Money or Love?

EXERCISE-IN-A-BOX LESSON PLAN (16-17 years old)

OVERVIEW

This lesson educates students about cyberattack tactics like urgency, intimidation, and love bombing, helping them understand how these methods manipulate and deceive. By recognising these tactics, students can better protect their personal information and take appropriate actions to stay safe online.

LEARNING OBJECTIVES

Students will be able to:

- Explain how urgency can be used to manipulate individuals into acting hastily without considering the risks.
- Evaluate the tactic of intimidation in coercing individuals into divulging personal information or making payments.
- Identify and describe the concept of love bombing in relation to romance scams, and demonstrate how to avoid falling victim to this tactic by recognising warning signs and being cautious with online relationships.

DURATION

60 minutes

KEYWORDS

- **Urgency**: A tactic used by scammers to create a sense of urgency in their victims to take immediate action without thinking it through. The message is designed to cause fear and panic within the recipient.
- **Intimidation**: Intimidation is a scare tactic used by cybercriminals to create fear or a sense of threat in the victim to coerce them into clicking on a link, providing personal information, or making a payment.
- **Love Bombing**: Scammers may quickly profess their love and affection for their victims, using language that is romantic and overly sentimental. They often love bomb in romance scams to quickly gain the trust and affection of their victims through excessive flattery and declarations of love.

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.

Money or Love?

EXERCISE-IN-A-BOX LESSON PLAN (16-17 years old)

WARM-UP

5 MINUTES

Slide 1

Say: Today, we will be learning about phishing and scams. Cybercriminals use sophisticated, psychological manipulation tactics to scam their victims out of sensitive information and money, which is why it is very important for us to learn how to protect ourselves against these attacks.

Slide 2

Ask: Why do you think phishing attacks and scams occur? What do the cybercriminals want?

Phishing attacks and scams occur because cybercriminals want to exploit the vulnerabilities of victims in order to steal valuable information or scam them out of lots of money.

Slide 3

Ask: How do phishing attacks and scams impact victims?

Phishing attacks and scams can have a devastating impact on victims. If their personal information has been stolen, this data will forever be lost to cybercriminals as they will have a record of the information to use indefinitely. Victims who have been scammed out of a lot of money would also suffer the financial losses.

DEFINE THE KEYWORDS

15 MINUTES

Slide 4

Ask: **Does anyone know what urgency, intimidation, and love bombing 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: **When you receive an urgent message asking you to do something, how do you react?**

The nature of urgent messages requires someone to act fast, which may mean they don't always pause and think about the situation at hand. Cybercriminlas exploit this as a phishing and scam tactic in order to stop individuals from exercising their critical judgement until it's too late.

Slide 6

Read the contents of the slide aloud.

Discuss: Why would intimidation work as a phishing and scam tactic?
This tactic works because individuals are usually compliant when they are in an intimidating situation. Many scammers will intimidate victims by impersonating authority figures such as government officials, which puts the victim in a mindset where they'll agree to as they're told.

Slide 7

Read the contents of the slide aloud.

Discuss: Have you heard of romance scams before? Why do you know about it?
Romance scams are popular amongst online scammers as they reap great financial gains from each victim. This is when someone believes they have a relationship with a person they've met online, but in reality they're speaking to a scammer who asks for money for all kinds of reasons, such as for help paying rent or medical bills.

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 email.

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?
In this example, the scammer has used intimidation and urgency to instil fear in the victim. Many phishing emails or messages will pose as government officials to create a sense of fear or panic in the recipient, because people generally don't want to get in trouble with the law.

2. What's the motivation behind this phishing scam?
This email is designed to scam victims out of a lot of money and provide personal information (passport details) on a short deadline. The combination of urgency and intimidation forces the victim to act quickly and not think things through carefully.

3. What red flags should we look out for?
1. Always check the sender before acting out of fear. If you are unsure, call the official or national helpline to verify the email.

2. Scammers may use official logos to trick users. Don't blindly believe the message because of the logo.

3. The intimidating and urgent nature of the message can make you act carelessly. Seek help from trusted adults or official authorities.

4. Always check the URL before making payments or providing personal information.

Slide 11

Investigate this text conversation.

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?
Jodie is love bombing Calvin in this romance scam. Jodie's messages are full of flattery and compliments which quickly escalates to declarations of love. This is a common tactic to gain the trust of victims.

2. What's the motivation behind this phishing scam?
Romance scams often target vulnerable victims to send them money or gift cards for a variety of reasons. They usually ask for a small amount to start, such as buying a plane ticket or asking for gift cards, and will increase the amount quickly for reasons such as paying for rent or medical bills.

3. What red flags should we look out for?
1. Love scammers will often shower you with flattery and compliments to gain your trust.

2. Love bombing can often feel like the relationship is moving very fast. Listen to your gut feeling to see if the pace feels unnatural or forced.

3. Jodie doesn't use a lot of personalised language (such as calling Calvin by name) and often mirrors what Calvin has just said without providing much information about herself.

4. Be careful of sending money to someone you don't know in real life.

Slide 13

Investigate these SMS messages.

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 is an example of the urgency tactic used in an SMS phishing attack (also known as smishing). The scam creates a sense of urgency, resulting in victims acting without checking for red flags.

2. What's the motivation behind this phishing scam?
Attacks like this often target victims to enter their login credentials or banking details through a phishing link, as it preys on the victim's sense of urgency and panic.

3. What red flags should we look out for?
1. Always check the URL link before clicking to ensure it's the official address.

2. The grammatical errors in these messages are red flags. Official communications from banks will be written properly.

3. If you are unsure of a message's authenticity, call your bank's official hotline for assistance. Do not call any phone numbers that may be in the suspicious messages.

KEY TAKEAWAYS
10 MINUTES

Slide 15

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

1. Don't panic. If you receive messages that instil fear, panic, or urgency, remember to take a step back and look out for the red flags. Scams are often designed to persuade the victims to act fast without thinking.

2. If you are unsure of a message you've received, ask a trusted adult for help. You should call the national or official hotline for verification and assistance. Never call the phone number provided in the suspicious message as it could lead you back to the scammer.

3. Be aware of anyone who showers you with compliments and love too quickly or early. This could be a sign of love bombing in a romance scam.

4. Remember to always check who the sender of the message is.

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