



# 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 weak vs. strong passwords
2. Create a strong password
3. Change your email password
4. Identify hyperlinks
5. Identify 'phishing' emails and text messages, and how to respond to them

## 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 a website
- **Email skills:** open an email message
- **Mobile phone skills:** open the "messages" app and other messaging apps

## 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

## Handouts

- Module 7-CLB 2/3-Digital Skill 1-Learn-Handout Are these strong passwords?
- Module 7-CLB 2/3-Digital Skill 1-Learn-Handout-Answer Key
- Module 7-CLB 2/3-Digital Skill 1-Practice-Handout True or False?
- Module 7-CLB 2/3-Digital Skill 2 -Your Turn-Handout Strong Password Checklist
- Module 7-CLB 2/3-Digital Skill 3 -Learn-Handouts A, B or C
- Module 7-CLB 2/3-Digital Skill 4-Learn Handout A Phishing
- Module 7-CLB 2/3-Digital Skill 4-Learn Handout B Stealing Personal Information
- Module 7-CLB 2/3-Digital Skill 4-Learn Handout C Catching Victims
- Module 7-CLB 2/3-Digital Skill 4-Learn Handout D Catching Victims
- Module 7-CLB 2/3-Digital Skill 4-Learn Handout E Hyperlink Styles
- Module 7-CLB 2/3-Digital Skill 4-Practice Handout Identify Hyperlinks
- Module 7-CLB 2/3-Digital Skill 5-Learn Handout A Identifying Phishing Emails
- Module 7-CLB 2/3-Digital Skill 5-Learn Handout A-Answer Key
- Module 7-CLB 2/3-Digital Skill 5-Learn Handout B Phishing Emails – Dos and Don'ts

# LESSON

## Introduction to the Module

Maximum  
10 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... they can destroy 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:  
30-45 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 breaks the law (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 20-30 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 our homes, passwords protect our online accounts*

Tell students that in today's online world, hackers use computers to crack, or get

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 2/3-Digital Skill 1-Learn-Handout Are these strong passwords? on Smartboard, project on screen in room, or give as handout. Ask the class if they use any of the examples shown as their password. Go through all the passwords as a class, and ask the students to choose 'Yes' or 'No'. After they finish, tell them to go to <https://howsecureismypassword.net/> to check their answers. You may also assign one or two students to each number, to save time. Refer to Module 7-CLB 2/3-Digital Skill 1-Learn-Handout-Answer Key and go through the reasons why all the passwords are weak.

Review 'symbols', and 'upper and lower case letters' by typing and projecting on the screen. Go through how to type symbols and upper case letters by using the Shift key.

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. Check the results on <https://howsecureismypassword.net/>.

**Practice**

Approximate time:  
15-25 min

Distribute Module 7-CLB 2/3-Digital Skill 1-Practice-Handout True or False? Ask students to try the quiz. Go through the answers.

Alternatively, this can be used as a class quiz with the students divided into different teams. The teacher shows Module 7-CLB 2/3-Digital Skill 1-Practice-Handout: True or False? on Smartboard, or project on screen in room – question by question, explaining where needed. The teams choose True or False. The teacher or a designated student can keep score. The team with the highest number of correct answers wins.

**DIGITAL SKILL 2**

Approximate time:  
60-90 min

**Create a strong password**

**Information for the teacher:** At the time of writing, the following YouTube video by Google for Education 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**

- **random** – chosen by chance; not planned

**Learn**

Approximate time:  
25-35 min

**Design a strong password**

Say:

*Weak passwords are easier to remember but unsafe. But how can we remember difficult 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 found a job in December at Scotiabank.

Take the first letters of the sentence.

- MfAfajiDaS

Replace some letters with numbers or symbols.

- MfAfaji12@S

Say:

*Check these 2 passwords on the website:*

<https://howsecureismypassword.net/>.

*How long will it take a computer to crack these passwords?*

In case you have to explain the ‘quintillion’ and ‘sextillion’ years, this is the link to [Wikipedia: https://en.wikipedia.org/wiki/Names\\_of\\_large\\_numbers](https://en.wikipedia.org/wiki/Names_of_large_numbers), or you can just google them.

**2) Put unconnected words together**

Explain ‘random’.

- SnowHeaterWindowBeautiful becomes Sn0wHeaterW1nd0wBeaut1ful when you change ‘i’ into the number ‘1’, and ‘o’ into the number ‘0’
- 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 how can we create 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:  
20-35 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:  
15-20 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 2/3-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:  
45-60 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. It would be very helpful if there were class volunteers for this activity.

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](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**

- **current** – belonging to the present time
- **verify** – make sure something is true or correct

**Learn**

Approximate time:  
45-60 min

Say:

*It is good to change your passwords at least every six months. This keeps your accounts safe.*

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 last 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. (Or you can have volunteers, or appoint a team leader at each table to check that everyone's copied password is the same. For this activity, everyone is using the same password so that the teacher, volunteers 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 2/3-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 details. Ask them to click "Remind me later" for Yahoo Mail and ignore it for Gmail. If you have class volunteers, then you may consider to continue with the steps for recovery email/phone number. For Outlook, you have to go through the recovery phone number or recovery email with the students. It cannot be skipped. You will need classroom volunteers if you are using Outlook.

Pair a stronger student with a weaker one. Make sure each is in their own email account. Go through the steps one by one. Ask the students to check each other that they have completed the steps you demonstrated before going on to the next.

When they get to the step about entering their new password, tell them to use the winning password they created from Digital Skill 2 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. (demonstrate on the screen)*

If there are students who are using another email provider than the one you demonstrated, the volunteers may use the relevant Module 7-CLB 2/3-Digital Skill 3 -Learn-Handouts A, B or C to change their passwords with them.

## DIGITAL SKILL 4

Approximate time:  
45-60 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:  
30-40 min

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.*

*It is also a good idea to have an antivirus program on your phone or computer. It is a program that protects your phone or computer.*

*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 2/3-Digital Skill 4-Learn Handout A Phishing 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”.

Explain to students:

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

Elicit from students examples of personal information shown on Module 7-CLB 2/3-Digital Skill 4-Learn Handout B Stealing Personal Information that criminals

want to steal. 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 2/3-Digital Skill 4-Learn Handout C Catching Victims on Smartboard, project on screen in room, or hand out printed copies for students.

Tell students:

*Criminals use emails, text messages or phone calls to make you feel afraid or scared about a 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*

*Very often, they also tell you that something bad will happen if you tell someone about the problem. But the problem is not true (not real)!*

Show Module 7-CLB 2/3-Digital Skill 4-Learn Handout D 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 such as a:*

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

Tell students:

*You are surprised or excited.*

*What do you do? Do not give money or personal information!*

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 emails, messages or calls.

Teach students about hyperlinks. It is 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-CLB 2/3-Digital Skill 4-Learn Handout E 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)*



	<p><i>What is this? (Answer: different colour / underlined)</i>  <i>What is this? (Answer: different colour / underlined)</i></p> <p>Tell students:  <i>These are hyperlinks. When you hover over them, the cursor becomes a hand. This means it is a hyperlink</i></p> <p>(Demonstrate on a live webpage's hyperlink)  <i>Hyperlinks take you to another page or website.</i>  <i>Do not click on hyperlinks on emails and text messages you don't trust. Some hyperlinks are bad.</i></p>
<p><b>Practice</b>  <i>Approximate time:</i>  <i>15-20 min</i></p>	<p>Show Module 7-CLB 2/3-Digital Skill 4-Practice Handout 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.</p>
<p><b>DIGITAL SKILL 5</b>  <i>Approximate time:</i>  <i>45 – 60 min</i></p>	<p><b>Identify phishing emails and text messages, and how to respond to them</b></p>
<p><b>Objective</b></p>	<p><b>Students will be able to:</b></p> <ul style="list-style-type: none"> <li>Identify phishing emails and text messages, and know how to respond.</li> </ul>
<p><b>Vocabulary</b></p>	<ul style="list-style-type: none"> <li><b>phishing</b> – an email, text message or phone scam used to steal (“fish for” or “catch”) your personal information</li> <li><b>smishing</b> – phishing using SMS text messages</li> <li><b>confirm</b> – prove or make sure something is true</li> <li><b>legitimate</b> – allowed by law or done according to the rules of an organization or activity</li> <li><b>suspicious</b> – making you feel that something illegal is happening or that something is wrong</li> </ul>
<p><b>Learn</b>  <i>Approximate time:</i>  <i>35-45 min</i></p>	<p>Tell students that besides recognizing emails and text messages that make them feel afraid or excited, the following are other signs of phishing emails and text messages. Be sure to teach the meaning of ‘confirm’ and ‘legitimate’ first.</p> <ul style="list-style-type: none"> <li><i>The text message or email asks to confirm your personal information: The email may look real, but legitimate, or real 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.</i></li> <li><i>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 or 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.</i></li> </ul>

Demonstrate on the screen by hovering over a hyperlink.

- *Spelling and grammar errors. A legitimate company will check all spelling and grammar before sending out emails and text messages to their customers.*
- *Beware of suspicious attachments. Be careful if you receive an email that you do not expect, and it contains an attachment. Scan it first with an antivirus software.*

Show Module 7-CLB 2/3-Digital Skill 5-Learn Handout A 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 Module 7-CLB 2/3-Digital Skill 5-Learn Handout A-Answer Key. 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 information 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 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.*

Show Module 7-CLB 2/3-Digital Skill 5-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:

*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?*

### **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*

---