Tempting Offers

EXERCISE-IN-A-BOX LESSON PLAN (13-15 years old)

OVERVIEW

This lesson teaches students about curiosity baiting, tempting offers, and scarcity in relation to phishing and scams, helping them recognise and avoid these cybercriminal tactics. By promoting critical thinking and healthy scepticism, students will be better equipped to protect themselves, their families, and their personal information.

LEARNING OBJECTIVES

Students will be able to:

• Identify and describe the concept of curiosity baiting in relation to phishing and scams, and demonstrate how to avoid clicking on links or opening attachments in suspicious emails that use this tactic.

• Recognize and explain how tempting or "too good to be true" offers are used to lure individuals into phishing and scamming attempts.

• Explain the concept of scarcity in relation to phishing and scams, and describe how to avoid making rash decisions in response to limited-time offers or urgent messages.

DURATION

60 minutes

KEYWORDS

• **Curiosity Baiting**: This is when scammers use something interesting or mysterious to grab your attention and get you to click on a link or download a file.

• **Tempting Offer**: Also known as "Too Good to be True" offers. Scammers might make you an offer that sounds too good to be true in order to trick you into giving them your personal information or money.

• **Scarcity**: Scammers might use the idea of scarcity to make you feel like you need to act fast in order to get a good deal or avoid missing out on something important.

INTERNET INDEPENDENT FRAMEWORK

The learning objectives in this workshop are aligned with the **Phishing & Scams** pillar of the Internet Independent Framework. Visit cyberlite.org for more information.

© Cyberlite Books Pte. Ltd. All Rights Reserved.

Tempting Offers

EXERCISE-IN-A-BOX LESSON PLAN (13-15 years old)

WARM-UP
5 MINUTES

Slide 1

Say: Today, we will be learning about phishing and scams. Cyberspace is filled with millions of users, which means there are good people and bad actors that share the internet with us. We need to learn to identify red flags when a bad actor is in our space.

Slide 2

Ask: Do you know what phishing means? Why do cybercriminals and bad actors do it?
Phishing is a type of cyberattack. It is where bad actors and cybercriminals create fake websites or messages intended to trick people into giving away their personal information, like passwords or credit card numbers. They are generally motivated by financial gains.

Slide 3

Ask: Do you know any examples of online scams?
The common types of online scams students this age will have come in contact with are in games and social media. In games, a common scam is tricking the player into giving away information in exchange for "free" in-game upgrades. A common scam seen on social media is the free gift scam where scammers offer free gifts or giveaways in exchange for personal information or payment.

DEFINE THE KEYWORDS
15 MINUTES

Slide 4

Ask: **Does anyone know what curiosity baiting, tempting offers, and scarcity tactics are?**
Allow students to guess or extrapolate meanings. Guide them to think about it in the lesson's context of phishing and scams.

Slide 5

Read the contents of the slide aloud.

Discuss: **What have you seen online that has piqued your curiosity?**
Have students fallen for clickbait before, where they couldn't resist clicking on a video or article that had a sensational headline? Encourage students to share their experiences and what kinds of content will pique their curiosity.

© Cyberlite Books Pte. Ltd. All Rights Reserved.

Slide 6

Read the contents of the slide aloud.

Discuss: Why do you think people fall for tempting offers?
Tempting offers are exactly that - tempting! They play on a person's greed and curiosity, no matter how unbelievable it sounds. A good way to teach critical thinking in the classroom is to ask your students how many of them have received a lot of money just by walking down the street. If people won't give you free money in real life, then ask yourself why anyone would give you free money or products online? What do they want in return?

Slide 7

Read the contents of the slide aloud.

Discuss: Have you ever done anything impulsively without thinking, then regretted it after?
Students might share that they have bought something and regretted the purchase, or agreed to do something only to regret it later. The scarcity tactic plays on a person's impulsivity as it encourages the individual to act fast without thinking it through.

INVESTIGATE THE SCENARIO
30 MINUTES

Slide 8

Say: In this next section, we will explore a few pieces of evidence illustrating the different tactics used in phishing and scams. Remember to keep the keywords we've just learned in mind.

Slide 9

Investigate this social media message.

Ask: Which tactic(s) has the scammer used here?

Identify all the clues that tell you this is a phishing scam.
The answers are on the next slide.

Slide 10

Discuss the following questions:

1. Which tactic has the scammer used here?
This is an example of curiosity baiting, where the scammer has sparked curiosity by tempting you with a chance to see who's been on your profile. By clicking the link, it takes you to a fake website that's designed to look like the real one.

2. What's the motivation behind this phishing scam?
When you click on the phishing link, you're prompted to type in your real username and password to their fake website. Once the scammer gets a hold of

© Cyberlite Books Pte. Ltd. All Rights Reserved.

your login credentials, they will be able to change your password and take over your social media account.

3. What red flags should we look out for?
1. Unknown sender. This message was sent by an unknown sender who you are not following. Don't click on any links for people you don't know.

2. HTTP, not HTTPS. Always make sure any link you click starts with "HTTPS".

3. Fake website and wrong URL. You should never enter your login credentials into websites or apps that's not the official ones.

Slide 11

Investigate this online marketplace website.

Ask: Which tactic(s) has the scammer used here?

Identify all the clues that tell you this is a phishing scam.
The answers are on the next slide.

Slide 12

Discuss the following questions:

1. Which tactic has the scammer used here?
The scammer is using the tactic of scarcity to create a sense of urgency in Justin and Arianna by claiming that there are only two tickets left for a popular music festival. This is also a tempting offer that may pressure buyers to act quickly without considering if the offer is legitimate.

2. What's the motivation behind this phishing scam?
Scarcity and tempting offers are powerful triggers that can make people feel like they might miss out on something if they don't act fast. When buyers act fast, they might not stop to think if the seller is legitimate or not.

3. What red flags should we look out for?
1. Sold on an online marketplace. Sites like this allow anyone from anywhere to sell their things, which makes it difficult to verify if the seller is legitimate.

2. Persuasive language. This enhances the idea of scarcity and creates a sense of urgency.

3. No ratings. It's a good idea to only make purchases with sellers who have high ratings on these platforms.

4. No negotiations or refunds. The seller wants you to make the purchase as quickly as possible without thinking.

Slide 13

Investigate this gamer's message.

© Cyberlite Books Pte. Ltd. All Rights Reserved.

Ask: Which tactic(s) has the scammer used here?

Identify all the clues that tell you this is a phishing scam.
The answers are on the next slide.

Slide 14

Discuss the following questions:

1. Which tactic has the scammer used here?
This scammer has a very tempting offer, because Robucks (R$) has to be purchased with a credit card in the official app. Offering something that's "too good to be true" is a common tactic to entice users to click on phishing links.

2. What's the motivation behind this phishing scam?
Cybercriminals target gamers for many reasons, one of them is to obtain your login information. Once they get into your account, they can take any existing in-game purchases you have made before (such as money, premium features, skins, or characters). The other reason is to trick you into downloading a malware virus that would infect your device and allow them access to your data.

3. What red flags should we look out for?
1. "Too good to be true" offer. Don't fall for this tempting offer!

2. Unknown link from an unknown user. Do not click on any links that don't look right.

3. Asking to connect your account. Only enter your information to official websites.

4. Download this virus. Never download and install anything to your device from suspicious websites.

KEY TAKEAWAYS
10 MINUTES

Slide 15

Say: Here are some things we've learned from this lesson.

1. Cybercriminals and bad actors create tempting scams to trick you into giving them your personal information, login credentials, or money.

2. Think before you click. Never click or download anything that was sent to you by an unknown or unverified user.

3. Use your critical judgement and don't fall for "too good to be true" offers.

Ask: What are some key takeaways you've learned from this lesson?
Call on volunteers to share what they've learned.

© Cyberlite Books Pte. Ltd. All Rights Reserved.