SCAMS AND YOUNG PEOPLE

INSTRUCTIONS

For this activity you will need printouts of:
Factsheet - Scams and Young People

For the young people (find in the resources folder):
Printouts x how many in your group:

- **Could you be a victim of a scam?**
- **Would you respond?**
- **Pencils or Pens**

1. **Have a short discussion with your group to see if they have encountered any scams aimed at them? (5 minutes)**

2. **Go through the scams factsheet**
   - Scams impacting young people – page 2-3 (Page 3 - recommended age 11+)
   - How to protect yourself – page 4

3. **Pick the most appropriate activity or do both if you have enough time. This can be done individually (recommended age 11+) in pairs or a group depending on the age group.**
   - Could you be a victim of a scam? (5 minutes)
   - Would you respond? (15 minutes)

SCAMS IMPACTING YOUNG PEOPLE

Anyone can be a scam victim, regardless of age, gender, education or economic background.

Younger people are especially likely to fall victim to online scams such as fake websites which are used to get people to give them personal information such as bank account numbers or credit card numbers and pin codes.

Younger people often think they are less likely to be hit by scams, however there are many common scams specifically targeted to this age group. Common types of scams targeting this age group include subscription traps, social media, gaming, ticketing and job/rent scams.

Half of young people say they would never fall for an online scam.

PHISHING

Phishing is a way that criminals get sensitive information like usernames and passwords. This is usually done by an urgent email which will take you to a fake website which may look real or familiar to you. They are fake sites set up by criminals to gain your personal details.

Phishing can also happen by phone via text messages known as smishing or by a call which is called vishing.

GAMING

Games that contain virtual money such as Fortnite have become an avenue of exploitation for criminals. There are many websites that are offering free virtual money for different games, provided you pass on your personal details. This could result in criminals having access to yours or your parent's bank accounts.

As games are being turned into mobile versions, criminals have started to create fake downloadable versions of the game. This is another way to get you to give your personal data to criminals.

Recommended for age 11+

MONEY MULES

Money mule scams target individuals who are likely to be in need of money or want money. It is an easy way to make some cash, therefore many young people can become victims of this scam. Criminals transfer stolen money into a young persons bank account and then they are persuaded to transfer the money to a different bank account while getting to keep some of the illegal money.

They do this by:

- Making friends with a potential mule.
- Offer big money for no effort.
- They may become violent or threaten the person.

If you are caught being a money mule you will have your bank account closed and could go to prison for up to 14 years.

SOCIAL MEDIA

Social media scams usually appear as promotional deals and competitions that are too good to be true.

- They may have genuine links, use official brand logos and/or links to enter your personal details.
- Clicking on these links sends your personal information to the criminals and potentially shares features and status messages from your own personal account for all your friends and family to see which could lead to them falling for the same scam.

How to spot them:

- You may be seeing a high volume of the same/similar status updates from people on your social media.
- Always check the branding for irregularities from what you believe it should be.
- Stay vigilant when you see new companies, organisations or brands pop up on your social media. It may be a scammer pretending to advertise.

HOW TO PROTECT YOURSELF

As well as protecting your community against scams, there are also ways you can protect yourself from scams that are targeted more at young people. Some of these may not apply to you now but they are great to know for your future:

1. If you think you have been scammed or a victim of cyber crime contact Action Fraud or Citizens Advice to report it.
   - Action Fraud: 0300 123 2040
   - Citizens Advice: 0808 223 1133
2. You can report spam texts from your mobile phone by forwarding the message to 7726 for free!
3. Do not download anything unless a parent approves it.
4. If you get any suspicious emails or messages with links, asking for your personal details, report it and then delete it!
   - If you are not sure get a parent to look over it.
5. If you're suspicious of a link in your email, hover over it with your mouse and you can see the real URL.
   - On mobile phones you can do the same by tapping and holding your finger on the link.
6. Only visit parent-approved websites.
7. Always check you are on genuine, secure websites. You can do this by looking at the website address.
   - Does it look suspicious?
   - Does it match the website address of the company?
   - If you are logging onto a website, make sure it is the genuine login page.
   - HTTPS - S stands for secure - look for this.
8. Be careful of strangers or people you are not sure about contacting you through social media or in person.
9. Do not share personal information on social media or with people you do not trust.
10. Never give your bank details to anyone in person or over the internet.
    - Your bank will never ask you for all the details - they should already know some of them!