Secure Connections!

Mini-Unit Overview (Remote Optional)

The purpose of this mini-unit is to introduce students to basic cybersecurity, and more specifically how they can stay safe online.

Lesson 1: Cybersecurity - Students will be able to identify unsafe websites and phishing text messages. (NI-02)

Lesson 2: Powerful Passwords - Students will be able to define what a password is, understand why passwords are important, and create strong passwords. (NI-02)

Cybersecurity

Secure Connections: Lesson 1

Lesson Overview

Introduction
5 minutes

Staying Safe Online
10 minutes

Hack Attack! Activity
10 minutes

Reflection
5 minutes

Standards

NI-02 Explore digital footprint and data

Materials

1 Images in Resources

Introduction

Today is the first of 2 lessons focussed on cybersecurity. Before discussing cybersecurity, students need to know what “data” is. Have students volunteer to say what they think data is. After calling on a couple students to give their answers, you can describe data as just being information, and particularly for our purposes in the next few lessons, we can think of data as being information that is stored online or on a device.

Have students give some examples of data. If they are struggling, you can give examples such as photos on a phone or a website, the directions to get somewhere, and someone’s information on their Facebook profile (ie name).

Staying Safe Online

Ask the class if anyone has heard of a hacker or hacking before. We care about our data being online because hackers could steal our data!

One way hackers can steal people's data is by using viruses. You can explain a computer virus as being very similar to a stomach virus or the flu, where the virus spreads between people, or in this case, computers! We're going to look at how hackers are able to "infect" us with the virus.

Display the Dangerous Website image (resources). Tell students that you have visited a website that you saw after doing a Google search, and that you see the following pop-ups on the site. Ask students what they think you should or should not click on, and why. After, explain that pop-ups like these are common across several sites and that we should never click on any of them! These are tactics used by hackers to trick us into either giving them some of our information or downloading a virus onto our computer.

Now display the Website Warning image (resources). Tell students you got this warning from your browser while trying to visit a different website. Explain that "malware" is basically another word for "virus." Ask students if you should visit the website anyways, click the "Back to Safety" button, or close the tab.

After having some students answer, say that we should always just close the tab when we see a message like this. The reason is that while often it will be our browser giving us this warning, meaning it is safe to click the "Back to Safety" button, other times, a dangerous website like in the first example will display a pop-up like this to trick us into clicking the button and downloading a virus!

Phishing Attacks

These were examples of things to be aware of while on the internet. However, another common tactic used by hackers is something called a phishing attack! Ask a student to describe fishing (with an f). They will likely describe how when fishing, you put bait on the end of your fishing rod, put it into the water, and then wait for a fish to come bite the bait.

This is the idea behind phishing attacks, and hence why they have similar names! In a phishing attack, a hacker will send many people (the fish) an email or text message with a dangerous link in it (the bait) and wait for someone to click the link! These links can download viruses, but more often, they are designed to trick the user into giving away personal information.

We are going to look at 4 text messages (text1, text2, text3, and text4 in resources), and students are going to vote on whether we should click the links and also describe why or why not.

After going through all of the texts, you should reveal that they were all phishing texts except for text3 (Verizon). It can be really hard to tell what is phishing and what's not! Go through the texts again and point out that the Verizon text message was the only one with a legitimate link. All of the others appear to have been generated somehow. When in doubt, students should always google the number they received the message from to see if it is legitimate and pay close attention to the link.

Reflection

- Have you ever seen any ads, pop-ups, or texts like the ones we showed in class today? Did you click on them? Would you click on them if you saw them again?

Powerful Passwords

Secure Connections: Lesson 2

Lesson Overview

Introduction
5 minutes

Powerful Passwords Worksheet
15-20 minutes

Making Powerful Passwords
10 minutes

Reflection
5 minutes

Standards

NI-02 Explore digital footprint and data

Materials

1. Comb. Lock (opt.)
2. Worksheet (prvd.)
3. Paper

Introduction

Today, we will be focusing on passwords. We'll begin by comparing passwords to locks. Ask the students if they know what a combination lock is and if someone can explain it. (A picture or an actual lock here may be useful if possible) A basic explanation is that a combination lock only opens after you have turned all the dials to the correct numbers. Ask students what things you would use a combination lock for (ie bicycle, locker).

Ask students if someone can define a password. A good definition is that a password is a secret word/phrase/combination of letters and numbers that is used to protect your information online. They are used for signing in to some websites (like Facebook) if you want to visit them.

Explain to students that online passwords are similar to the combinations for a lock. They are secret combinations of letters and numbers that only you know. Passwords keep other people from seeing your private information on the Internet. For example, tell students that passwords allow them to save their points after playing an online game. When they're older, they will use passwords to do many things, such as keep track of their money or shop online.

Explain that knowing how to create powerful passwords will prevent other people from pretending to be them and help them keep their private information and money secure. Passwords protect one's identity and information.

Powerful Passwords Worksheet

Have students complete Powerful Passwords Dos and Don'ts Worksheet.

After completion of the worksheet, review the answers with the students, having an explanation for each:

DO make passwords eight or more characters long. (Longer passwords are harder to crack than shorter ones.)

DON'T use dictionary words as your password. (Others could guess your password this way - easier to guess if you use dictionary words -- better to use made up words.)

DO include letters, numbers, and symbols in your password. (It can be harder to guess passwords with this combination of different characters.)

DO change your password at least every six months. (This way, even if someone does guess your password, they won't be able to get into your account for long.)

DON'T use private identity information in your password. (Others could guess your password this way.)

DON'T use your phone number as your password. (Others could guess your password this way.)

DON'T use your nickname as your password. (It could be easy for others to guess.)

DO give your password to your parent or guardian. (They will help you remember it if you forget it.)

Powerful Passwords Worksheet (cont.)

DON'T share your password with your friends. (Even if you trust them, they might unintentionally do something that puts you or your information at risk.)

DO create a password that you can remember. (It's okay to create a random password, but keep in mind that it should be one that you can remember, or else it won't do you much good.)

Ask the students which of the DOs and DONTs surprised them.

Remind students that they should not carry their passwords with them, or share them with friends, but they should remember them. It is also wise for students to let trusted family members know about their passwords. They can help students find a safe place to store their written passwords.

Create a Powerful Password

Tell students that you will now practice creating a new, secure password.

Have each student gather 4 strips of paper. Instruct students to write down an answer for each of the following categories, one per strip of paper:

- Favorite number
- Pet's name, or favorite character's name
- A symbol (#, $, %, *, or &)
- Favorite food

Have students arrange the four strips in various combinations to create a new password, keeping in mind the DOs and DON'Ts tips they discussed earlier. For a challenge, students can split words apart to create more options for combinations, or come up with new questions for words to use.

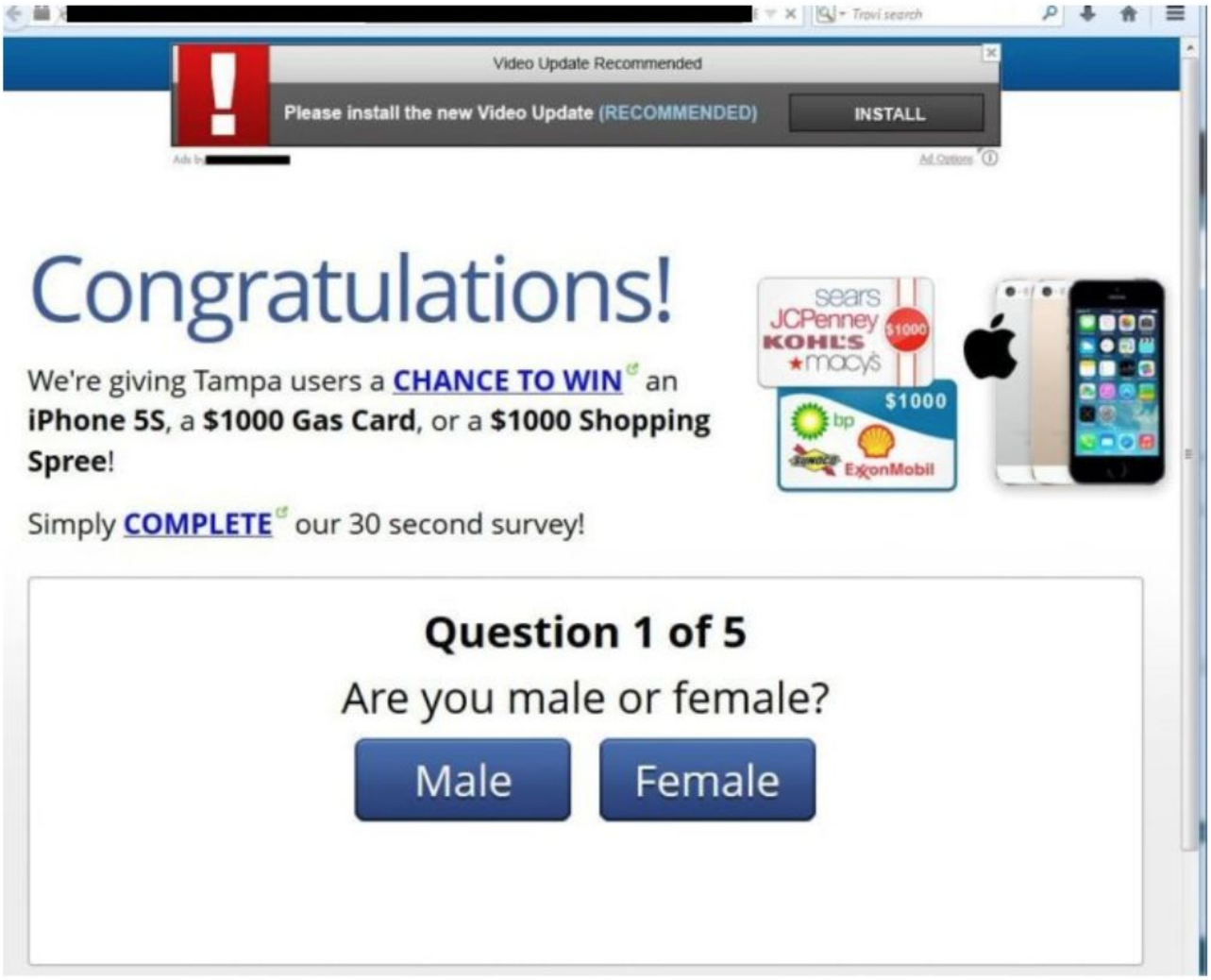
Invite 3 students to share their passwords with the class, and discuss what they think makes them so strong.

Reflection

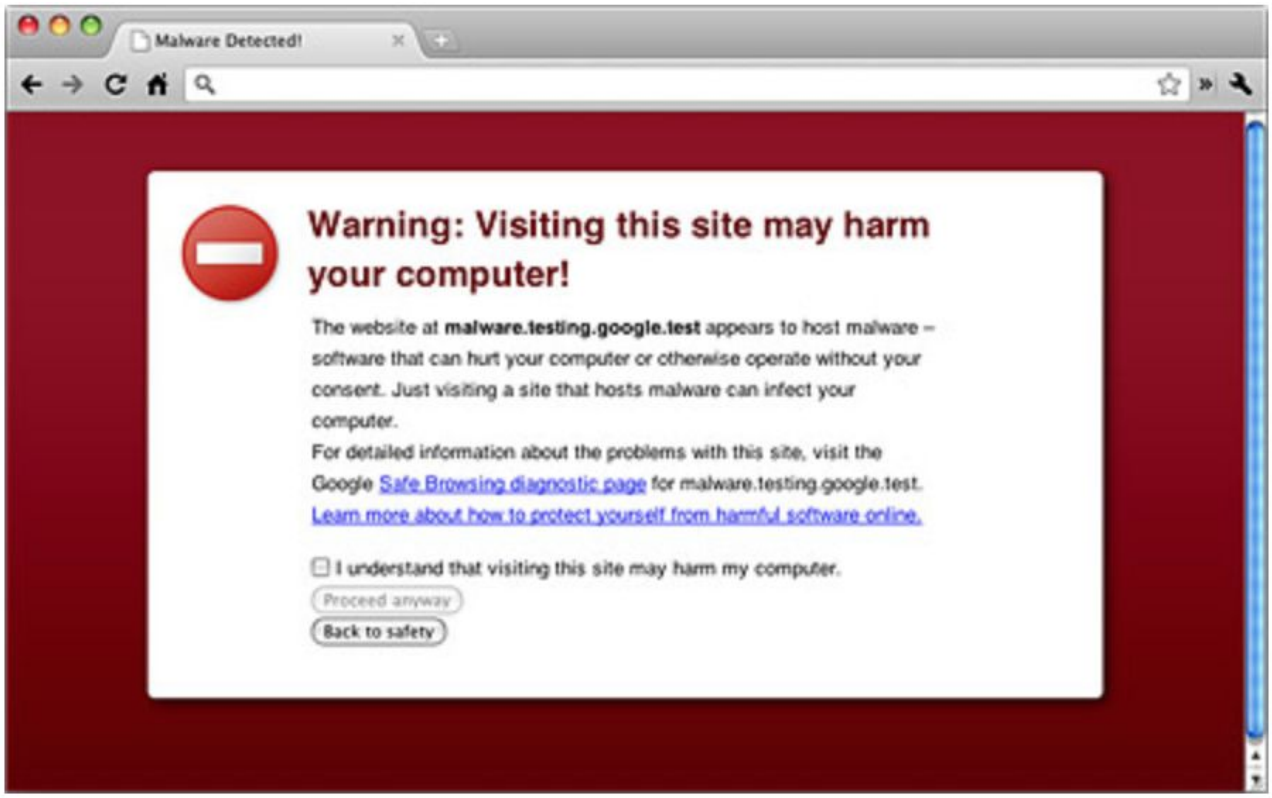
Ask the Students:

- What is a password?
- Why are strong passwords helpful?
- What are some Do's and Don'ts to remember about powerful passwords?

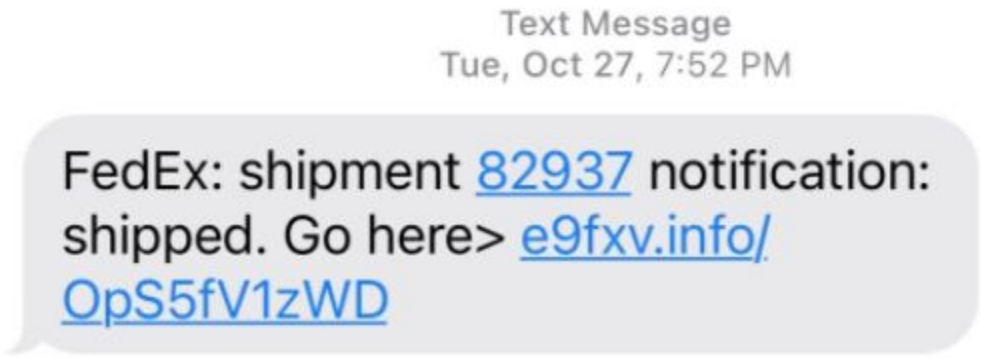
Resources



Dangerous Website



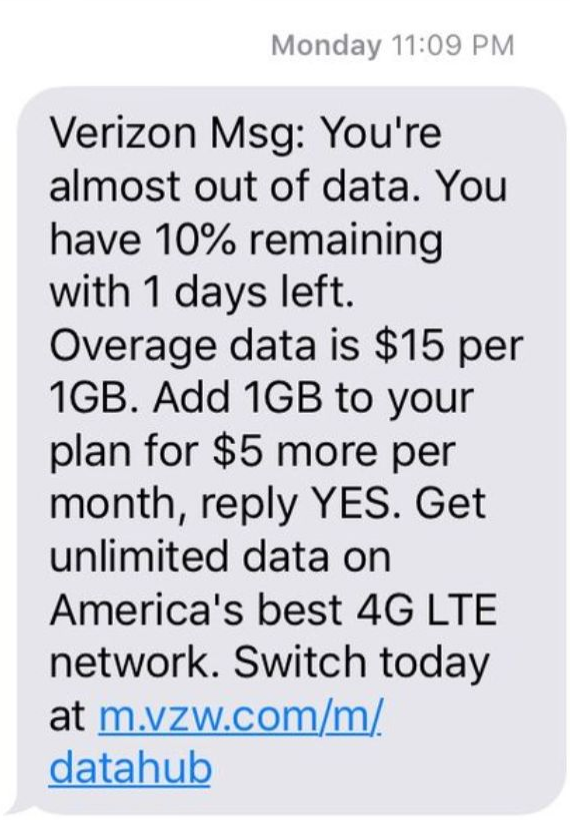
Website Warning


Text Message
Tue, Oct 27, 7:52 PM
FedEx: shipment 82937 notification: shipped. Go here> e9fxv.info/OpS5fV1zWD

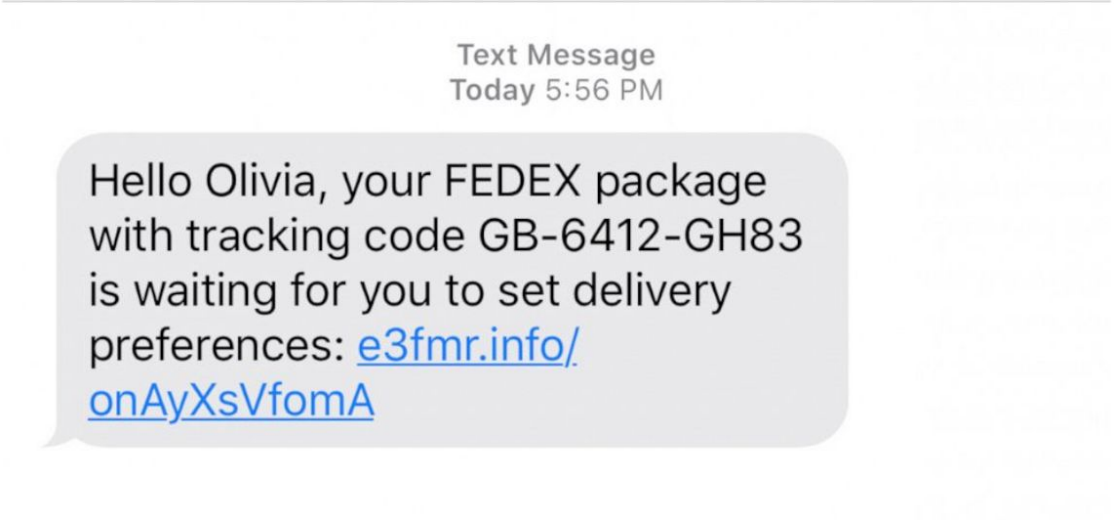
Text 1


Text Message
Today 01:15
Dear Customer,
Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.
Apple smsSTOPto43420

Text 2


Monday 11:09 PM
Verizon Msg: You're almost out of data. You have 10% remaining with 1 days left. Overage data is $15 per 1GB. Add 1GB to your plan for $5 more per month, reply YES. Get unlimited data on America's best 4G LTE network. Switch today at m.vzw.com/m/datahub

Text 3


Text Message
Today 5:56 PM
Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsVfomA

Text 4

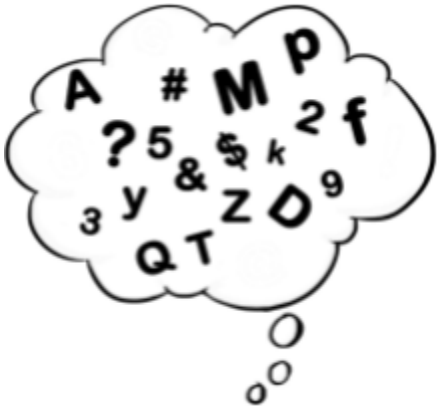
Name(s)_____ Period _____ Date _____

WORKSHEET

Powerful Passwords

Directions

Do you know how to make a powerful password? Write the word DO or DON'T into each of the statements below to show how to make the best passwords.



1. _____ make passwords eight or more characters long.
2. _____ use dictionary words as your password.
3. _____ include letters, numbers, and symbols in your password.
4. _____ change your password at least every six months.
5. _____ use private identity information in your password.
6. _____ use your phone number as your password.
7. _____ use your nickname as your password.
8. _____ give your password to your parent or guardian.
9. _____ share your password with your friends.
10. _____ create a password that you can remember.

Use Common Sense!

It's okay to write down passwords, but …

- Remember not to carry them with you
- Don't tape them on your computer
- Ask a parent or caregiver to help you find a safe place at home to keep them