Lesson Plan S2 - Unit 1

“The one where we teach them how to phish”

HOW TO **PHISH**

----X

Essential Question

What is identity theft, how is it perpetrated and how can you protect yourself from it?

Estimated time: 45 minutes

Curriculum impact

Digital literacy - cyber resilience and internet **TCH 2-03a**

Digital literacy - Searching, processing and managing information responsibly **TCH 3-01a**

Digital literacy - cyber resilience and internet safety **TCH 3-03a**

Lesson Overview

Students will learn how threat actors use emails and links to access their private information online. They learn what identity theft is and what kind of information identity thieves want and what can be done with the information. Students then analyse fake emails and identify tricks that identity thieves use online. Finally they create a phishing email that includes the features they have learned about, and see if their classmates can identify the scams.

Key Vocabulary

Identity theft: a type of crime where your private information is stolen and used for criminal Activity.

Phishing: when people send you fake emails, pop-up messages, social media messages, texts, calls or links to fake websites to hook you into giving out your personal and financial Information.

Learning Objectives

Pupils will be able to:

- Understand what identity theft is and why it is important to guard against it.
- Learn to recognise strategies that scam artists use to access private information.
- Learn how to guard against phishing and identity theft.

Materials and preparation

- Laptops & Pi server with “Unit 1 S2” module
- Computer misuse act & exec summary
- Spotting scams S2U1 handouts - teacher and student version.

Family resources

Send home the spotting identity theft tips for families sheet.

WARM UP - ASK (5 minutes)

- - - - X

"Do you know someone who has been scammed? What happened?"	Pupils might tell stories of instances in which someone has been convinced to send someone else money or purchase fake or bad product.
"What is the purpose of a scam? What tricks do people use to carry out a scam?"	Pupils should understand that the ultimate purpose of a scam is to get someone to give the scammer money, or information that can help the scammer steal money such as a credit card number, ATM code or password. To achieve this, scammers tell lies and often pretend to be someone they are not
"Can people get scammed on the Internet? How?"	Allow student to tell stories of friends of relatives who have been scammed online. Then encourage them to revisit what they know about scams, and how they might be used online. Sample responses: • Someone can be tricked into buying bad or fake product online • Someone can be lured into sharing information that a scammer can use to steal from them.

EXPLAIN to pupils that they will be learning about phishing including which kinds of information hackers are looking for, and how that information will be used. They will also learn how to protect themselves against phishing attacks.

ETHICS (5 minutes)

- - - - X

"Can people get scammed on the Internet? How?"	Cyber security and ethical hacking teaches techniques which could get students into trouble if used inappropriately.

SHOW the **Computer Misuse Act** and briefly discuss

DISTRIBUTE the computer misuse act executive summary to each pupil

WHAT IS **IDENTITY THEFT** - (10 minutes)

----X

“How do you think thieves might try to get your information?”

Encourage pupils to share some responses, even if they have not previously encountered identity theft.

DEFINE the Key Vocabulary term **phishing**.

EXPLAIN to students the best way to avoid phishing scams is to be sceptical about any online request for personal information. It is also good to be sceptical of online messages or posts from friends that seem out of character for them, which is a warning sign that their accounts have been hacked. There are clues that can help people to spot phishing, and they will learn some of these in the next part of the lesson by studying one type of phishing scam: a fake email message.

ASK...

“How do you think thieves might try to get your information?”

Encourage pupils to share some responses, even if they have not previously encountered identity theft.

DIVIDE the students into pairs.

DISTRIBUTE the **S2U1 spotting scams student handout**

INSTRUCT pupils to complete the **S2U1 spotting scams student handout** together. When students are done, have two pairs get together to exchange their handouts and compare their answers.

READ aloud the instructions found on the **S2U1 spotting scams student handout - teacher version**, and share with students the extended explanation of each feature of a phishing email.

INVITE volunteers to share their answers with the class. Use **spotting scams student handout - teacher version** for guidance.

REMIND pupils that phishing emails can be very convincing, and some may not contain many of the clues they just learned about. So it is smart to distrust any email that asks them to provide private information.

MAKING IT **REAL** - (10 minutes)

----X

INVITE the teams of two to login to their Macbook Pro email account

ASK the pupils to look at the emails on their computer, there will be some genuine and some fake. Instruct the pupils to sort their emails into **real** and **fake.** The server will rank the teams in terms of speed and accuracy.

SHOW the fake emails and show the techniques used

BECOME THE **HACKER** - (15 minutes)

----X

INSTRUCT pupils to choose at least four of the eight features of a phishing email listed in their **Spotting scams student handout**. Have them create a phishing email on their computer that demonstrates the features that they choose to highlight and email them to the *hack@cyberbus.com*.

SHOW the emails to the class on a projector. Classmates can try to identify which features tipped them off to the fact that this is a phishing email and provide prizes to the best ones.

CLOSING - (5 minutes)

----X

You can use these questions to assess the class's understanding of the lesson objectives.

ASK...

"What kinds of information do identity thieves look for – and why?"

Students should respond with examples of private information, such as full name, address, date of birth, account numbers, and passwords.

Identity thieves try to use this information in order to recreate someone's identity for unlawful purposes.

"How do thieves try to get at your information?"

Thieves use phishing to try to get people's personal information. Have students discuss some of the features of phishing they learned about.

“*What can you do to avoid falling for online scams?*”

Students should remember to be suspicious of any online communication that asks for private information, or that seems out of character for a friend to have sent or posted.

DISPLAY the following URL. Tell pupils they can go to ***www.getsafeonline.com*** for more information about identity theft. If they are worried about any aspect of cybercrime they can speak to a teacher or ***Police Scotland?***