Curriculum Resource

Cybersafety 1

OALCF Alignment

Competency	Task Group	Level
Competency D - Use Digital Technology	**N/A**	**1**
Choose an item.	**N/A**	**1**
Choose an item.	**Choose an item.**	**Choose an item.**
Choose an item.	**Choose an item.**	**Choose an item.**
Choose an item.	**Choose an item.**	**Choose an item.**

Goal Paths (check all that apply)

- ☒ Employment
- ☐ Apprenticeship
- ☐ Secondary School Credit
- ☐ Postsecondary
- ☒ Independence

Embedded Skills for Success (check all that apply)

- ☐ Adaptability
- ☐ Collaboration
- ☐ Communication
- ☐ Creativity and innovation
- ☒ Digital
- ☐ Numeracy
- ☒ Problem Solving
- ☒ Reading
- ☐ Writing

Notes: Cybersafety 1 and Cybersafety 2 cover more basic and more complex issues of cybersafety and are aimed at level 1 and level 2 respectively.

Cybersafety: Part 1

What is Cybersafety?

Computers and smartphones are helpful in the modern world, and they can be a lot of fun. But using them comes with risks. **Cybersafety is about managing those risks.**

Cybersafety means protecting yourself so you can use computers or smartphones safely.

Goals of This Resource

By the end of using this resource, you will have an introduction to:

- ✓ **Protecting your passwords** so they don't get lost or stolen.
- ✓ Managing your online **information** and online **presence**.
- ✓ Spotting untrustworthy websites and links to avoid **viruses** and **spam**.
- ✓ Handy cybersafety **tips** and **tricks**.

Plus:

- ✓ *Some practice activities to make sure you're on the right track.*

Table of Contents:

1. *Introduction: Why Do We Need Cybersafety?*

There's no need to be afraid of using computers, smartphones or the internet. But it's a good idea to be **smart** and **cautious** to avoid the risks that do exist.

What are the risks?

- If you **forget** or **lose** your passwords, you may be **locked out** of your smartphone and important websites, like your bank.

- If you are not careful about your **privacy**, companies can **track** your info and location.

- If you don't **back-up** your data, you could lose important items like photos and videos.

- If you're not **careful** about what you post online, if could **negatively** affect your relationships or your chance to get a job.

- If you click on **dangerous links** or visit **risky websites**, you could get a computer **virus** or even have your information stolen.

2. *Passwords*

These days, we are often required to have **multiple** passwords! Passwords for smartphones, for email, for online banking, and more. That's why it is ***so important to keep your passwords safe.***

Here's what you need to know:

What are the risks?

a. ***Forgetting*** *or* ***losing*** *a password might mean that:*

- You are locked out of your computer or phone.
- You are locked out of your email.
- You are locked out of your online banking.
- You are locked out of other important apps.

b. *But even worse, if someone* ***guesses*** *or* ***discovers*** *your password, they can:*

- Access your information.
- Snoop in your email.
- Steal money out of your bank account.
- Steal your information and identity.

What can you do about it?

There are three key steps to protecting your passwords:

a. **Make STRONG passwords.**
b. **Keep them written down somewhere safe that only you have access to.**
c. **Don't tell ANYONE your passwords.**
d. **Don't use the same password for everything.**

The trickiest one is the first one: ***how do you make a strong password?***

Tips for Making Strong Passwords

*A strong password is **easy for you** to remember but **hard for other people** to guess.*

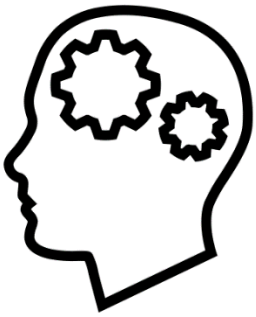
- **DON'T** use your name, your birthday, or other personal information like your address or the name of your dog.
- **DON'T** use the same password over and over again for different things.

- **DO** use a long password that is at least eight characters long. *(Characters are letters, numbers, and symbols.)*
- **DO** use some numbers and symbols, and some upper and lower case letters.

Activity #1

Listed below are three different passwords.

a. Circle whether each is **strong** or **weak**.
b. **Explain why** and **how it could be better**.



Password 1:

Steve is choosing a password for a new email account. He chooses his address, thinking it will be easy to remember. He comes up with: ***maplestreet22***

Circle whether it is:

STRONG ***WEAK***

Explain why and how it could be better:

Password 2:

Anna is choosing a password for a new bank account. She chooses the name of her kids with their ages. She comes up with: ***max10amber6***

Circle whether it is:

STRONG ***WEAK***

Explain why and how it could be better:

Password 3:

Steve is choosing a password for a new Google account. He chooses his favourite food, with an easy to remember number. He comes up with: ***banana123***

Circle whether it is:

STRONG ***WEAK***

Explain why and how it could be better:

Password 4:

Anna is choosing a passcode for her new iPhone. She chooses the year she was born, thinking it will be easy to remember. She comes up with: ***1985***

Circle whether it is:

STRONG ***WEAK***

Explain why and how it could be better:

---

3. *Protecting Your Privacy and Personal Information*

We don't hand out our personal information to strangers on the street, but we put **a lot** of information about ourselves online! That's why it's ***so important to protect your personal data***.

Here's what you need to know:

What are the risks?

a. *If you don't protect your privacy, companies or individuals can:*

- **Take** your personal information, like your photos, and use it.
- **Take** your personal information to help them sell you things.
- **Track** your location.

b. *But even worse, people with bad intentions can:*

- **Steal** your information.
- **Steal** money out of your bank account.
- **Steal** your identity.

What can you do about it?

The first thing to do is **SIGN OUT** and **check your privacy settings** whenever you are using a new device or social media account. Usually, you go into settings by clicking on your **profile icon** in the top right corner and then going to **privacy**.

Here are some examples:

Protecting Your Privacy on Your iPhone:

Protect your photos:

a. Go to your **Settings** app  and scroll down to **Privacy**.
b. Tap Privacy, and then tap **Photos**.
c. You will be shown a list of apps that want access to your photos.
d. Tap the apps you don't want to have access and tap **None**.

Protect your location:

a. Go to your **Settings** app  and scroll down to **Privacy**.
b. Tap Privacy, and then
c. Tap **Location Services**.
d. You can turn this off so that your location **can't be tracked** but if you do, apps like **Maps** and **Find My** won't work until you turn it back on.
e. Instead, you can scroll through the apps you don't want to have access and tap **Never**.

Protecting your Privacy on Facebook:

a. Control your **privacy settings**.
   - Click the little circle with your profile picture in the top right corner.
   - Click Settings & Privacy.
   - Click Settings again.
   - Click Privacy again on the left.

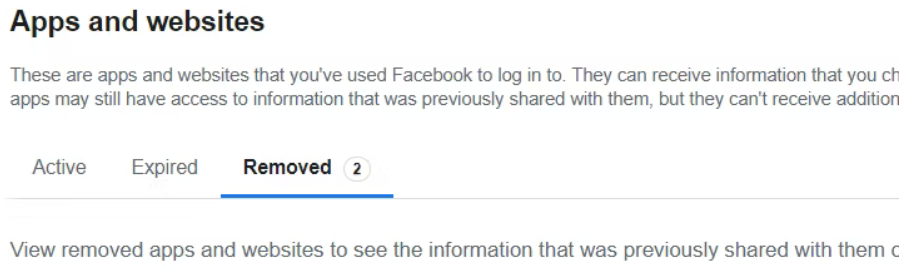
A window will open that allows you to manage ***who sees your account***. For example, this shows you who can see your future posts:

Your Activity	Who can see your future posts?	**Friends**

You can edit any of these settings so that you feel more secure.

b. Make sure no one is **stealing your information** by preventing invasive apps from doing so.

- Find the arrow in the top right corner and click on it.
- Click on **Settings and Privacy** from the menu.
- Then click **Settings** again.
- Scroll down to **Apps and Websites** and click.
- Select the **Active** tab at the top of the window:



Use this screen to remove apps that you don't want to have access to your information.

c. Choose your friends wisely!

Unfortunately, ***not everyone*** *who asks to be your friend on Facebook is trustworthy*.

- Only accept friend requests from people you know in real life!
- NEVER give out personal information to people you don't know!
- NEVER give out personal information over the computer!

4. Backing up Your Data

We used to keep our important photographs and letters in **shoeboxes**, but now so many things that matter to us are stored online. That's why it's ***so important to ensure you don't lose your precious data.***

Here's what you need to know:

What are the risks?

a. Losing valuable **photos**, **videos**, **letters**, professional documents (like **resumes**) and other **memorabilia**.

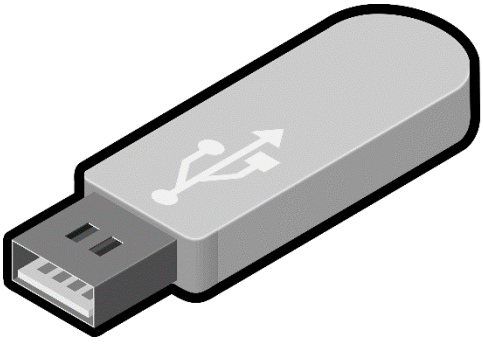
What can you do about it?

Backing up the Data on a Computer

If you are using a computer, always back up your documents on a **USB** stick. A USB stick can be plugged into **any computer** and purchased at a corner store **fairly cheaply**.

In **MS Word** or **Google Docs**:

- Click File.
- Click Save As.
- Click Computer.
- The USB stick should appear as an option in the list on the left.
- Click it and save your document.



Backing up the Data on your iPhone

It's important to have a **backup** of all the things stored on your iPhone, ***especially your photos and videos!*** To make sure you have backup:

a. Go to your **Settings** app  and tap on your **name**.
b. Tap **iCloud** and then **iCloud backup**.
c. Switch your backup **on**.

This will allow you to access your data through iCloud on the internet.

5. Spam and Viruses

Most websites we visit and emails we get are safe, but some bad people out there have built websites or links that can be harmful to your computer or smartphone. That's why it's ***so important to avoid spam and viruses and know what to do if you can't***.

Here's what you need to know:

What is spam?

- Spam is any kind of **annoying, unwanted email or text** that is sent to you. Sometimes it is just advertisements, but sometimes it contains a **virus**.

What are viruses?

- A virus is a type of computer "code" that can **wreck your computer or phone**.
- It can also be used to **steal** your personal information.

How do you get spam or viruses?

The most common way to get spam or viruses is by:

- Going to **untrustworthy websites.**

Or:

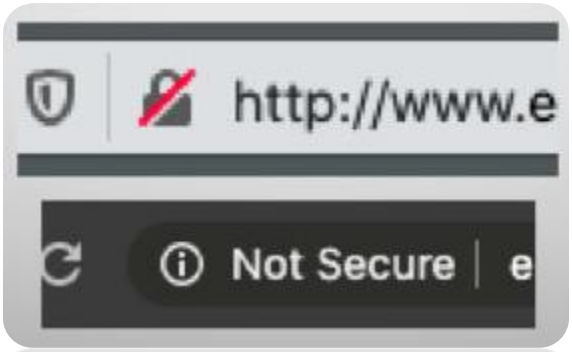
- Clicking **untrustworthy links**.

What can you do about it?

Unsafe Websites

The first thing you need to know is which websites are trustworthy.

- Most popular websites like YouTube and Facebook and Amazon are **very secure**, and you don't need to worry.
- But you should be **more careful** when going to less familiar websites.
- If you go to a website and see the warning **Not Secure**, you should leave right away.



You know the website you are on is secure in two different ways:

a. The Lock

*Notice the **locked** lock displayed by three main web browsers:*

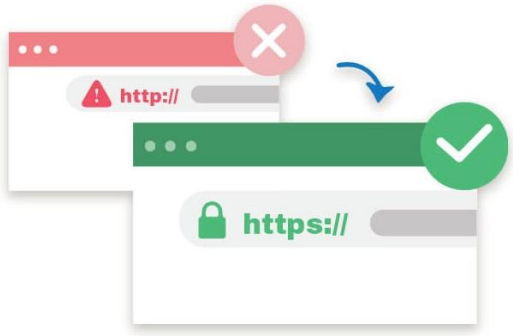
GOOGLE CHROME

INTERNET EXPLORER

MOZZILA FIREFOX

b. The “s”.

Secure websites begin https:// but unsecure websites don’t have the “s”, which stands for **SECURE**.



Unsafe Links

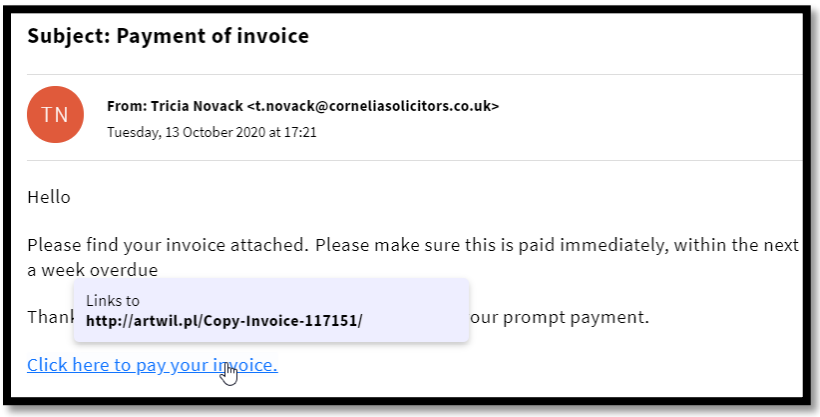
The second thing you need to know is which links not to open.

Links are parts of an email, a text message or a website that you can **click on** to make something happen.

- You can identify links by looking for words that are **underlined** or **written in blue**.
- When you scroll over a link, your pointer changes from **the arrow to the hand**.
- When you click a link, a new **window** or **webpage** opens.

Safe or Unsafe?

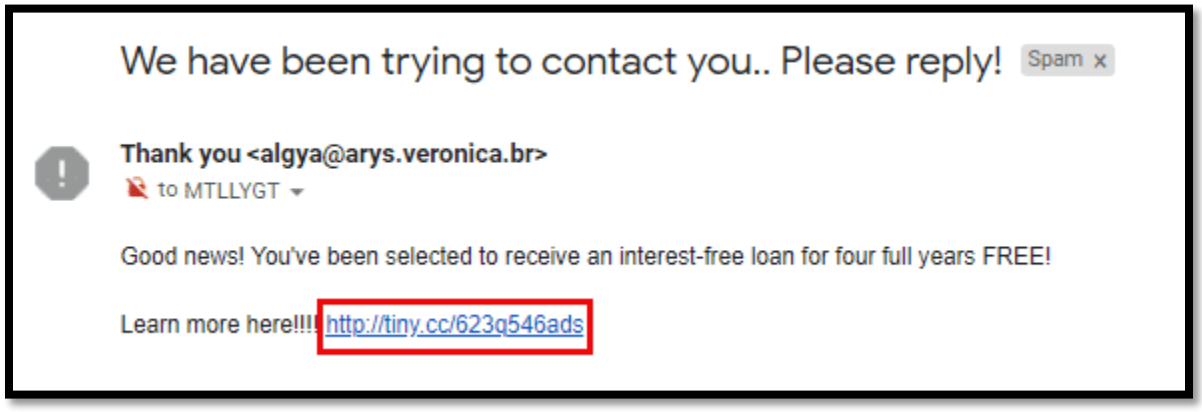
- Links on secure websites will be **safe**.
- Links in emails or texts sent to you directly by trusted friends or employers **should be safe**.
- Links in emails from email addresses you don't know **might be unsafe**:



If you clicked on that link, you would likely get a virus on your computer!

IMPORTANT: ***When in doubt, NEVER open links you are unsure of!***

Let's look for clues about viruses by looking at another email:

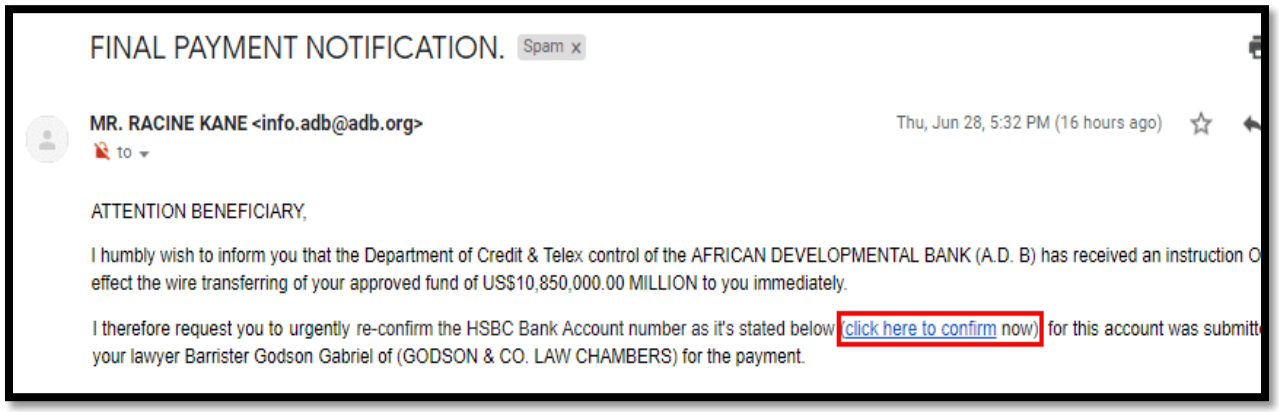


There are many clues to indicate that the link in the email is unsafe.

a. Gmail has warned that it might be **Spam** in the top right corner.
b. Gmail has attached a **stop sign** as further warning:
c. Gmail has also provided an **unlocked** warning:
d. The sender's **email address** is unfamiliar and strange.
e. The **link** (underlined in blue) is unfamiliar and strange.
f. The email is very pushy, and it's trying to get you to **hurry!!!**
g. The email promises **BIG THINGS**, so you won't stop and think.

Activity #2

Circle as many clues as you can that show that this link is **unsafe**:



6. *Managing Your Online Presence*

In the real world, we don't act **inappropriately** at work or say rude things to loved ones, but employers and family might see inappropriate things we post online. That's why it's ***so important to maintain a strong and respectful online presence.***

Here's what you need to know:

What are the risks?

If you post inappropriate messages or photos online, you might:

- Harm relationships with friends and family.
- Risk losing your job.
- Have a harder time getting a new job.

What can you do about it?

The best way to maintain a strong and respectful online presence is to:

- Remember that your profiles and posts may be **seen** by lots of different people, including **children**, **grandparents** and **employers**.

- So: **THINK** before you post.

*Keep **your content tasteful** so that all people can enjoy it, and it won't get you into trouble!*

7. Review

*Now you are familiar with many of the **risks** of using a computer, a smartphone, or social media.*

- You have learned how to **protect** your passwords and personal information.
- You have learned how to **avoid** spam and viruses.
- You have also learned how to **manage** your online presence.
- You can go back to this guide any time you want to review the information about cybersafety and protecting yourself online.

This Employment Ontario service is funded in part by the Government of Canada and the Government of Ontario.

The opinions expressed in this resource are the opinions of Community Literacy of Ontario, and do not necessarily reflect those of our funders.