Curriculum Resource

Cybersafety: Part 2

OALCF Alignment

Competency	Task Group	Level
Competency D - Use Digital Technology	**N/A**	**1**
Competency A -Find and Use Information	**A1. Read continuous text**	**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: Can be used with Cybersafety 1 or as a second installment.

Cybersafety: Part 2

What is Cybersafety?

Computers and smartphones are helpful in the modern world and they can be a lot of fun. But using then 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 this resource, you will have an introduction to:

- ✓ Protecting yourself from **PHISHING** and other scams.
- ✓ Protecting yourself from online **predators** and **identity theft**.
- ✓ Shopping safely online.
- ✓ Avoiding **cyberbullying**.

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, tablets or the internet. But it's a good idea to be **smart** and **cautious** to avoid the risks that exist.

What are the risks?

- If you give your information to the wrong people, you might become the target of **PHISHING** and identity theft.
- If you don't use wise judgment when receiving emails or texts, you could become the target of other online **scams**.

- If you use social media, you might have to deal with **cyberbullying**.
- If you're not careful about who you connect with online, you could become the target of an online **predator**.

- If you don't shop wisely, you could become the target of online **shopping scams**.

2. *Phishing*

Phishing is a term that refers to online tricks used to carry out **identity theft**. Identity theft can happen when someone **steals** enough information about you to be able to pretend to be you online, with ***many bad consequences***.

How can it happen?

The main trick of a phishing attack is a **text** or **email sent to you** requesting your personal information. *These texts or emails might ask for your:*

- Usernames
- Passwords
- Credit card numbers
- Banking information
- Social Insurance Number
- Date of Birth

What are the risks?

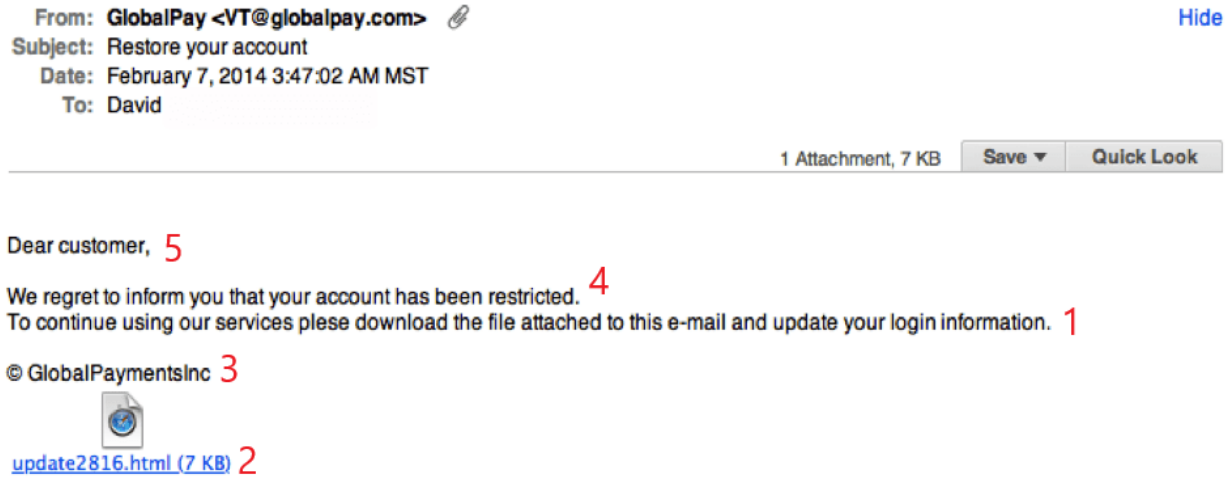
Phishing is the most common online attack. With enough information, someone could **steal your identity** and:

- Open a new **credit card in your name**, which you could be responsible for.
- Access your bank account and **steal your money**.
- Buy things using money from **your bank account or credit cards**.
- Change your passwords or other information to **lock you out** of your own accounts.

What can you do about it?

a. *WATCH OUT for phishing emails.*

Phishing emails often have certain features to watch out for. Consider this example:



1. These emails usually **ask for private information** and/or
2. Ask you to **click on a link**.
3. These emails often look **official** and seem to be from a bank, a business or a government agency.
4. These emails often use **concerning** or **urgent words** like ***"your account has been restricted"*** or HURRY or LATE or LAST CHANCE to pressure you.

5. These emails **often don't use your name** but call you something like "Valued Customer."
6. Check the sender's email. Even if they use a company name, the email address will often be obviously fake.

IMPORTANT: Don't be fooled by the official look of the emails or the pressure tactics in the message!

b. NEVER fill out sensitive information in an email.

The easiest way to avoid a phishing attack is to **NEVER send information** like your passwords, your date of birth, your banking information, or your social insurance number in an email.

IMPORTANT:

- ***Your bank will NEVER ask for information from you by email!***
- ***Your bank will always call and speak to you directly or ask you to come into a branch!***

c. **NEVER** click on suspicious links in emails, even when the email urges you to do so.

d. **REVIEW** your banking and credit card information regularly to be sure it is correct and no money is missing. *If anything seems wrong, call your bank or credit card company so that you can cancel your credit cards right away!*

Activity #1

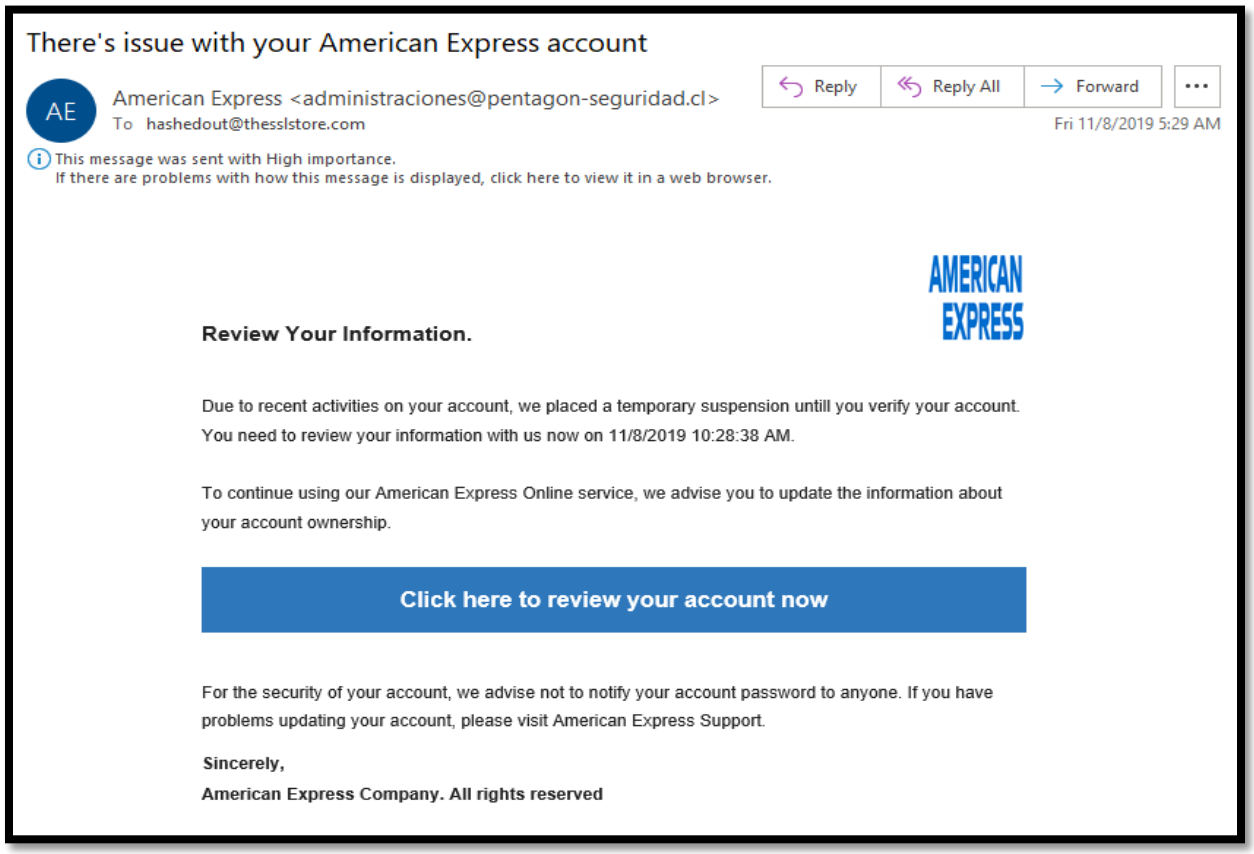
Here are three different phishing emails. For each one:

a. **Circle clues** that show it might be phishing.

b. **Explain** below why you circled each of those clues.

c. **See answers at the end of this resource.**

Phishing Email 1:



There's issue with your American Express account

AE

American Express <administraciones@pentagon-seguridad.cl>

To hashedout@thesslstore.com

Reply | Reply All | Forward | ...

Fri 11/8/2019 5:29 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

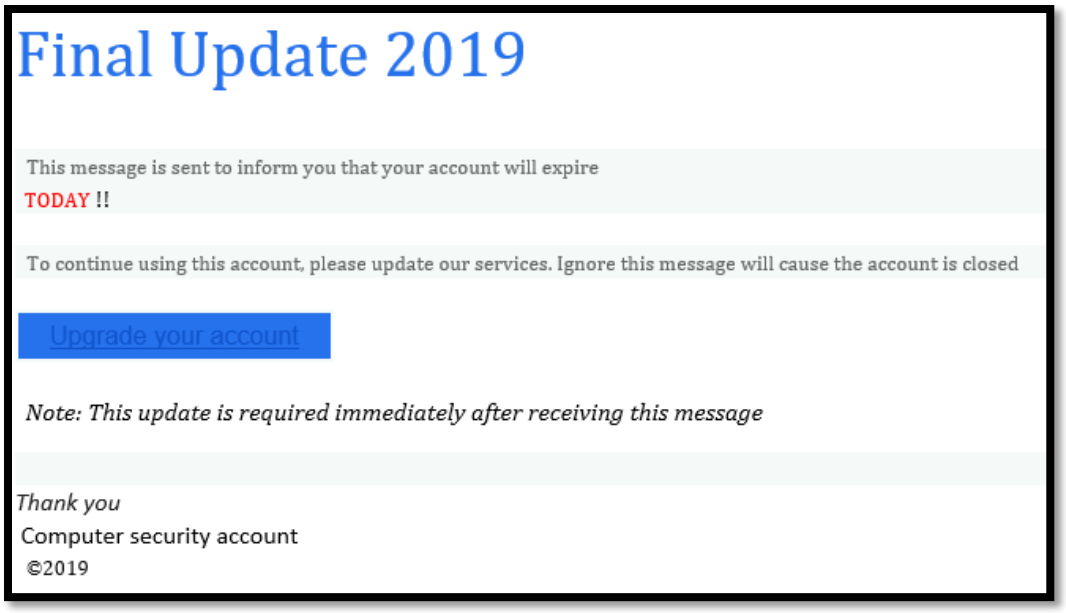
For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,

American Express Company. All rights reserved

Circle the phishing clues and explain them below:

Phishing email 2:



Final Update 2019

This message is sent to inform you that your account will expire
TODAY !!

To continue using this account, please update our services. Ignore this message will cause the account is closed

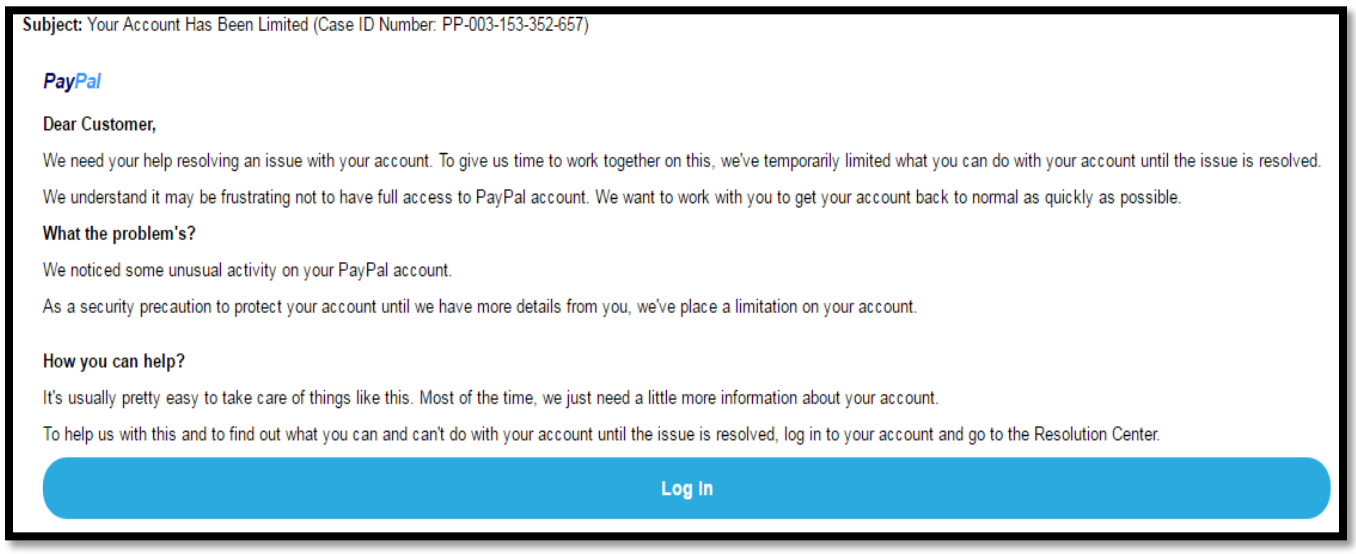
Upgrade your account

Note: This update is required immediately after receiving this message

Thank you
Computer security account
©2019

Circle clues and explain them below:

Phishing email 3:



Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Circle clues and explain them below:

3. *Other Scams*

a. Prize Scam

Sometimes scammers will try to lure you with emails that offer you a chance for **quick money** or **prizes**.

IMPORTANT:

- ***Real companies don't send prize offers by email!***
- ***NEVER click a link like this, even if it offers a prize!***

b. Pre-Approved Credit Card Scam

If money is tight, it might be tempting to get an email telling you that you are **"pre-approved"** for a credit card. Sometimes these offers ask you to **pay a fee up front** before receiving your credit card.

IMPORTANT:

- ***Real credit card companies NEVER email you a pre-approved offer.***
- ***Read credit card companies NEVER ask you to pay a fee up front.***

c. Scareware Scam

Sometimes you might get a "pop-up" on your computer warning you that your computer is infected by a **virus**. You will be directed to click a link to **download an "antivirus" program.**

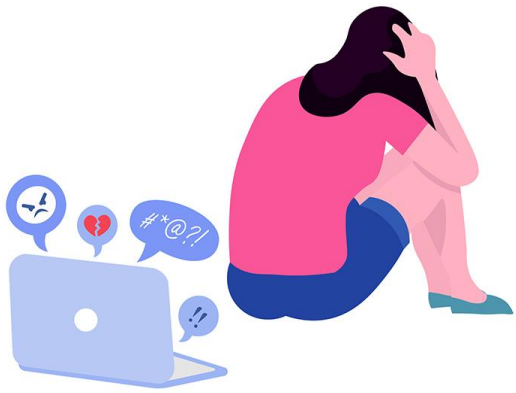
The pop-up warns that you have a virus, but it is by clicking on it that you will actually get a virus on your computer

If you click the pop-up, you may be taken to a new page that will ask for your credit card information to pay for the fake "antivirus" program. **Avoid** this situation by:

- **NEVER** clicking a pop-up like this on your computer.
- Using the **free** antivirus provided by your computer.
- Purchasing a **higher quality antivirus** directly from a reputable website like Norton Antivirus or McAffee Antivirus.

4. Cyberbullying

Just like in the real world, the Internet can be a place where **old friends gather** and **new friends meet**. But, even more so than in the real world, the Internet can be a place where people are **treated poorly**.



Cyberbullying *means treating others in mean or cruel ways online. It is most common among teenagers, but it can happen to adults too.*

What are the risks?

Cyberbullying almost always occurs through social media like Facebook, Twitter, TikTok, Snapchat and Instagram. *It can take **many forms** and have **many consequences**.*

a. Forms of Cyberbullying

Harassment

- Posting **nasty** messages about someone.
- **Bothering** someone with messages, questions or insults.
- Posting gossip or other mean information about someone to **attack their reputation**.

Exclusion

- Kicking someone out of a social media group like a group chat or a Facebook group.

Outing

- Revealing someone's private information or secrets in an online forum.
- Posting revealing or embarrassing pictures of someone online.

Cyber-stalking

- Repeated harassment of someone online.
- Pursuing someone's private information or location.

Cyberbullying can be worse than bullying in real life.

b. *Consequences of Cyberbullying*

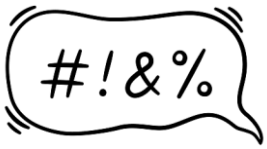
Cyberbullying can have serious consequences for its victims:

- Feelings of low self-esteem, stress and loneliness.
- Threats to the victim's job or school life.
- **Depression** and **suicidal thoughts**.
- *Posts can be **online forever** and accessible to **anyone across the world**!*

What can you do about it?

Cyberbullying can be a devastating experience, but there are ways to **prevent** it and **deal with it** if it does happen to you.

a. *Tell others what is happening to you.*
   - Don't feel like you have to go through this alone.
   - Tell friends and loved ones and **get advice**.
   - In the case of threats or hate speech, ***report the bullying to the police***.



Some types of bullying are illegal and can be punished by law.

b. *Block people who are bullying you.*

c. *Report the cyberbullying to the social media platform using their reporting tools.*

The simplest way to stop getting harassing messages is to block the person sending them.

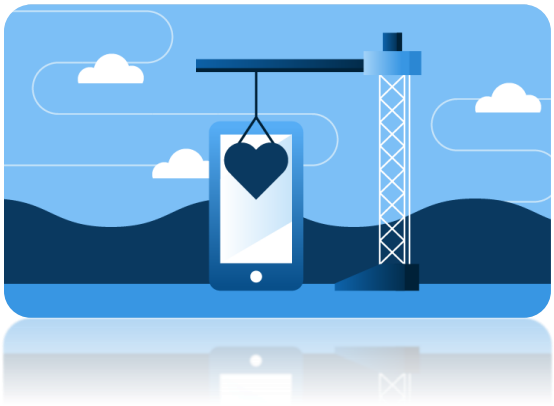
To "unfriend" someone from Facebook:

1. Type their name into the search bar at the top of Facebook.
2. Click this button  above their profile.
3. Click **Unfriend.**

To block someone from texting you:

1. Tap the texter's name or number at the top.
2. Tap the  button, scroll down a little, and then tap **"Block this Caller."**

d. Be a good social media user.



- Take a social media break from time to time.
- Be calm and polite in online exchanges.
- ***Don't be a bully yourself!***

5. Online Predators

Rarely, very bad people online want more than to steal your money or your identity. The worst online predators are **dangerous** and should be taken very seriously and avoided at all costs.

What are the risks?

Online predators always **pretend to be someone they are not**—this is known as **"CATFISHING."** They try to trick you into thinking they are someone else to **lure** you into a relationship in order to do you **harm** in some way.

IMPORTANT:

Their motives range from stealing from you to committing acts of VIOLENCE.

What can you do about it?

Avoiding online predators is all about spotting someone who is pretending to be someone else, or "catfishing."

The best ways to spot someone who is catfishing is to ask yourself these questions:

a. ***Do they agree with everything you say?***
b. ***Do they already know a lot about you?***
c. ***Are they more attractive than usual, with a photo that seems professional?***

If they are especially nice or attractive, they may be "too good to be true."

d. Do they have a very new profile with few friends?

e. Do they avoid face-to-face calls?

If they don't leave much of a trace online and won't show their face, that is a red flag.

f. Do they ask for money or explicit images?

g. Do they want to meet in person?

These are the biggest red flags of all.

IMPORTANT:

NEVER give money or images of yourself to someone you met online!

NEVER meet with someone in person unless you are 100% sure it is safe!

Even if you are sure it is safe, only meet up with someone in person in a safe location where there are other people, such as a coffee shop or even a library. Never meet someone alone!

6. *Shopping Safely Online*

Shopping online can be very convenient. You can buy things that are not available in local stores and have them shipped right to you.

But **online shopping scams** exist that can cost you a lot of **money** and **pain**, so it's important to know the risks and how to deal with them.

What are the risks?

a. *The main risk with online shopping is **paying for something that you never get**.*
b. *Or you might hand over your **credit card information** to untrustworthy people.*
c. *Someone could log into your shopping account and **buy things for themselves**.*
d. *As a seller, you might ship something and **never get paid for it**.*

What can you do about it?

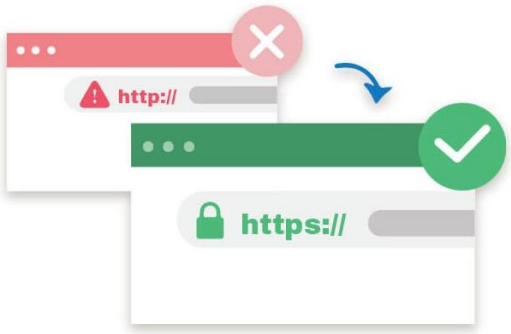
Only use trusted websites.

- Websites from trusted companies are your safest bet.
- These companies have secure websites, but you should always double check.

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

a. The Lock icon at the end of the address bar
b. The "s" in the website address

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



*Use **strong passwords** for your online shopping accounts. Don't shop on **public computers**, and if you do be sure to log off when you are finished so the next person using the computer can't access any of your information.*

- If you forget to log off, people can **buy things from your account** and change your account information.

Check your credit card statements regularly.

- If you see anything unusual or suspicious, call or visit your bank immediately and cancel your credit cards.

Read the reviews!

- It's a good idea to read the reviews of the product you plan to buy, **expecially** when you won't be able to see it and hold it until it arrives.

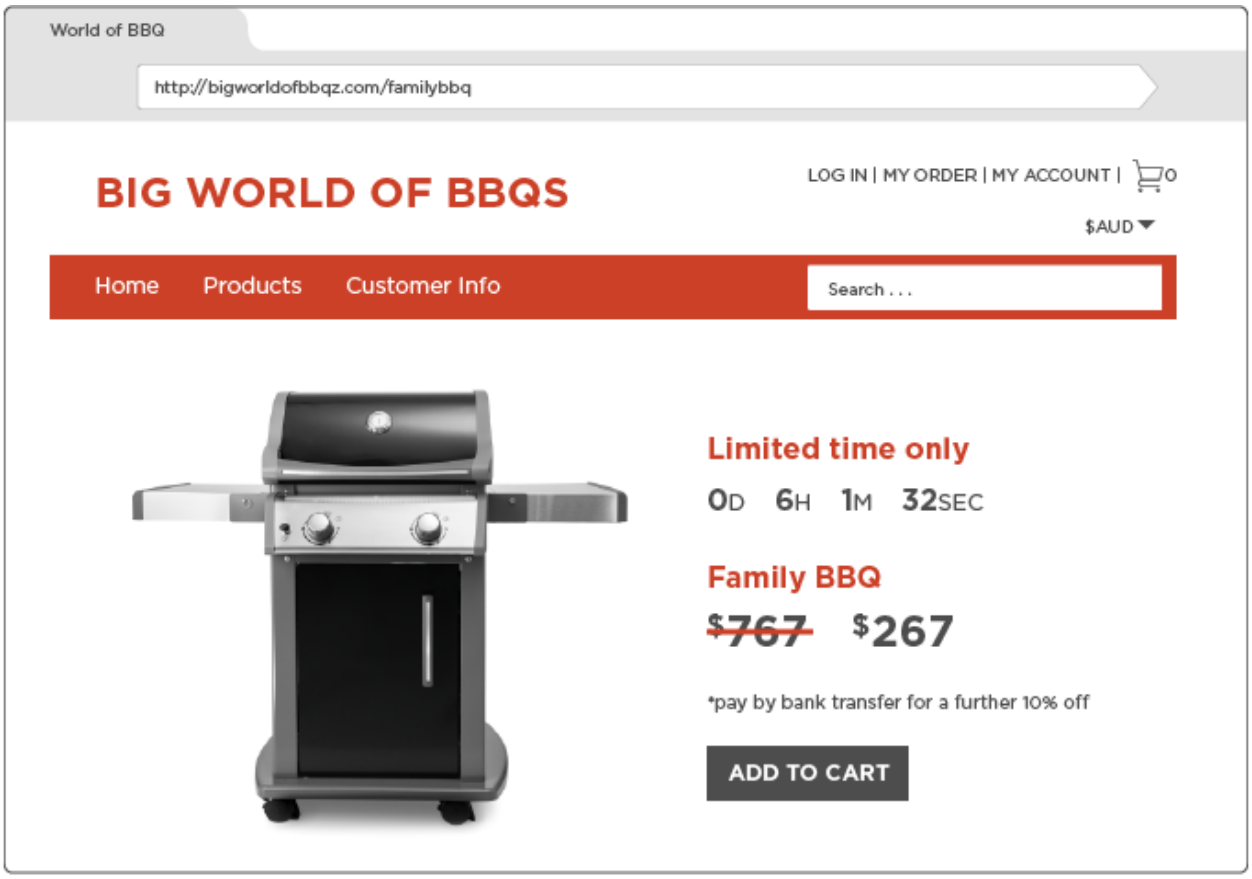
If you are buying from a second-hand seller's forum like Kijiji or Facebook Marketplace, you should always read the reviews of the sellers to see how **trustworthy** they are.

Some final red flags about online shopping

- Are you paying by a **SECURE** method like a credit card or an **UNSECURE** method like a bank transfer?
- Do you feel **rushed**?
- Does the deal seem **"too good to be true"**? *If so, it probably is!*
- *Never give out your phone number or respond to someone asking you to get a code for them. This is a common scam on Facebook Marketplace. Immediately block those accounts.*

Activity #2

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



Explain your reasons and then see below for the answers:

_____

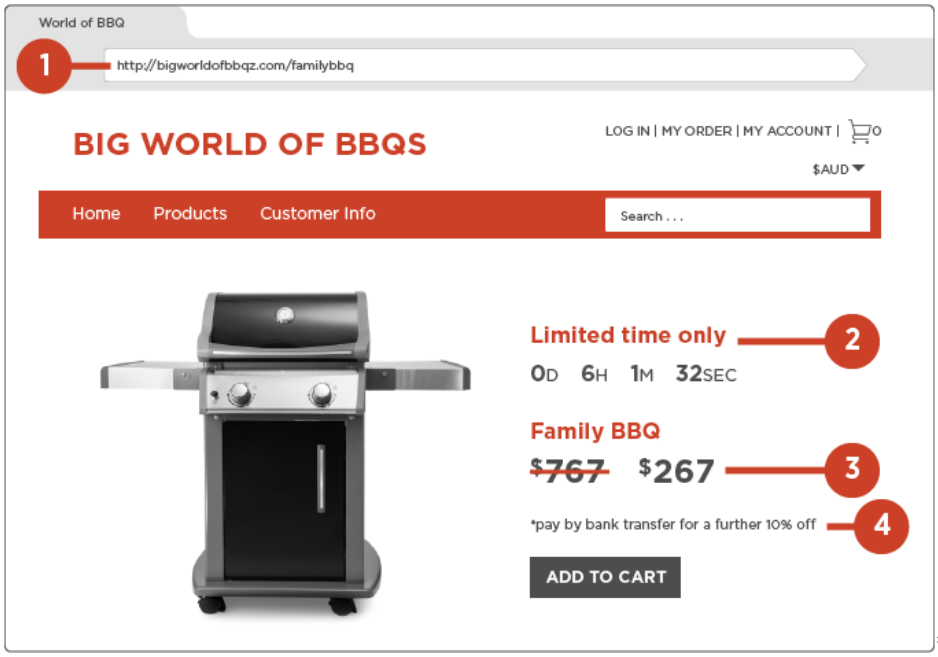
_____

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 yourself from **PHISHING** attacks and other scams.
- You have learned how to avoid and deal with **cyberbullying** and **online predators.**
- You have also learned how to **shop safely** online.
- You can go back to this guide any time you want to review the steps for using Facebook.

Answers to Activity #2



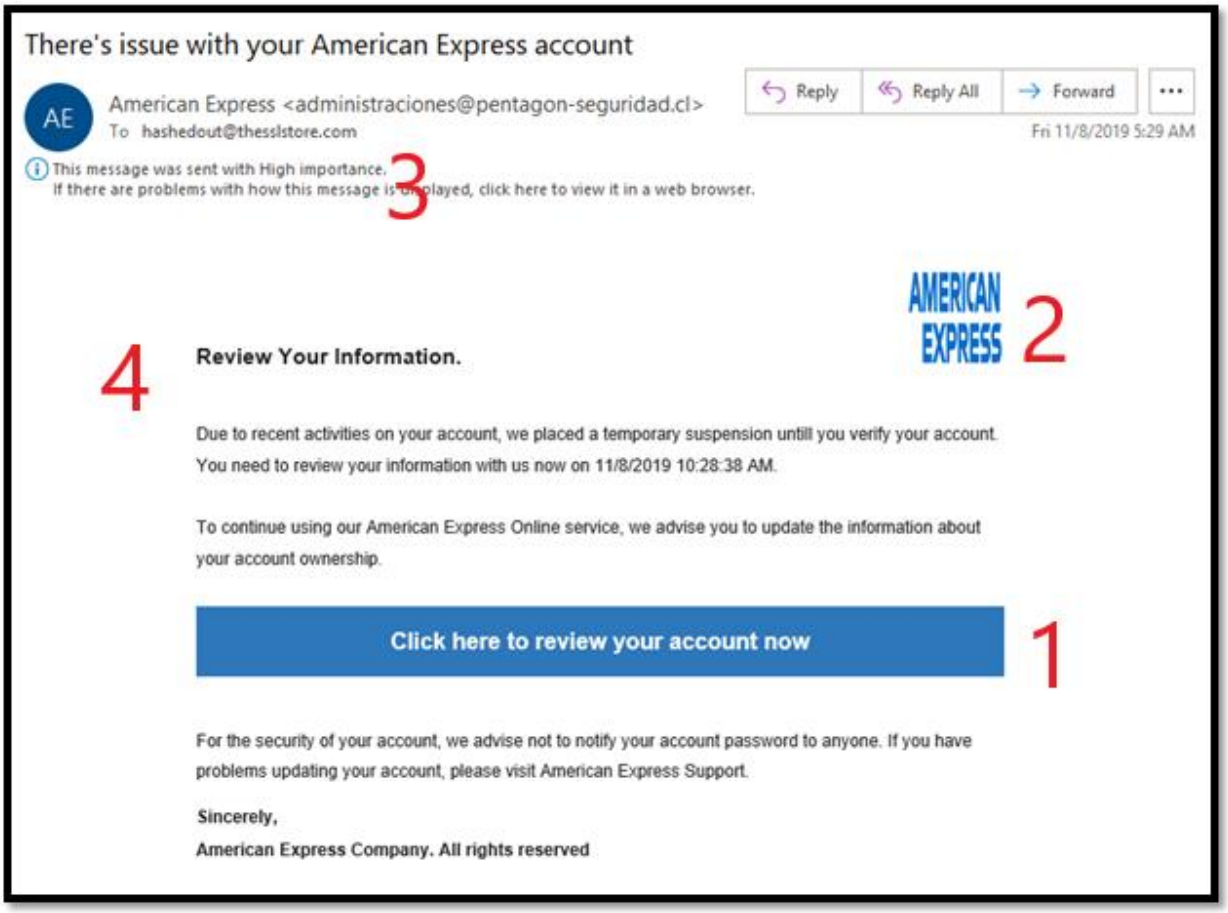
*

1. Not a secure website.
2. They are trying to rush you.
3. The deal is “too good to be true.”
4. It is not a secure payment method.

(*Activity credit: https://www.scamwatch.gov.au/about-scamwatch/tools-resources/online-resources/spot-the-scam-signs)

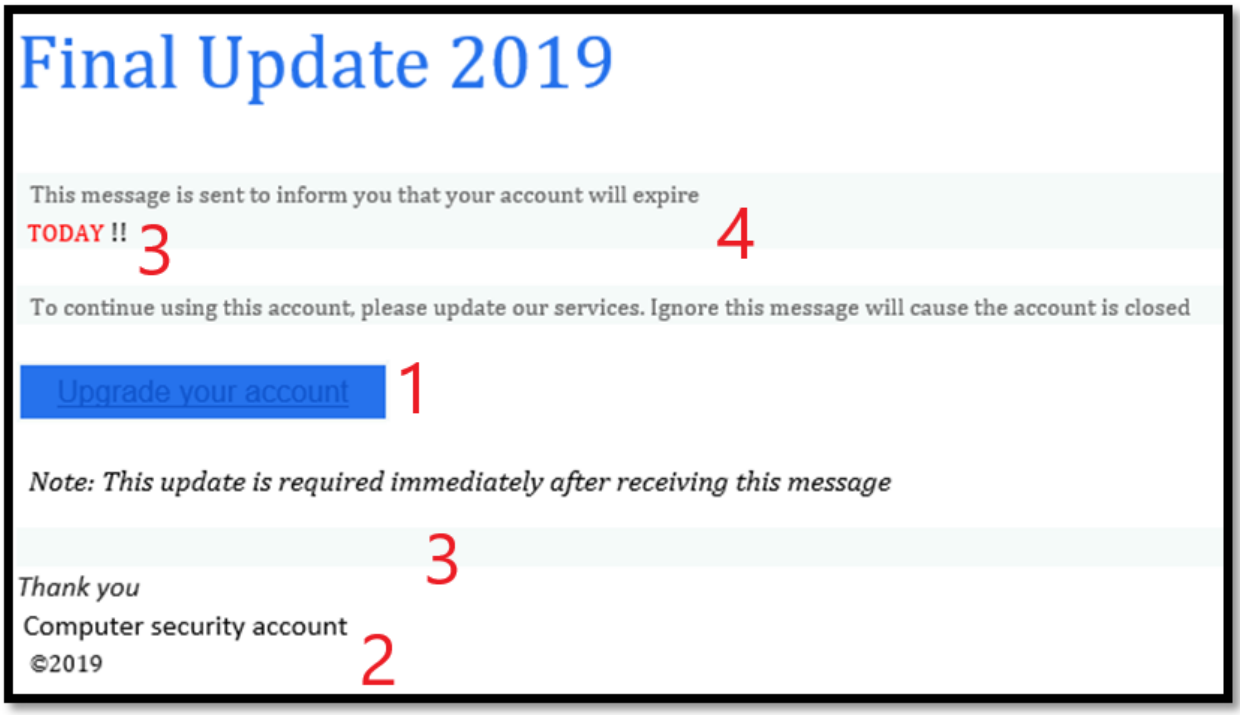
Answers to Activity #1

1.



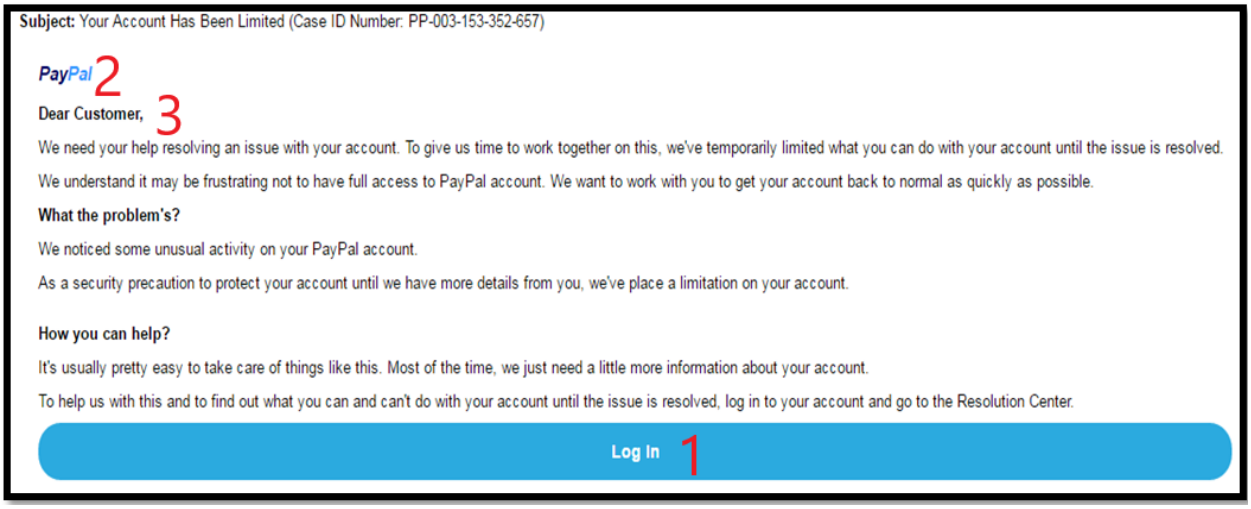
1. Asks you to click a link.
2. Looks official.
3. Uses urgent words.
4. Doesn't use your real name.

2.



1. Asks you to click a link.
2. Looks official.
3. Uses urgent words.
4. Doesn't use your real name.

3.



1. Asks you to click a link.
2. Looks official.
3. Doesn't use your real name.

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.