

Title: Identifying Fake Links and Pop-Ups

Description: In this scenario, students will actively explore and practice identifying suspicious links and pop-ups through specific tasks. They will analyze real-world examples and perform hands-on actions to recognize the traits of fake links and pop-ups, ensuring a better understanding of safe browsing habits.

Purpose: The purpose of this practical is to engage students in identifying fake links and pop-ups through actionable steps. By performing these tasks, they will develop the ability to recognize and avoid online threats effectively.

What is Phishing: Phishing is like a **trick or a trap** on the internet. Imagine someone pretending to be your friend to steal your lunchbox. Similarly, in phishing, someone pretends to be a trusted website or person to steal your personal information, like passwords or money.

For example, you might get an email or message saying, "You won a prize! Click here to claim it." But when you click, they ask for your password or credit card details. If you share this, they can use it to harm you.

The best way to avoid phishing is to **never click on links or share personal information** unless you're 100% sure it's safe. Always double-check!

Steps:

1. Play an Interactive Game to Identify Fake Links:

- Open your web browser, go to **Phishing Quiz by Google** (<https://phishingquiz.withgoogle.com/>)
- **Start the quiz** by clicking "Take the quiz" or something similar

Can you spot when you're being phished?

Phishing attacks attempt to trick unsuspecting users into revealing personal or financial information, often by mimicking content from well-known, trusted companies.

AI is already making phishing attacks more sophisticated, personalized, and common.

Think you can tell what's real or fake?

Take the quiz

2. Make up a name and email:

- Enter any dummy name and email.
- Don't worry the email is not necessary to be valid or yours.

Make up a name and email.

Create a name and email — neither need to be real — to make this quiz seem more realistic.
Don't worry, this information won't leave your device. *More*

Name*

Rahul Hinduja

Email*

incorrect@email.com|

Get started

3. Look at the email shown on the screen and play the quiz:

- Your task is to decide if the email is **Phishing (Fake/Spam)** or **Legitimate (Real/Valid)**. Select your answer.
- **Hint:** check out link URLs by hovering or using long presses

Let's start with this Google Doc email.

Be sure to check out link URLs by hovering or using long presses, and to explore the email addresses. Don't worry, none of the links will work - we don't want to send you anywhere funny!

Phishing

Legitimate

 **Luke Johnson** <luke.json8000@gmail.com>
to me ▾

6:47 PM

Luke Johnson shared a document

 Luke Johnson (luke.json8000@gmail.com) has invited you to **edit** the following document:

Hey there. Here is the doc you asked for. Let me know if you need anything else!

 2024 Department Budget ☆

- If you chose **Phishing**, great job! You're correct.
- If you selected **Legitimate**, that's not the right answer.

Incorrect! This is actually a phishing email.

The URL looks correct but is actually a look-alike. Be cautious about hyperlinks and attachments you open from emails — they may direct you to fraudulent websites where you're asked to input sensitive information.

Show me

- Let's see why. Click on "Show Me"
 - The email might look real, like it's from someone you know, but look closely. Move your mouse over the attachment or link without clicking. Notice the link says something like **drive--google.com/** instead of **drive.google.com/**.
 - That small change makes the link fake.
 - This is a phishing email trying to trick you into clicking it!

Mousing over this link or using a long press will show you that it goes to the insecure imitation domain "drive--google.com."

Next

- Click **Next** to attempt a new question and continue testing your skills.
 - Carefully examine details like the **sender's email address** and **link URLs** for any suspicious signs.
 - Be cautious of emails making unrealistic claims, such as winning a lottery or receiving unexpected offers.
 - At the end of the quiz, **note down your score**. Discuss your results with the class and learn from each other's observations!

Good effort, Rahul Hinduja!

You got 8/10 correct.

Practice makes perfect and the more you understand what to look for, the safer you are from phishing attacks.

You can also take a few simple steps to better protect your online accounts. Learn more at g.co/2SV.

Share the quiz:



Take the quiz again

4. Take the quiz again:

- Retake the quiz to improve your score and enhance your ability to spot phishing attempts.