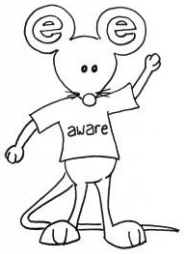
eaware LESSON PLANS

PHISHING

Years 5 & 6



Learning Objectives

Understand the meaning of 'phishing'
Understand what to look out for when identifying phishing emails
Understand what to do if a phishing email is identified

Resources

- Learning pathway video
- Printed copies of Resource 1
- Displayed or printed copies of Resource 2
- Printed copies of Worksheet 1

Success Criteria

- I know what 'phishing' means
- I can identify a possible phishing email
- I know what do if I receive a phishing email.

Key Vocabulary

- Email
- Phishing
- Spam
- Personal information
- Scam/scammer
- Identity theft

Main Lesson Sequence (40-60 minutes)

- Watch the learning pathway video 'Phishing' (They may remember this video from Year 3/4). Ask them how many of them use email? Do they remember what junk mail or spam is? Why are phishing emails more dangerous than spam emails?
- Remind them that Phishing is a way that criminals get sensitive information (like usernames or passwords). Very often, phishing is done by email. This mail appears to come from a bank or other service provider. It usually says that because of some change in the system, the users need to re-enter their usernames or passwords to confirm them. The emails usually have a link to a page that looks almost like that of the real bank. Phishing allows criminals to get access to bank accounts, or other accounts like shopping, auction or gaming accounts. It can also be used for identity theft.
- Distribute the scenario cards (Resource 1) to small groups. Ask the children to read the scenario and discuss what the risks are and what they think the person should do. Discuss these as a class.
- Explain there are many clues to look out for when trying to detect phishing/scam emails and messages. Display these on the board (Resource 2) and discuss them. Distribute copies of Worksheet 1 and ask the children to look at the messages carefully. Using a high-lighter they should highlight the clues that we have discussed from resource 2 and name the clue (red writing).
- Do the children remember from year 3/4 what to do if they come across an email or message which they suspect is a scam? Do not open the email. Move the email to your junk folder. If the email has been opened, do not click on any links. Tell a trusted adult that you have received the email. Ask a trusted adult to help with reporting the email.

Extension Activities

- While this is a serious topic, there is a light-hearted video on TED Talks that you could show your class if you feel it is suitable
  https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email#t-90947
- The children could have a go at creating their own scam/phishing email on a computer. How difficult is it to make it look genuine?