BE INTERNET ALERT

Lesson summary It’s important for children to understand that online content isn’t always honest or reliable, and is sometimes even deliberately designed to steal personal information. The activities in this lesson help give children the skills to stay safe online by spotting the clues that something may be suspicious, misleading or a scam.

Print page 3-4 and handout 1 between 2

**Focus on page 3**

Here are some more questions to ask yourself when assessing messages or sites you find online:

* Does this message look right? What’s your first instinct? Do you notice any untrustworthy parts?
* Is the email offering you something for free? Free offers usually aren’t really free.
* Is it asking for your personal information? Some websites ask for personal information so they can send you more scams. For example, a ‘personality test’ could be gathering facts to make it easy to guess your password or other secret information.
* Most real businesses, on the other hand, won’t ask for personal information over email.
* Is it a chain email or social post? Emails and posts that ask you to forward this to everyone you know can put you and others at risk. Don’t do it unless you’re sure of the source and sure the message is safe to pass on.
* Read the fine print. At the bottom of most documents you’ll find the fine print. This text is tiny, and often contains the stuff you’re supposed to miss. For example, a headline at the top might say ‘you’ve won a free phone’, but in the fine print you’ll read that you actually have to pay that company £200 per month.

**Focus on page 4**

What is this phishing thing anyway?

Phishing in the online world (not to be confused with ‘fishing’ with an ‘f’) is when someone tries to steal information like your login or account details in an email, text, or other online communication by pretending to be someone you trust. Phishing emails — and the unsafe sites they try to send you to or the downloads and attachments they try to get you to open — can also put viruses on your computer that use your contacts list to target your friends and family with more phishing emails. Other scams might try to trick you into downloading malware or unwanted software by telling you that there’s something wrong with your device. Remember:

* A website or ad can’t tell if there’s anything wrong with your machine!
* Some phishing attacks are obviously fake. But others can be sophisticated and convincing. For instance, when a scammer sends you a message that includes some of your personal information, it’s called ‘spear phishing’, and it can be very effective.
* It’s important to know how to spot anything odd or unusual in emails and texts early, before you click on questionable links or enter your password on risky websites. Here are some questions to ask when you’re assessing a message or site:
* Does it include the indicators of a trustworthy site, such as badges?
* Does a siteʼs URL match the name and title youʼre looking for?
* Are there any pop-ups? (Theyʼre often bad news.)
* Does the URL start with ‘https://’ preceded by a green padlock? (That means the connection is encrypted and secure.)
* What’s in the fine print? (That’s where they put the sneaky stuff.)

And what if you do fall for a scam? Start with this: Don’t panic!

Tell your parent, teacher, or another trusted adult right away. The longer you wait, the worse things could get.

Change your passwords for online accounts.

Let any friends who might be targeted as a result know.

Use settings to report the message as spam, if possible.

Group Discussion, ask each group to discuss a scenario, using the sheet to guide discussion

#### Is this real or fake?



Real Fake

#### Is this real or fake?



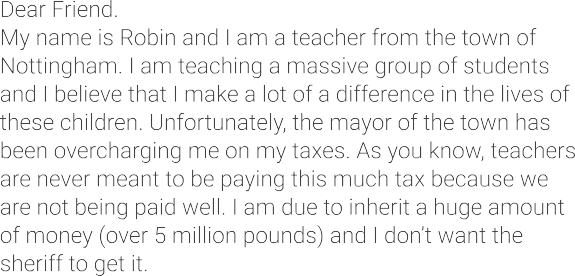
Real Fake

#### Is this real or fake?



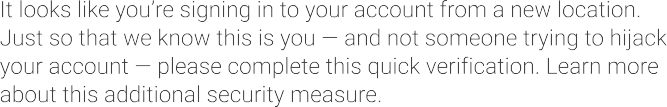
Real Fake

#### Is this real or fake?



Real Fake

#### Is this real or fake?



Real Fake