Detecting phishing scams

Please refer to the online lesson plan on the DT Hub to access all website links and additional resources.

**Year levels: 7–8; Duration: 1 x 60min**

**Digital Technologies:** Privacy and security, Generating and designing

****

Source: Pixabay

In this learning sequence, students work in groups to create and analyse common phishing scams, gaining a deeper understanding of the techniques used by scammers. They then develop rules for artificial intelligence (AI) algorithms to detect these scams, promoting critical thinking about cybersecurity and online safety.

# Learning map and outcomes

**Learning intention**

To understand common phishing techniques and how AI algorithms can be trained to detect them.

**Success criteria**

Students will be able to:

* identify and explain common phishing techniques
* develop rules or criteria for AI algorithms to detect phishing scams
* evaluate the effectiveness of their rules in detecting phishing scams.

### Preparation and materials

* Phishing scam detection rules [Word]
* Phishing scam detection flowchart [Word]
* Teacher slides: Phishing scams
* Optional:
* Sample phishing emails
* Video Phishing Email Example – Office 365 Lure
* Website Spotting scams
* Phishy Emails interactive activity – Grok Academy (requires log-in)

### Key terms

**Phishing:** a ‘fraudulent practice of sending non targeted emails asking people to reveal sensitive data such as bank details or encouraging people to open a malicious attachment or download malicious content’.

**Scam:** a dishonest scheme or fraud, typically for financial gain. A phishing scam combines the elements of phishing and a scam. It involves the fraudulent practice of sending emails or messages that appear to be from reputable sources. These messages aim to deceive recipients into revealing sensitive personal information (such as passwords, credit card numbers, or bank details) or into performing actions that compromise their security (such as opening a malicious attachment, downloading harmful content, or clicking on a link). The primary goal of a **phishing scam** is typically financial gain through unauthorised access and misuse of the victim's information or resources.

**Spoofing**: when someone pretends to be someone else to trick you. For example, if you get a call that looks like it’s from a friend but it’s really a scammer asking for your password, that’s phone spoofing. Or, if you get an email that looks like it’s from your teacher asking for personal info, that’s email spoofing. People spoof to steal your information or money. To protect yourself, be suspicious of unusual requests, check for mistakes in messages, and never share personal info unless you’re sure it’s legitimate. Stay cautious to avoid being tricked!

# Learning hook

Discuss what phishing scams are and why they can be harmful.

Use the Teacher slides: Phishing scams to support this lesson.

Divide students into small groups and give each group 5 minutes to come up with a common phishing scam. Encourage them to think about the different tactics used in phishing scams, such as urgency, curiosity or impersonation. Share these with the class. Discuss the common techniques used in each scam and why they might be effective.

Compare the class suggestions to relevant examples, such as these:

* View the video Phishing Email Example – Office 365 Lure.
* Refer to the Australian Government website Spotting scams, which provides an overview of phishing messages and includes a short engaging quiz for students to apply their knowledge.

# Learning input and construction

Explain that AI algorithms can be trained to identify phishing scams by recognising patterns and techniques commonly used by scammers.

Explain that students are going to create a phishing detection algorithm.

Ask each group to consider a particular phishing technique to investigate further. Have each group brainstorm a set of rules or criteria that an AI algorithm could use to detect emails or messages using that specific phishing technique.

After each group has been assigned a specific phishing scam, provide them with some starting points for brainstorming rules or criteria. For example, you could suggest looking for specific keywords or phrases, checking the sender's email address for authenticity, or examining the email's formatting for inconsistencies.

You may decide to scaffold this process using a scaffold such as:

Rule number [#]:

* Criteria: [Describe the specific characteristics or indicators that the AI should look for.]
* Rationale: [Explain why these criteria are important for detecting the phishing scam.]
* Example: [Provide an example of an email or message that meets these criteria.]

Encourage students to think about the characteristics of the phishing scam that make it identifiable and how these characteristics could be translated into rules for an AI algorithm.

Have each group work together to develop a list of rules or criteria based on their assigned phishing scam. They should consider how these rules would be applied by an AI algorithm to detect similar scams in real-world situations. Encourage students to be specific and detailed in their rules, considering factors such as language use, sender information and formatting.

As a precursor to their algorithm, they could write the rule considering criteria, rationale and their example, as in the scaffold above.

Provide the Phishing scam detection rules sheet to scaffold the activity.

Here’s an example Phishing scam description:

The phishing scam involves receiving an email that appears to be from a popular online retailer, claiming there is an issue with your account and requesting you to click on a link to resolve it.

Rule 1: Sender email address verification

* Criteria: check if the sender's email address matches the official domain of the online retailer (e.g. @amazon.com).
* Rationale: legitimate emails from the online retailer would typically come from an official domain while phishing emails often use spoofed or unofficial domains.
* Example: if the email claims to be from Amazon but the sender's email address is something like ‘amazon-support@gmail.com’, it is likely a phishing scam.

Differentiation (Support)

* For students who need support, assign one simple phishing scam with more obvious indicators, such as spelling errors or suspicious sender addresses.
* Some students may not be familiar with algorithms and require support to follow an algorithm before being able to create their own. Provide these students with the Phishing scam detection flowchart sheet.

**Differentiation (extension)**

* Some students may be able to create an algorithm in pseudocode.
* To create an algorithm in pseudocode some students may need guidance and could use a flowchart as provided in *Phishing scam detection flowchart* sheet as a starting point.

**Sample pseudocode (guide only)**

START

IF sender's email address does not match official domain

THEN flag email as phishing scam and END

ELSE IF there are signs of email spoofing

THEN flag email as phishing scam and END

ELSE IF there are grammar or spelling errors

THEN flag email as phishing scam and END

ELSE IF email contains urgent requests or threats

THEN flag email as phishing scam and END

ELSE

flag email as legitimate email and END

END

# Reflection

Discuss the effectiveness of each rule in detecting phishing scams and identify any limitations or improvements that could be made to the rules.

### Why is this relevant?

By learning about common phishing techniques and how AI algorithms can be used to detect them, students become more informed and vigilant online users. They also gain an understanding of how technology can be both beneficial and potentially harmful, empowering them to make safer choices in their online interactions.

# Resources

* Spotting scams : This Australian Government website provides an overview of phishing messages and includes a short engaging quiz for students to apply their knowledge.
* Video: Phishing Email Example – Office 365 Lure
* Phishing scam detection rules sheet
* Phishing scam detection flowchart sheet
* Teacher slides: Phishing scams
* Successful pseudocoding provides useful background to teaching your students about pseudocoding

# Assessment

**Achievement standard**

By the end of Year 8 students select appropriate hardware for particular tasks, explain how data is transmitted and secured in networks, and identify cyber security threats.

# Australian Curriculum alignment

**Technologies – Digital Technologies**

##### Privacy and security

* Explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats AC9TDI8P13

##### Generating and designing

###### Design algorithms involving nested control structures and represent them using flowcharts and pseudocode AC9TDI8P05