Lesson 3.2: What is Smishing?

Objectives

In this lesson, students will:

- ❖ Gain an understanding of cybercrime
- ❖ Learn what Smishing is, how to recognize it and how to avoid it

Agenda

1. What is Smishing?	10 mins
2. Student Activity: Josh Got “Smished”	20 mins
3. Student Activity Solution Discussion: Josh Got “Smished”	15 mins
4. Wrap Up and Reflections	5 mins

Preparation

- ❏ Projector for class demonstration and discussion
- ❏ Print student activity worksheet student team.

Resources & Links

- ❏ Reference Video on Cybersecurity and Crime: https://tinyurl.com/yawtjhjh
- ❏ Reference Article: “What is smishing and how can it be avoided?” https://tinyurl.com/y4rtwxbu

1. What is Smishing?

Smishing is basically a scam that can lead to a security attack on your mobile device through a text message. If you fall for the scam, a virus or other malware could be downloaded onto your mobile device or they will trick you into giving out private information.

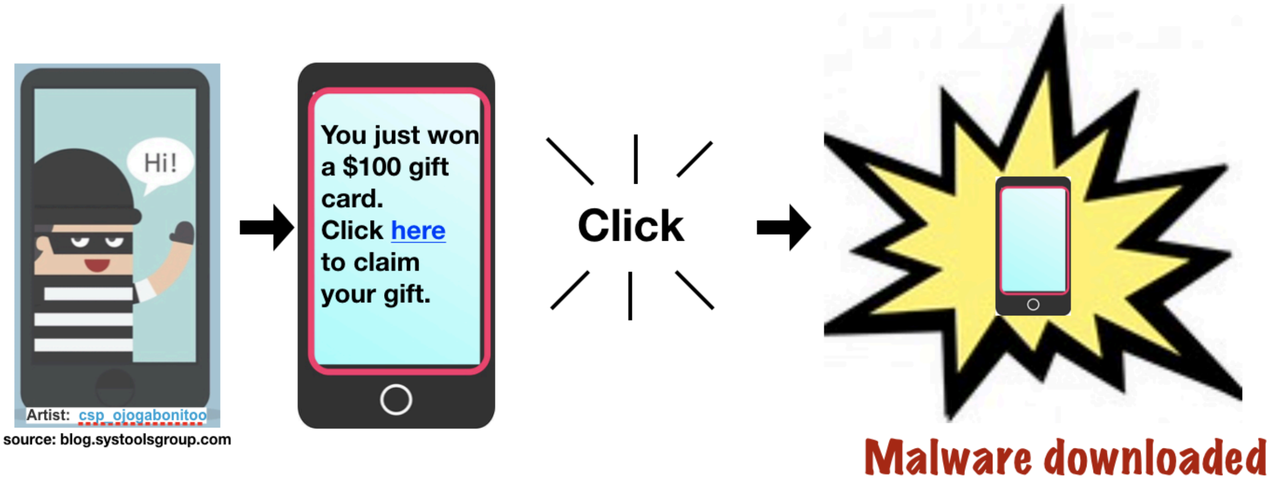
Let’s make sure we understand some of this cyber talk.

What is a scam? A scam is an attempt to trick someone.

What is malware? Malware, short for malicious software, is a kind of software that can be installed on a computer without approval from the computer's owner.

Kinds: viruses, worms, trojan horses, adware and spyware

Here is how a smishing scam might occur:



You just won a $100 gift card. Click here to claim your gift.

source: blog.systoolsgroup.com

A cyber criminal sends you a text to trick you into clicking on it. You click on it and now your phone is infected with some type of malware.

The possible consequences are:

❑ Adware pop-ups

❑ Faster battery drain

❑ Unfamiliar apps

❑ Apps start crashing

❑ More data usage

❑ Information stolen

2. Student Activity: Josh Got “Smished” (not an actual word)

In this activity students are presented with a story and prompted to engage in a set of reflections and questions about it.

Explain the activity and read the following story aloud to the class:

Josh is an avid gamer. He especially likes Doom, Sonic The Hedgehog, and Minecraft. He receives the following text message:

> **“We have large selection**
> **of games free, plus enter to**
> **win a free game today!**
> **Click here to check out**
> **these games you love!”.**

“Cool”, he shouts. Josh clicks on the link. Next thing you know this ad pops up advertising pimple cream. “I don’t even have pimples” he thinks. He tries to close the ad and another pops up advertising breath freshener. Every time he tries to close the ad, another pops up and he can’t seem to gain control of his phone !

Distribute the activity worksheet. It is recommended that students work in teams of 2-3 for this activity.

3. Student Activity Solution Discussion: Josh Got “Smished”

When students have completed the activity, engage them in a class discussion of the activity questions and answers.

Question	**Answers/Discussion Points**
What could Josh have done differently to avoid what happened?	Not click on the link. Deleted the text right away. Ask an adult what to do.

What are some things in the text message that could have alerted Josh that it was a scam?	Too good to be true. The english is a little odd, for example, it should be “we have a large selection of free games” and ‘check’ is misspelled. A legitimate business would typically have no typos and missing words. **Here are some other ways you might tell a message is a scam:** 1. Need to verify account information 2. Sense of urgency 3. Spelling errors 4. Alert that your account is in trouble 5. Link in attachment or email 6. Too good to be true 7. Generic greeting
What happened to his phone when he clicked on the link?	Malware was apparently downloaded onto his phone in the form of **adware**.
What are other things that could have happened by clicking on that link?	Other malware like a virus or spyware could have been downloaded infecting his phone and personal information could be stolen.
Who came up with their own smishing text message? Prompt students to share their text message.	Students share their text message

2. Wrap Up and Reflections

Hackers are attacking smartphones more and more through text messages. So it’s a good idea to know what we can do to protect ourselves and not be tricked into some scam. Here are some other things you can do to avoid a smishing scam:

1. Avoid clicking on any links in unknown messages.
2. Don’t respond to text messages that ask you about your personal or private information.
3. Do not call back the number that is associated with an unknown text message sender
4. If the message says ” Dear user, congratulations, you have won….” It is a sign that it is Smishing. If it is too good to be true, it usually is !

5. Overall, it's good practice to only text with people you know or know about.

Reflection Points:

- What did you learn today?
- What is "smishing"?
- What are ways you can avoid a smishing scam?

Student Activity: Josh Got "Smished"

Read the story aloud with your team:

Josh is an avid gamer. He especially likes Doom, Sonic The Hedgehog, and Minecraft. He receives the following text message:

> "We have large selection
> of games free, plus enter to
> win a free game today!
> Click here to check out
> these games you love!".

"Cool", he shouts. Josh clicks on the link. Next thing you know this ad pops up advertising pimple cream. "I don't even have pimples" he thinks. He tries to close the ad and another pops up advertising breath freshener. Every time he tries to close the ad, another pops up and he can't seem to gain control of his phone !

Answer the questions below.

1) What could Josh have done differently to avoid what happened?

____

____

2) What are some things in the text message that could have alerted Josh that it was a scam?

____

____

3) What happened to his phone when he clicked on the link?

____

____

4) What are other things that could have happened by clicking on that link?

____

____

____

5) Can you come up with a smishing scam text message? Give it a try and write one.

____

____

____

____