NORTHSTAR DIGITAL LITERACY
A program of Literacy Minnesota

Internet Basics, Lesson 8: Viruses and Email Scams

Northstar Digital Literacy Standards *This lesson aligns with the following standard/s.*	Vocabulary *This lesson focuses on the following digital literacy terms.*
6. Demonstrate understanding of when it's safe and appropriate to share personal, private, or financial information (e.g., recognizing phishing attempts, identifying unsecured websites). 7. Identify ways to protect your devices (e.g., anti-malware software, recognizing possible virus attacks).	**anti-malware/anti-virus** **download** **phishing** **suspicious** **virus**

Technology Concepts

Important lesson background and teaching tips for instructors

In this lesson, learners will practice identifying common ways their computer may get a **virus**. They will learn about **viruses** and **anti-virus** software. They will also learn how to recognize **phishing** emails.

Teaching Tips:

- It can sometimes be difficult to tell the difference between an authentic email and a **phishing** email. If an email is suspicious, going to the website directly without clicking on the links in the email is a great way to see if there is a problem with your account.
- Three example **phishing** emails are included in the references for this lesson. Consider Googling '**phishing** email examples' if you would like more examples to share with learners.

Teacher Prep Guide

Follow these steps to prepare for teaching this lesson

General Prep	❑ **Prepare to project Reference A for Model & Explain 2.**
Pair Explore	❑ **Copy Handout A for each learner (double sided).**
Vocabulary Work	❑ **Copy Handout B for each learner.**

Warm Up

Find out what learners know and prime them for the work ahead.

Pair/Small Group Work (Think-Pair-Share)**:**

- ➔ Give two minutes to <u>think</u> about questions projected on screen, then discuss in <u>pairs</u> for two minutes, and finally <u>share</u> together as a class.
    - ◆ What can you do to prevent theft?
    - ◆ The internet can be a dangerous place for theft. How do you think you can protect your information when using the internet?

We will Learn…

Sharing learner friendly objectives helps set goals for today's learning.

List objectives on board or project. Read through them together to set goals for today's learning.

We will learn to:

identify when your device could be infected with a **virus**.

identify emails that could hurt your computer or steal your information.

MODEL & EXPLAIN 1

Teacher models and explains (thinks aloud) to complete a digital literacy task while learners observe. To help learners focus on the demonstration, they should not work on their own computers at this time.

<u>Computer Viruses</u>

- ➔ Say to learners:
    - ◆ "When you use the internet or open emails, there is a danger your computer could get a **virus**. A **virus** is something that can hurt your computer."
    - ◆ "How does your computer get a **virus**? You can get a computer **virus** by going to a bad website or opening a bad email and **downloading** something. Every time you choose a song, picture, video, or file from the internet and put it on your device, you are **downloading**. Most **downloading** is good, but on a bad website, you can accidentally **download** a **virus**."
    - ◆ "A bad website is a website that wants to give your computer a **virus**. Bad websites want to give your computer a **virus** so they can steal information from your computer or so they can put ads (advertisements) on your computer."
    - ◆ "How do you prevent **viruses**? You can buy **anti-malware** or **anti-virus** software for your computer. **Anti-malware** protects your computer from **viruses**."

DO IT TOGETHER 1

Teacher asks the class to restate the steps to complete the digital literacy skill modeled. This time, the teacher prompts with questions to learners.

- ➔ Ask learners the following questions. Read each question aloud. Then, have learners turn and talk and then share out:
  - ◆ "What do you call something that can hurt your computer?" (**virus**).
  - ◆ "How does your computer get a **virus**?" (**downloading** from a bad website, opening a bad email)
  - ◆ "What software can protect your computer?" (**anti-virus/anti-malware**).

MODEL & EXPLAIN 2

Teacher models and explains (thinks aloud) to complete a digital literacy task while learners observe. To help learners focus on the demonstration, they should not work on their own computers at this time.

Suspicious Emails

- ➔ Say to learners:
  - ◆ "A common way computers get **viruses** is through **suspicious**, or bad, emails."
  - ◆ "There are two kinds of bad emails. In the first kind of bad email, you might get an email from someone pretending to be a friend, or someone you don't know, that asks you to click a link or **download** something. If you decide to download the item, you get a virus."
  - ◆ "In the second kind of bad email, you get an email that looks like its from a real website (like Netflix, Amazon, or Facebook) and it will ask you for private information like a password or credit card number. However, the email is actually from a thief, and not from Netflix or Facebook. This is called **phishing**, because the thief is fishing for your private information."
- ➔ Project example **phishing** emails on Reference A.
- ➔ Say to learners:
  - ◆ "There are some clues that can help us know when an email is **suspicious**. Here are some clues to look for:"
    - "The email doesn't have your name, only says 'dear customer'."
    - "There are spelling and grammar mistakes."
    - "The email asks you to email important information, like your password."
    - "The email is from a company you don't use."
- ➔ Say to learners:
  - ◆ "If you get a **suspicious** email don't click anything. Instead follow these steps;"
    1) "Go to the real website, like Amazon's real website."
    2) "Log-in to your account."
    3) "If there's a problem, the company will tell you in your account. If there isn't a problem, delete the email."

DO IT TOGETHER 2

Teacher asks the class to restate the steps to complete the digital literacy skill modeled. This time, the teacher prompts with questions to learners.

- ➔ Ask learners the following questions aloud. Have learners discuss in pairs first. Then, share answers as a class.
  - ◆ "What will **suspicious** emails ask for?" (credit card info, passwords, etc.)
  - ◆ "What are some clues to help you recognize a **suspicious** email?" (no name, spelling mistakes)
  - ◆ "What should you do if you get a **suspicious** email?" (do not click links, delete the email)

PAIR EXPLORE

*Teacher has modeled the skills, and skills have been practiced together. Now, allow learners time to explore these skills with a partner **without step-by-step guidance from the teacher**. *Refer to the "How to Facilitate Pair Explore" for teacher support.*

- ➔ Give Handout A to learners.
- ➔ In pairs, learners work to decide if an email is safe or unsafe.
- ➔ Answers:
  - ◆ 1 - safe
  - ◆ 2 - unsafe
  - ◆ 3 - safe
  - ◆ 4 - safe
  - ◆ 5 - unsafe
  - ◆ 6 - safe
- ➔ Some learners may think numbers 3 and 6 are unsafe. Clarify with learners, if they are ever unable to decide if an email is unsafe or safe, they should not click any links and go to the website directly.

Vocabulary Work

Learners practice vocabulary presented within the lesson.

- ➔ Give Handout B to learners.
- ➔ Learners draw lines to match the words with the definitions.
- ➔ As they finish, learners write the words and definitions into the chart.
- ➔ Check answers together as a class.
- ➔ Answers:
  - ◆ **Virus**: something that can hurt your computer
  - ◆ **Anti-malware/anti-virus:** software that protects your computer from **viruses**
  - ◆ **Download:** putting a file from the internet onto your computer
  - ◆ **Suspicious:** something that can hurt your computer
  - ◆ **Phishing** emails: bad emails that ask you for personal information

Wrap-Up

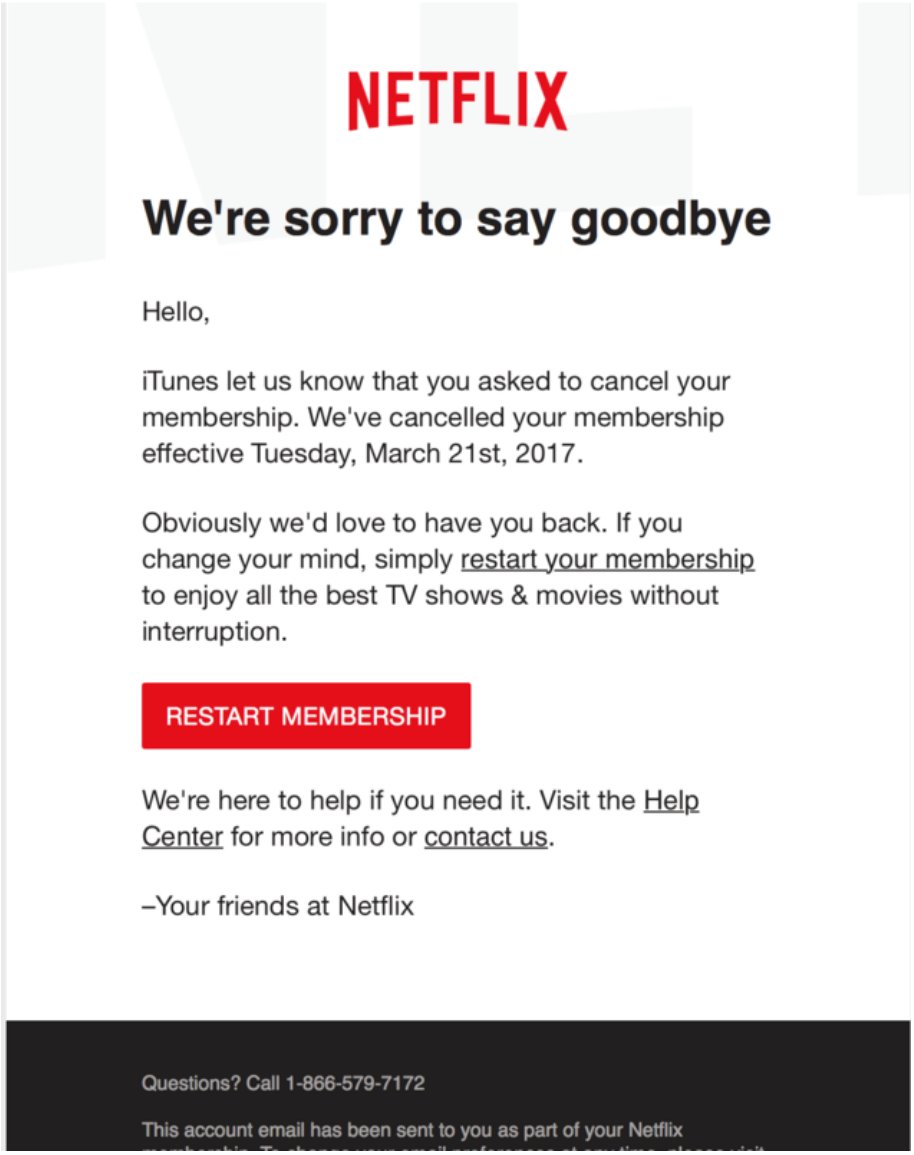
A final check in with learners. An opportunity to review, reflect, or check for understanding.

- ➔ Ask learners the following questions aloud, one at a time. Have learners turn and talk and then share out:
  - How can your computer get a **virus**? (**downloading** from bad websites, following a link in a bad email)
  - What should you do if you get a **suspicious** email? (go to the real website and check)

Reference A (page 1)

Suspicious Emails

Directions: How do you know these are phishing emails? Point out the clues.



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

Reference A (page 2)

Exclusively for: | VALUED CUSTOMER
Online Banking

Bank of America

Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please click here to continue the verification process and ensure your account security.

Email Preferences
This is a service email from Bank of America. Please note that you may receive service email in accordance with your

irs Identity Verification Service — Inbox

irs gov Today at 5:02 AM
To: @kaspersky.com
irs Identity Verification Service

IRS

Dear Tax Payer,

This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

Handout A (page 1)

Safe or Unsafe?

*Directions: Read each email and decide if it is **safe** or **unsafe.***

Email 1

From: Jose Salvador
Subject: Project meeting
Hi Ron, I was wondering - what time can we meet to discuss next week's project? I'm free Tuesday and Wednesday. -Jose
Is this email Safe or Unsafe? I think this email is _____ because _____.

Email 2

From: Facebookteam.com
Subject: URGENT Account Locked Security breach
Dear Facebook user, We have recieved Notification that someone is trying to hack youre account. Pleese reply to this email at customerservice@facebookteam.com with your username and password in order to secure your account. Thank you, Facebook
Is this email Safe or Unsafe? I think this email is _____ because _____.

Email 3

From: Amazon
Subject: Your credit card did not work
Dear Rosana, Your last order #1235345433 was not processed because your credit card was expired. Please visit amazon.com to update your credit card in order to process your order. Thank you from Amazon.com
Is this email Safe or Unsafe? I think this email is _____ because _____.

Handout A (page 2)

Email 4

From: Mohammed Hassan
Subject: Class cancelled today
Hello class, Today's class will be cancelled due to bad weather. I hope you all stay safe today! Thanks, Mohammed
Is this email Safe or Unsafe? I think this email is _____ because _____.

Email 5

From: US Bank
Subject: Your Accounts has been locked!
An error was detected in your informations so your account has been temporarily locked for your security. We need you to update your informations such as credit card info immediately. Please click below to update your informations.
Is this email Safe or Unsafe? I think this email is _____ because _____.

Email 6

From: FirstBank Credit Card
Subject: Your statement is available
Dear Sam, This is an email to let you know that your latest bank statement is available. A copy can be downloaded if you visit our website at firstbankcredit.com. Sincerely, FirstBank Team
Is this email Safe or Unsafe? I think this email is _____ because _____.

Handout B

Computer Viruses

Directions: Draw a line to connect the words with the correct definitions. Then, copy the words and definitions into the chart below.

Virus	Something that seems bad, something that might be bad
Anti-malware/ anti-virus	Putting a file from the internet into your computer
Download	Something that can hurt your computer
Suspicious	Bad emails that ask you for personal information
Phishing emails	Software that protects your computer from viruses

Word	Definition