email account to demonstrate changing password for the first time as there are more steps involved. Subsequent changes are straightforward.

You can easily close the account afterwards if you do not want to keep it. Follow the links below and the instructions.

Yahoo Mail: https://yahoo.mydashboard.oath.com/delete-my-account

Gmail: https://myaccount.google.com/deleteaccount?rapt=AEjHL4NrONArTY6FPgj6Qi3fadAhYn-lojRBmhKjF2iTGXZz3t41wvWzTK69YtZ4_bsH1icDiZm_Oirrx0ydgZsIPt1_7qmaKw

Outlook: https://account.live.com/closeaccount.aspx

Objective

Students will be able to:

- Change their passwords on their Yahoo, Gmail or Outlook email accounts for the first time.

Vocabulary

- **verify** – make sure something is true or correct

Learn

Approximate time: 30-50 min

Say:

> *It is good to change your passwords at least every six months. This reduces the risk of your accounts getting hacked.*

Tell them they are going to learn how to change their email account passwords for the first time. Say:

> *First, write down the winning password from the previous activity in your notebook. Be careful to copy it exactly. Check each other's copied password to be sure that that everyone has the same info. (For this activity, everyone is using the same password so that the teacher or stronger students can easily help if the weaker students have problems.)*

Ask the students to log in to their email accounts.

It is best that all students use email accounts from the same email provider. Depending on which email provider you're using, go through the steps one by one with the students and make sure everyone is at the same step before going on to the next one.

Refer to **Module 7-CLB 5/6-Digital Skill 3 -Learn-Handouts A, B** or **C** for the step-by-step instructions on how to change passwords for the first time for Yahoo Mail, Gmail and Outlook.

The email provider will ask for recovery email/phone details. Explain that giving this information will help them recover their email accounts if they forget the passwords. This is recommended. You may want to continue this with students. Or ask them to click "Remind me later" for Yahoo Mail and ignore it for Gmail. For Outlook, you have to go through the recovery phone number or recovery email with the students. It cannot be skipped.

When they get to the step about entering their new password, tell them to use the winning password from **Digital Skill 2's Practice Activity**. Say:

> *It is very important that you follow all the characters – upper case or lower case letters, and all the symbols exactly, 100%. To check if you typed correctly, click on the eye icon to the right where you enter the password.*

Practice

Approximate time: 15-20 min

Say:

> *Now, we are going to practice changing your email password again. This time, you will use your own password.*

Ask students to use the password they created in **Digital Skill 2 Your Turn** activity.

Distribute **Module 7-CLB 5/6-Digital Skill 3-Learn-Handouts A, B** or **C**, depending on the email provider you have covered. Students can follow the instructions to change passwords for their own email accounts. Alternatively, pair the students up so that student A reads out the instructions, while student B follows the instructions to change their password. Student A can double check that Student B is following instructions correctly and help if needed. Switch roles.

DIGITAL SKILL 4

Approximate time:
50-75 min

Identify phishing emails and text messages, and how to respond to them

Objective

Students will be able to:

- identify phishing emails and text messages, and know how to respond.

Vocabulary

- **phishing** – an email, text message or phone scam used to steal ("fish for" or "catch") your personal information
- **smishing** – phishing using SMS text messages
- **hyperlink** (also: **link**) – a word or picture in a document or web page that you can click on to go to another place in the same or a different document or web page
- **scam** – an illegal way of making money, usually by tricking people
- **legitimate** – allowed by law or done according to the rules of an organization or activity
- **suspicious** – making you feel that something illegal is happening or that something is wrong

Learn

Approximate time:
35-45 min

Introduction: Elicit from students what they had previously learned in Module 4 on how to identify safe websites.

Make sure to review the following if students do not cover everything:

- *Never use public networks or public computers (e.g. library computers) to do any online banking or shopping. If you need to do something important online, turn off the WiFi and use your phone data instead.*
- *It is also a good idea to have antivirus software on your device.*
- *Look at the address bar of a website. A lock symbol and/or 'https' at the beginning means the website is safe to use.*

Ask students:

> *How do criminals get our personal information on the internet? They go phishing!*

Show **Module 7-CLB 5/6-Digital Skill 5-Learn Handout A Stealing Personal Information** on Smartboard, project on screen in room, or hand out printed copies for students. Be sure that students understand the images.

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".

In English, they are called "homophones". Elicit from the students if they know of other homophones.

Explain to students:

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

Elicit from students examples of personal information that criminals want to steal, such as shown on the handout. If students did not mention the following, add:

Criminals also want to steal (take) your...

- *email address and email messages*
- *computer login information (username and password)*
- *information stored on the cloud*

- *information saved to your phone*
- *bank card or credit card information and money*

Show Module 7-CLB 5/6-Digital Skill 4-Learn Handout B Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

Through emails, text messages or phone calls, criminals want you to feel afraid or scared.

They also want you to deal with the problem urgently. Very often, they also tell you that something bad will happen if you tell someone about the problem.

They make you feel afraid or scared by telling you about a problem with:

- *your bank account*
- *your taxes / the government*
- *your mobile phone account*
- *your computer*
- *your SIN*
- *or something else*

Show Module 7-CLB 5/6-Digital Skill 4-Learn Handout C Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

They may also want you to feel surprised or excited by telling you about a surprise:

- *Government tax refund*
- *money transfer*
- *package or parcel delivery*
- *free vacation or prize*
- *or something else*

Elicit who has received such an email, text message or phone call which made them feel afraid, or excited, and how often they receive such messages and calls.

So how can we identify phishing emails and text messages? Here are some more pointers:

- *The text message or email asks to confirm your personal information: The email may look real, but legitimate companies will not ask you to click on a link to confirm your personal information. Go online and search for the organization's contact and ask them. Do NOT click on any hyperlinks in the text message or email.*
- *Double check the email addresses and the hyperlinks: Often the phishing email address or hyperlink looks real because it includes the name of the real company within the structure of the email and hyperlink. For example, @staples.ca vs. @bit.ly/staples-ca. Before you click on a link, hover over the link. You'll be able to see the link address on the bottom left corner of your screen. Check it with older emails that you had received from this company.*
- *Spelling and grammar errors: A legitimate company will have checked all spelling and grammar before sending out emails and text messages to their customers.*
- *Beware of suspicious attachments: If you receive an email from a company unexpectedly, and it contains an attachment, be careful as it may be infected. Scan it first with an antivirus software.*

Show **Module 7-CLB 5/6-Digital Skill 4-Learn Handout D Hyperlink Styles** on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

> *Not all hyperlinks look like underlined words or numbers. They may be in different coloured words or numbers (not black), or a box. When you hover over them, the cursor becomes a hand. This means it is a hyperlink. They take you to another page or website. Some hyperlinks may be phishing attempts, or they can infect your computer or cell phones with viruses.*

Show **Module 7-CLB 5/6-Digital Skill 4-Learn Handout E Identifying 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 "Dear 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 into your account (in a separate tab). Check your information.
- Ask yourself: did I buy something?
- Do not reply to (answer) the email.
- Think before you click. If something looks suspicious, delete it.

Practice

Approximate time: 15-30 min

Distribute **Module 7-CLB 5/6-Digital Skill 4-Practice Handout A, B and C Phishing Clues** handout to each student.

By referring to Handout A, ask students to work in pairs to circle and identify the phishing clues in Handouts B and C.

Go through the answers.

(At the time of writing, Google has a very good phishing quiz which you may want your students to try: https://phishingquiz.withgoogle.com/?hl=en)

DIGITAL SKILL 5

Approximate time: 25-45 min

Choose suitable antivirus software for your computer or phone

Note to teacher:

Apple iPhones' IOS platforms are developed with security in mind and do not need antivirus at all. You only need to install updates to keep your device safe.

Objective

Students will be able to:

- Choose suitable antivirus software for their computer or phone

Vocabulary

- **malware** – any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

Learn

Approximate time: 10-15 min

Say:

> *Have you heard of computer viruses? Trojan horses, worms, spyware, ransomware etc.? They are all bad programs that can infect or damage your computer or computer network. Together, they are called malware. Don't worry, there are ways to protect yourself from these threats.*
>
> *First and most importantly, make sure you have installed the latest updates on your device. This is because updates remove security holes that have been discovered, and fix and remove computer bugs. You'll also get the latest features on your device.*
>
> *Secondly, you can install antivirus software in your computer or android phone. It is a computer program used to prevent, detect and remove malware. We will look at some free antivirus available out there.*

Computer antivirus software

> *If you're using a computer with Windows 10, it comes installed with Microsoft Windows Defender by default. Experts say it is actually a pretty good antivirus software. For many of us, it is all we need. There is also other free and paid antivirus software programs that we can download.*

To check if you have antivirus installed, look for the antivirus icon in the task bar of your desktop. It is on the bottom right corner of your screen. Show Module 7-CLB 5/6-Digital Skill 5-Learn Visual Antivirus icon on Smartboard, project on screen in room, or hand out printed copies to students.

Antivirus for android phones

> *If you have an iPhone, you don't have to worry about installing antivirus. However, if you have an android phone, and you do online transactions and have lots of sensitive information on your phone, then you should download a free or paid version of an antivirus app.*

Practice

Approximate time: 15-30 min

Tell the students that they are going to search for a free antivirus for their computer or android phone.

Instructions:

- Open your web browser.
- Search for free computer antivirus 2020 (or current year) or free android antivirus 2020 (or current year)
- Remember results that appear on top are usually ads.

- Choose two websites to compare. (If students are not sure which websites are good, suggest trusted sites such as pcmag, cnet and tom's guide)
- Record your findings in the handout.

Distribute **Module 7-CLB 5/6-Digital Skill 5-Practice Handout Comparison of Free Antivirus** to students.

Big names such as Bitdefender, Kaspersky, Avast and AVG are all acceptable, as long as students can explain why. McAfee and Norton have trial editions but need a subscription after the trial period.

Closing

What have you learned today?

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

- What are the characteristics of a strong password?
- What are two ways to create a strong password?
- What are the signs of a phishing email or text message?
- What are the steps to take if you receive a phishing email or text?
- How can you protect your device from malware?

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

Have students say what they will do for independent practice, e.g.

Do the Extra Practice Activities online