scamwiseNI PARTNERSHIP

Phishing for Trouble

Lesson Plan: Phising for Trouble

The activities in this resource aim to help pupils learn how identity theft can happen. Pupils identify ways they can protect their personal information and empower themselves, their family, friends and community to avoid a variety of scams, including phishing, vishing and smishing.

This resource embeds e-safety education into teaching and learning in Learning for Life and Work. There are opportunities in this resource to connect learning across other areas of the curriculum such as Financial Capability, The Arts, English and Using ICT.

Curriculum Links

Area of Learning	Learning for Life and Work
Subject Strand	Personal Development
Key Concept	Personal Health
Learning Outcome	Develop strategies to promote personal safety, for example developing safe practice in relation to the internet or understanding and managing risk.

Focus for Thinking Skills and Personal Capabilities

Managing Information
Thinking, Problem Solving and Decision Making
Being Creative

Learning Intentions

We are learning:

- to be aware of our personal information;
- about the risks of identity theft;
- how to be a critical consumer online; and
- strategies to stay safe online.

Keywords: personal information, scam, genuine, trustworthy, suspicious, identify theft, phishing, smishing and vishing

Getting Started

Remind the pupils of the importance of keeping personal stories private. Let the pupils know that this lesson will focus on what we mean by identity theft, how we can protect ourselves, friends and family and the importance of keeping personal information safe.

Consider providing sources of support for young people if they or someone they know has been affected by scams. Fraud prevention support information is provided at the bottom of resource 3.

A question box that allows pupils to submit questions anonymously is a useful feature for this learning sequence.

Activity 1: It's Private!

Setup an online collaborative whiteboard such as Google Jamboard or Padlet. Invite pupils to contribute what they know or understand about **identity theft**. Show **slide 2** from the **Phishing for Trouble** presentation.

Encourage pupils to use words and images. Use a whiteboard to discuss some of their contributions. We have started a Google Jamboard – you may wish to make a copy.

Show **slide 3** and share this definition of identity theft:

Identity theft is when your **personal information** is stolen and used for criminal activity.

Show **slide 4** and ask pupils what they think **personal information** is. Encourage them to think broadly, including and going beyond obvious considerations. For example:

- any information that can be used to identify you, including your name, email address, date of birth or where you live;
- less obvious examples might include who your family and friends are, where you go to school, a photograph or video showing what you look like, your hobbies or places you regularly visit; or
- usernames, passwords and bank or payment details.

Activity 2: What's My Identity?

Show **slide 5**. Ask pupils to choose one of the characters from **Resource 1: What's My Identity?** Encourage them to use the clues provided to list the personal information that defines the character's identity.

Ask the pupils to work in pairs to compare their lists and report back to the class to share their findings. As a class, decide which information might be private and what information the character **should only share** with **trusted** family and/or friends.

In pairs ask pupils to think about their character's activities and actions and decide if this is **safe** or **unsafe**, and report back to the class. Follow up with a class discussion about the consequences of sharing personal information. Discuss how scammers might use personal information to pretend to be you and what this might mean. For example, someone could use your personal information to:

- once you are over 18, apply for credit cards in your name and use them to buy items that you will be charged for;
- befriend and trick someone online into revealing even more personal information;
- cyberbully someone while pretending to be you; or
- create false identification documents.

Working in pairs, ask pupils to consider appropriate **strategies** to avoid risk to their character's personal information. Ask the pairs to feed back to the class. Use **Resource 2: Keep it Private!** as a prompt for developing strategies to avoid unsafe sharing. Encourage pupils to take this information home.

Activity 3: Don't Feed the Phish

Show **slide 6**. Invite pupils to contribute what they know or understand about **phishing**, **vishing** and **smishing**.

These are techniques scammers use to trick people into revealing or sharing their personal information.

Phishing is trying to gather personal information using email.
Vishing is trying to gather personal information by phone call.
Smishing is trying to gather personal information by text message.

Show **slide 7** to summarise phishing, vishing and smishing. Introduce the **4 SCAM Test Rules**, using **Resource 3**.

Show **slide 8**, discuss how the **4 SCAM Test Rules** are useful ways to spot these types of scams and help to avoid sharing personal information with scammers. Encourage pupils to take this information home.

Show **slide 9**. Ask pupils to use **Resource 4: Don't Take the Bait quiz** to practice their anti-phishing skills by deciding which examples are trustworthy and which are suspicious. Encourage them to use the strategies illustrated in the **4 SCAM Test Rules**. Remind pupils to be alert and to consider these questions:

- Does this message look right?
- What is your first instinct?
- Is the message offering you something for free?
- Is it asking you for personal information?
- Is it a chain email or social post they are asking you to forward?
- Do you trust the source?
- Is there small print?

Follow up with a class discussion. Ask pupils if they were surprised by any of the scams.

Take a moment to point out sources of support for young people if they or someone they know has been affected by scams. These are listed at the bottom of resource 3.

You may wish to extend the topic by using CCEA's Key Stage 3 Financial Capability Chapter 2: Banking resources.

CCEA's Banking activities focus on the move from traditional branch banking to the increasing use of online banking. These activities provide guidance on what pupils need to be aware of when it comes to banking online and possible scams. Activities include:

Activity 15	Vigilance when using a bank machine
Activity 16	Telephone banking scams
Activity 17	Online banking scams
Activities 18 and 19	How fraudsters use scams that target social media users

Activity 4: Pause and Reflect

Show **slide 10**. Return to the interactive whiteboard from **Activity 1**. Ask pupils to use a different colour font to add any new ideas or information they have learned since the start of the learning sequence.

Activity 5: Spread the News

Show **slide 11**. The activities in **Resource 5: Spread the News** provide opportunities for connected learning by drawing on knowledge, understanding and skills developed in English and Art as well as opportunities to develop Using ICT.

Encourage pupils, in their groups, to choose one of the options to spread the news about the **4 SCAM Test Rules** to their friends, family or the wider community.

Show **slide 12**. Talk about and send home **Resource 6: Family Tips – How to Stop a Scam**.

Activity 6: Exit Ticket

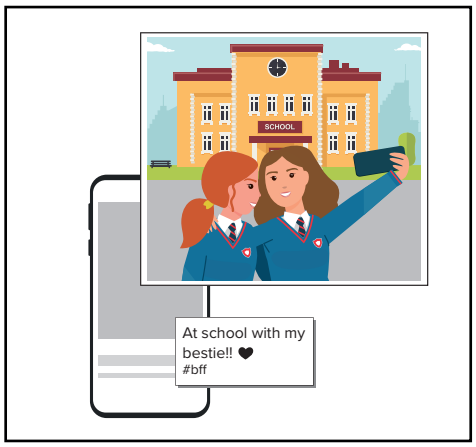
Show **slide 13** and **Resource 7: Exit Ticket**. Ask pupils to complete one ticket. Encourage them to keep this as a reminder:

The **4 SCAM Test Rules** are important to me because …
From now on I will try to …
I have learned to …
I should …
I realise that …

Resource 1: What's My Identity?

Choose one of the characters (or create your own). Use the clues to make a list of the personal information that defines the character's identity.

Niamh



Niamh's personal information

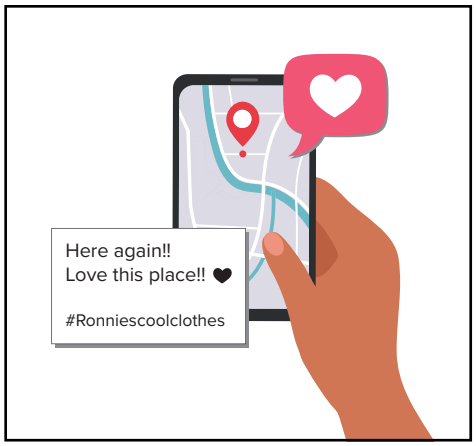
_____

_____

_____

_____

Tim



Tim's personal information

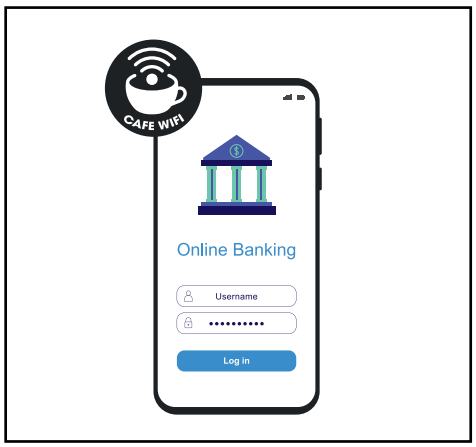
_____

_____

_____

_____

Sadie



Sadie's personal information

_____

_____

_____

_____

Decide which personal information might be **private** and what information the character **should only share** with **trusted** family and/or friends.

Think about your character's **activities** and **actions** and decide if this is **safe** or **unsafe**.

Resource 2: Keep it Private!

Strategies to keep your personal information private:

Think before sharing.

Remember that sharing anything online means that anyone could see it, including friends, family, teachers and scammers.

Keep it simple. Don't over share.

Avoid sharing too many personal or distinguishable features, for example photos of your school uniform, school badge or logo, addresses or tagging places you regularly visit or regular GPS check-ins. Scammers can use this information to build up a profile of your identity.

Don't get tricked into sharing personal information.

Be wary of unusual links, scam emails, text messages and web pop-ups. If an offer sounds too good to be true, it probably is.

Make sure your electronic devices are protected.

Update firewalls and antivirus software regularly and use strong, secure passwords. Regularly check our device privacy settings.

Don't access personal information on public Wi-Fi networks.

Always assume a public Wi-Fi network is not secure.

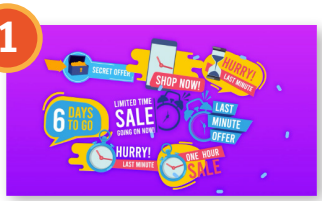
Avoid accidental sharing.

Always check before passing on someone's information, even to someone you know.

Resource 3: 4 SCAM Test Rules

Seems too good to be true? Contacted out of the blue? Use the **4 SCAM Test Rules** to spot a scam and stop a scam:

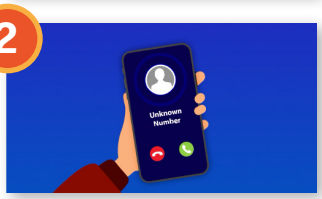
1



Seems too good to be true

Scammers often make false promises, like a last-minute chance to buy products, invest your money or receive free items. Take your time. If it seems too good to be true, it probably is.

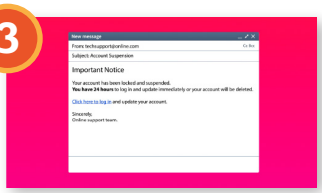
2



Contacted out of the blue

Receive an unexpected call, email, text message or letter? Think: could this be fake? Look out for poor spelling and grammar – this can include the way the email or web address is spelled. It's okay to challenge or refuse a request. Look up the organisation and get in touch directly.

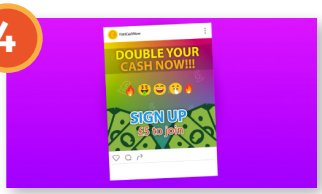
3



Asked for personal details

A phishing scam uses emails to lure you in. Phishing messages may look like they come from a big brand, bank or government office, but they are fake. No genuine organisation will ask for your personal information by email or message. Text message scams are called smishing. Phone call scams are called vishing.

4



Money is requested

Scammers often ask for payment for a 'free' gift, administration fee or sign-up promotion. If it sounds dodgy, it probably is.

If a scammer tries to contact you, you can report it to **Action Fraud on 0300 123 2040** or to the **PSNI** on **101**. Always report bogus callers to the PSNI.

We all have a part to play in the fight against crime. Share these tips to help protect your family and friends, too. Remember, if you can spot a scam, you can stop a scam. For more help and information visit: www.ccea.org.uk/scamwise

Resource 4: Phising for Trouble

Go to www.ccea.org.uk/scamwise choose KS3 and Phishing for Trouble resources.

Practice your anti-phishing skills by deciding which examples are trustworthy and which are suspicious.

Resource 5: Spread the News

News broadcast

Create a news broadcast about one of the scenarios in this resource. Plan and record your news piece. Think about who was involved, what happened and how personal information was protected to help stop an identity theft scam.

Telling the tale

Create a comic strip detailing a scam scenario between a consumer and a scammer. Choose the method and type of scam, illustrating how personal details have been used. Include visuals and captions to illustrate the events.

Don't take the bait!

Use the scenarios and **4 SCAM Test Rules** to craft your own phishing email, smishing text message or vishing voice message. Show your understanding of the techniques scammers use to encourage people to part with valuable personal information. When ready, share your work with your classmate and discuss the techniques used and how to avoid them.

Social media post

Create a (fake) social media post with a catchy headline. Tell the tale of how the **4 SCAM Test Rules** can help to stop an identity theft scam. Invent a profile, profile photo, tagline, add a few hashtags related to the post. Add a selection of images that present a timeline of how one or more scams were stopped. Write captions and relevant comments.

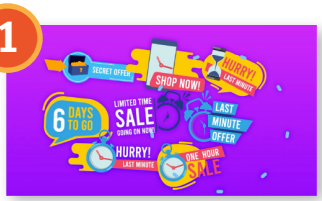
Write a collaborative story

Work with classmates on a collaborative story about a scam involving identity theft. Each writer takes turns adding to a story in different coloured fonts. Leave a cliff-hanger for the next writer until the story is completed.

Resource 6: Family Tips- How to Stop a Scam

Seems too good to be true? Contacted out of the blue? Use the **4 SCAM Test Rules** to spot a scam and stop a scam:

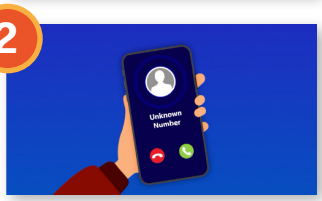
1



Seems too good to be true

Scammers often make false promises, like a last-minute chance to buy products, invest your money or receive free items. Take your time. If it seems too good to be true, it probably is.

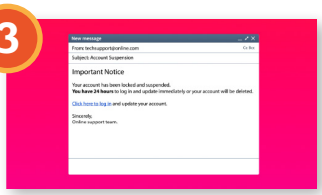
2



Contacted out of the blue

Receive an unexpected call, email, text message or letter? Think: could this be fake? Look out for poor spelling and grammar – this can include the way the email or web address is spelled. It's okay to challenge or refuse a request. Look up the organisation and get in touch directly.

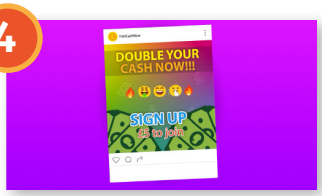
3



Asked for personal details

A phishing scam uses emails to lure you in. Phishing messages may look like they come from a big brand, bank or government office, but they are fake. No genuine organisation will ask for your personal information by email or message. Text message scams are called smishing. Phone call scams are called vishing.

4



Money is requested

Scammers often ask for payment for a 'free' gift, administration fee or sign-up promotion. If it sounds dodgy, it probably is.

If a scammer tries to contact you, you can report it to **Action Fraud on 0300 123 2040** or to the **PSNI** on **101**. Always report bogus callers to the PSNI.

We all have a part to play in the fight against crime. Share these tips to help protect your family and friends, too. Remember, if you can spot a scam, you can stop a scam. For more help and information visit: www.ccea.org.uk/scamwise

Resource 7: Exit Ticket

The **4 SCAM Test Rules** are important to me because ...

From now on I will try to ...

I have learned to ...

I should ...

I realise that ...