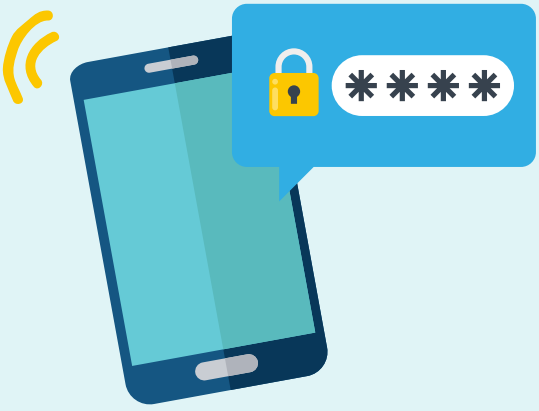
scamwiseNI
PARTNERSHIP

BECOME A SCAMWISE CHAMPION



WE DISCOVER, WE GROW Girlguiding Ulster

THE BOYS' BRIGADE >the adventure begins here Northern Ireland District

scouts be prepared . . .

Girls' Brigade Northern Ireland

Catholic Guides of Ireland

SCOUTING IRELAND

WHAT IS THE SCAMWISE PARTNERSHIP?

The Police Service of Northern Ireland (PSNI) chairs the ScamwiseNI Partnership and works with more than 30 organisations across Northern Ireland to fight against scams, raise awareness of the different types of scams and ensure people are not defrauded of their hard earned money.

We would like to work with the uniformed youth organisations to raise awareness among young people about scams.

DOJ
Department of Justice
www.dojni.gov.uk

The ScamwiseNI partnership would like to thank the Department of Justice (DOJ) for sponsoring this initiative with the uniformed youth organisations.

LET'S STAMP OUT SCAMS

We want young people to:

- Learn about the different types of scams;
- Identify ways in which they can protect themselves, family, friends, schoolmates, neighbours and people living in their community;
- Know who to report scams to;
- Protect their debit card and bank account; and
- Shop safely online and be password savvy.

In order to earn a badge and certificate, we ask the younger age group (10-14) to complete three activities and the older age group (15+) to complete five activities.

Once the boys and girls earn their silver 'Scamwise Champion' badge and certificate, they can progress to earn their gold 'Scamwise Champion' badge and certificate.

Decide what activities you and your unit would like to do, but feel free to complete a few more!

For some of the activities you will need large sheets of paper, colouring pencils, pens, crayons, scissors and markers.

WHAT IS A SCAM?

Scams are when criminals use lies and deceit to fool you into parting with your cash. You usually get nothing in return and lose your money. Scams are becoming increasingly sophisticated and varied but the aim remains the same - to take money from unsuspecting members of the public, so it's important to know what to look for.

There are four different methods through which people can be scammed:

Mail Scams

Scammers may write to you out of the blue using clever techniques to persuade you to send them money or ask for personal and/or banking details. Be wary of letters from lotteries, competitions, clairvoyants, charities and investments.

Phone Scams

Scammers may also call your phone claiming to be from financial institutions, the PSNI, utility companies, law enforcement, Her Majesty's Revenue and Customs (HMRC) (This UK Government department is responsible for the collection of taxes), internet and telecom providers, computer software providers, lottery organisers or other public bodies.

Doorstep Scams

Not all doorstep traders are bogus but watch out for rogue doorstep traders, rogue sales persons and bogus callers.

Online Scams

There are many different types of online scams such as bogus 'free trial' offers, bogus emails, counterfeit goods, loan scams and copycat websites.

HERE ARE SOME COMMON TYPES OF SCAMS

Gaming Scam

Scammers try to steal information and money from people who are playing online games, either by talking to them online or encouraging them to purchase features and upgrades. Ultimately gamers may unwittingly provide personal information and credit or debit card details to get free credits, currency and upgrades.

Phishing Emails

Phishing emails often have a web address embedded in the email and the consumer is asked to click on this link which takes them to a fake website. When the consumer is prompted to enter or update their personal information such as bank account numbers, credit card details or passwords, this allows the fraudster to use these details to commit fraud. These types of emails are often scammers pretending to be from financial institutions or from a music app store.

iTunes Email Scam

Apple customers are targeted by scammers pretending to be from Apple, who send an email to account holders regarding a song purchase. Users are tricked into clicking on a link to claim a refund for a purchase they did not make. After clicking on the link and providing their Apple ID and password, victims are prompted to enter additional personal information such as their full name, address, and credit or debit card details.

Mobile Phone Scams

These scams persuade the consumer to buy phone-related products and services that turn out to be substandard or non-existent; or to make phone calls or send texts to premium services by accident. Consumers can also unknowingly sign up to expensive subscription services.

Tickets Scams

This relates to tickets bought directly from another consumer or via a secondary ticket agent site. In some cases the ticket does not exist as the event is sold out, or the seller has no intention of handing over the ticket.

Catalogue Brochure Scams

Scammers send out literature that promises a variety of different ‘free gifts’ or ‘prizes’. These ‘gifts’ are either worthless, never materialize, or require an order to be placed by sending money or telephoning a premium rate number.

Vishing Scams

This is where scammers contact consumers on the phone and attempt to obtain personal or bank details to use to commit fraud. One example is where a scammer pretends to be from a financial institution and contacts a consumer to say that they have been a victim of fraud. No financial institution will ever phone you to ask for your PIN, or your online password, or to ask you to transfer money to a new account.

Charity Scams

These scams involve a person or a group of people who pretend to represent a non-existing charity and ask for a donation.

Financial Institution Scams

These scams typically involve a fraudster who poses as a member of staff and advises the consumer that they have been a victim of fraud. They will ask for personal and financial information in order to gain access to the consumer’s account and/or commit identity theft. Watch out for fake texts from scammers who pretend to be from a financial institution. Never reply to these type of texts.

Clairvoyant & Religious Scams

This is where a consumer receives a letter from someone who claims to be ‘psychic’ or from a religious order, and gives the impression that they are concerned about the consumer’s good health, wealth and happiness. They threaten harm or bad luck unless money is sent to them.

Computer Software Scams

Scammers who claim to be from a well-known software company contact consumers to say that there is a problem with their telephone or internet provider which will require remote access to resolve. A fee is often charged and the fraudsters may then have unlimited access to the computer to commit fraud and/or identity theft.

Printer Helpline Scam

Fraudsters pretend to offer assistance with the consumer's printer but really want remote access to their computer. This is an attempt to steal personal information and account details. If a consumer needs technical support for their printer they should only contact the manufacturer via the official contact details provided on their website. Consumers should be suspicious of helplines asking to take control of their computer to fix a printer problem.

Lottery & Prize Draw Scams

A consumer is told they have won a large amount of money in an international lottery, sweepstake or other prize draw. They may be asked to supply a copy of their password and account details. Once these have been provided, the fraudsters will then ask for various fees to be paid – e.g. taxes, legal fees, banking fees so they can release the non-existent winnings.

Parcel Delivery Scams

A postcard is put through the letterbox by a fake delivery company that claims it has a parcel for the homeowner and that delivery can be arranged by telephone. If the consumer calls, they are asked to pay a sum of money by credit or debit card and told that the (non-existent) package will be delivered the same day.

Online Job Scams

Fraudsters ask for money to write CVs or carry out police checks. In some instances, victims sign up for training courses that don't exist or the fraudsters pose as immigration lawyers or travel agents to offer a position internationally. Other types of job scams include fake telephone interviews for jobs that do not exist or money laundering from victims on a work-from-home basis.

Subscription Scams

This is where a consumer is invited to subscribe to a 'free' trial of a product and asked to provide account details to cover the fee for postage and packing. The small print terms and conditions will likely say that unless the subscription is cancelled at the end of the month, a monthly subscription fee will be charged. Scammers make their money by continuing to take a small (unnoticeable) amount every month for the 'free' subscription.

Copycat Government Scams

These involve websites designed to look like the official government websites, that charge a fee to process or renew official documents like passports or visas, which the consumer could do themselves for free or cheaper. Sometimes a fee is charged and the application is not processed at all.

HMRC Phishing Emails, Texts & Phone Tax Scams

In this instance scammers who pretend to be from HMRC contact the person and tell them that they are due a tax rebate. Often the victim is told that this is time limited and that it is vital that they make a claim as soon as possible. The fraudsters then attempt to obtain personal information including credit or debit card details. HMRC will never contact consumers via text or email informing them they are entitled to a tax rebate.

Romance Scams

This is where a person meets a scammer on line who, over time, convinces the person that they love them, even though they never meet face to face. The scammer will ask for money, often to pay off debts, or to buy a plane ticket to come and live with the person. Romance scams can go on for months and can be very emotionally upsetting for the victim.

Investment Scams

Fraudsters offer the chance to invest in things such as share sales, wine investments, land banking (practice of buying undeveloped land purely as an investment, with no specific plans for its development), precious stones, or carbon credits. Another emerging scam involves false claims about pension liberation, also known as 'pension loans'.

Unpaid Tax Scam

A fraudster will telephone a person and pretend to be from HMRC or the Court Service. They will say that the person owes money for tax or a fine. The fraudster will threaten that the person will be arrested if they do not pay. Often they will ask for the person to buy vouchers for iTunes or Google Play, to pay the money.

TOP TIPS

- Contacted out of the blue? Think – is it too good to be true?
- If you haven't bought a ticket – you can't win it.
- You should never have to pay anything to claim a prize, not even the cost of a stamp.
- Telephone scammers will often ask you to call another number, but then stay on the line. Check the number is genuine and call a friend first to ensure the line is clear.
- Your financial institution will never phone you to ask for your online password.
- Your financial institution will never come to your home to collect cash, your PIN, payment card or chequebook if you are a victim of fraud.
- Genuine computer firms do not make unwanted phone calls to help you fix your computer.
- Never click on links or files in emails unless you are sure of the source.
- If in doubt, don't reply. Bin it, delete it or hang up.
- Stop and think: Is the person genuine?
- Just because they sound professional and say they are from a financial institution, it doesn't mean they are.
- Ask for ID as bogus callers pretend they are from the council, a charity, or a gas, electricity or water supplier.
- Is the doorstep seller trying to sell something or pressurise you into buying something straight away?

NEVER, NEVER, NEVER TIPS

FINANCIAL INSTITUTIONS, THE PSNI, UTILITY COMPANIES, LAW ENFORCEMENT, HMRC, INTERNET AND TELECOM PROVIDERS, COMPUTER SOFTWARE PROVIDERS, LOTTERY ORGANISERS OR OTHER PUBLIC BODIES:

- Will **NEVER** ask for payment in vouchers.
- Will **NEVER** ask you to transfer money because your account is compromised.
- Will **NEVER** threaten you over the phone, by letter, or by email for not paying a fee.
- Will **NEVER** threaten arrest if payment is not made immediately.
- Will **NEVER** ask for money for a 'free gift', 'administration fee' or as part of a promotion.
- Will **NEVER** ask you to reveal your account security codes or online passwords in full.
- Will **NEVER** call out of the blue and ask for remote access to your computer or devices or ask you to download software.
- Will **NEVER** inform you about tax returns by email, text or voicemail.

If you think you have been the victim of a scam, call either the PSNI on 101 or Action Fraud on 0300 123 2040.

WHEN A TRADESPERSON OR STRANGER COME TO YOUR DOOR:

- **NEVER** answer the front door without ensuring the back door is locked.
- **NEVER** allow people into your house if you are not expecting them.
- **NEVER** give them access to parts of your house or property they do not need to be in.
- **NEVER** pay in cash or make cheques out to cash.
- **NEVER** let them take you to a financial institution to withdraw cash.
- **NEVER** accept anything other than a written quotation for any work.
- **NEVER** accept any increase to a price that has already been agreed on a written quotation.
- **NEVER** accept the word of a doorstep caller that your house needs "urgent repairs".

If you believe you have been scammed by a bogus caller call the PSNI on 101. In an emergency always use 999.

SCAM TEST

Stay four steps ahead of a scam by using this scam test:

- **S**eems too good to be true
- **C**ontacted out of the blue
- **A**sked for personal details
- **M**oney is requested

REPORTING SCAMS

You can report scams to either Action Fraud or to the PSNI on **101**. Always report bogus callers to the PSNI.

USEFUL CONTACTS

If you have been caught out by a scam or you think a friend or family member has been affected, contact Consumerline which can give advice and if necessary pass the matter onto the Trading Standards Service.

Consumerline
Tel: 0300 123 6262
Web: www.nidirect.gov.uk/consumerline

Report bogus callers to the PSNI
Tel: 101 (or 999 in an emergency)
Web: www.psni.police.uk

Report scams to Action Fraud
Tel: 0300 123 2040
Web: www.actionfraud.police.uk

Reduce unwanted mail and calls by registering with:

Mailing Preference Service
Tel: 020 7291 3310
Web: www.mpsonline.org.uk

Telephone Preference Service
Tel: 0345 070 0707
Web: www.tpsonline.org.uk

Quick Check
Tel: 101

NI Water Password Scheme
Tel: 03457 440088

NIE Password Scheme
Tel: 03457 643 643

For more help and information visit:
www.nidirect.gov.uk/scamwiseni and
www.facebook.com/scamwiseni

Activities


1. Poster Wheel Design


2. Scams Blockbuster


3. Scam Scenarios


4. Rap it


5. Bookmark - Scam Test


6. Your family needs you!!


7. Consumer Scenarios and Discussion


8. Role plays


9. Be a Scam Detective


10. Lights, Camera, ACTION!

11. Be a roving reporter for the day


12. Protecting your debit cards


13. Shopping safely online


14. Passwords


15. Scam Quiz


16. Spot the Scam

1. Poster Wheel Design

Activity One

Challenge:

Time:
20 minutes

Materials:

Wheel template, colouring pencils, scissors, crayons, markers and any additional crafts.

You have been asked to design a poster wheel on scams. You may wish to draw the template or this can be photocopied from the booklet. (Appendix 1).

The unit should be split into groups and each group should be given one/two portions of the wheel. Each group should decide on a key message on the topic of scams to include on the wheel. At the end of the activity the wheel portions should be joined together to create a full circle and different messages on scams.

You may wish to display your poster in your meeting place centre or community centre.

2. Scams Blockbuster

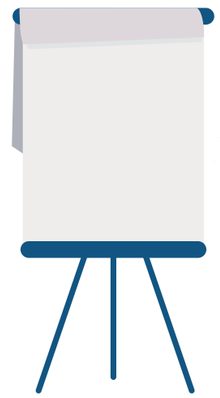
Activity Two

Challenge:

Time:
20 minutes

Materials:

Blockbuster board and markers.



As a unit, complete the following blockbuster activity by testing your knowledge on scams. Divide the unit into two teams. Use the blockbuster board as a template. This can be drawn out or photocopied from the booklet.

Each team needs to win a hexagon piece by answering the question matching the letter.

One team chooses to complete a line horizontally and the other vertically. The team making a line horizontally needs to answer one more question so they go first.

Working as a team, they must pick one of the hexagons. The host will ask the team the corresponding question for the letter they have chosen.

If they answer the question incorrectly, the opposing team has the chance to answer. If no one can answer the question, the host will need to come up with a new question for the same letter.

You can also 'block' the opposing team from advancing across the board, so choose your move wisely.

Activity Two

SCAMS BLOCKBUSTER

QUESTION AND ANSWERS

What **S** can be used to describe today's scams?
Answer: Sophisticated

What **M** is one of the ways people can be scammed?
Answer: Mail scam

What **P** is one of the methods through which people can be scammed?
Answer: Phone scam

What **D** is one of the ways people can be scammed?
Answer: Doorstep scam

What **O** is one of the methods through which people can be scammed?
Answer: Online scam

What **A** should you report scams to if you have been the victim of a scam?
Answer: Action Fraud

What **I** could be a scam in land, wine, precious stones or carbon credit?
Answer: Investment

What **F** is the number of steps in the scam test?
Answer: Four

What **C** refers to a scam involving a phone call claiming to be from a well known software company?
Answer: Computer scam

What **T** will a genuine financial institution never ask you to do if there has been suspected fraud on your account?
Answer: Transfer

What **L** could be a scam where you are told that you have won a large sum of money in something which you didn't buy a ticket for?
Answer: Lottery

What **N** is the name of the website where you can get more help and information on scams?
Answer: NI Direct

What **G** could be a scam where the scammers attempt to obtain personal and account details by advising that the participant can get free credits/currency or upgrades?
Answer: Gaming Scam

What **H** could be a scam claiming that you are due a tax rebate?
Answer: HMRC scam

What **Q** can consumers call to check if the caller to their door is genuine?
Answer: Quick Check

What **J** is a type of scam where fraudsters ask for money to write CVs or carry out police checks?
Answer: Job scam

What **V** is the type of scam where you receive a telephone call from a scammer claiming to be from your financial institution asking for personal information?
Answer: Vishing scam

What **U** is the type of call that you will never receive from genuine computer companies about your computer?
Answer: Unwanted phone calls

What **E** will HMRC never do to let you know that you are due a tax rebate?
Answer: Email

What **R** would you recommend people do with the Mailing and Telephone Preference Services?
Answer: Register

3. Scam Scenarios

Activity Three

Challenge:

Time:

15 minutes

Materials:

Paper, pens and props.

Here are five scam scenarios. Divide into groups and give each group a scenario. Each group will be asked to deliver these messages to the rest of the unit.

How will you decide to explain these types of scams and what advice would you give?

You can decide to do a presentation, design a poster, put on a play, use role-plays, write a poem, or design a catchphrase, motto or rap.

SCENARIOS

SCENARIO 1:

You are approached at home by someone claiming to be from a charity. They ask for a donation to a high profile cause. However, this charity is not registered and the caller is quite persistent that it is for a good cause.

SCENARIO 2:

You receive an email notification claiming that you have won £250 in a competition. However you don't recall entering a competition. To claim your prize, you have been asked to send a small fee within a particular time frame otherwise another winner will be chosen.

SCENARIO 3:

You and your friends are out shopping in Belfast and you see a designer hoodie for £125. Unfortunately you can't afford it so after some research, you find the same hoodie for £25 online. You have never used the website before and there is poor spelling in the content. The customer reviews are bad but the mega sale ends at midnight. Not one to pass on a bargain, you think you will go ahead and buy it. However, some of your friends don't think it is a good idea to buy the hoodie online.

SCENARIO 4:

You receive a phone call asking you to assist in a police investigation. The investigation is about corrupt staff in your financial institution where you have your account. The call handler asks you to visit your local branch and withdraw a specified sum of cash and take it home. A policeman later calls at your door to collect the money you withdrew at the request of the call handler.

SCENARIO 5:

You receive a phone call from your computer manufacturer stating that there is a problem with your computer and they need remote access to fix it. You don't want to lose all your photographs and are in a panic thinking that your computer is broken.

4. Rap It

Activity Four

Challenge:

Time:
15 minutes

Compose a rap on scams - you can choose to rap about one type of scam, several scams or the top tips!

This is a difficult challenge but are you up for it?

You can work in pairs or in small groups.

Good luck!!!

5. Bookmark - Scam Test

Activity Five

Challenge:

Time:
15 minutes

Colour in the scam test bookmark (Appendix 2) and present it to a member of your family that likes to read. You could even give the bookmark to a neighbour or another person that you know living in your community.

You are passing on important information to others which will help people protect themselves against scams. Why stop at one bookmark? Think of other people who could benefit from learning more about the scam test.

Tip:

You could be creative and attach a magnet to the back of the bookmark so the person can stick it to their fridge as a reminder on how to stay ahead of scams.

Materials:

Scissors, colouring pencils, crayons, markers.

6. Your Family Needs You!!

Activity Six

Challenges:

Time:
Variable

Challenge One:

With a parent/guardian, register with the Mailing Preference Service and Telephone Preference Service to reduce/stop unsolicited mail at the house, and unsolicited sales and marketing telephone calls. These are free services that should not be charged for by any company.

Either go onto the Mailing Preference Service website www.mpsonline.org.uk or call 020 7291 3310 to register your address.

Either go onto the Telephone Preference Service website www.tpsonline.org.uk or call 0345 070 0707 to register phone numbers.

Suggested Equipment:

Laptop/tablet/computer or mobile phone with access to the internet and access to a printer.

Challenge Two:

Inform two people of the Quick Check service. Homeowners can call the PSNI on 101 to check the identity of someone who says they are calling on behalf of a gas, electricity or water company. The Quick Check service can help consumers protect themselves from rogue traders/bogus callers.

Challenge Three:

Included in this information pack is a 'No Cold Calling' sticker. Your challenge is to decide who would be the best person to give a no cold calling sticker to so they can place it in their window to inform salespersons and traders to leave their property as it is a no cold calling zone.

Challenge Four:

Download and print the Nominated Neighbourhood scheme card from the PSNI's website. The Nominated Neighbourhood scheme means if an unrecognised caller calls at the property, the caller will be shown a card instructing them to contact their Nominated Neighbour, who will then try to check the caller's identity.

The scheme seeks the help of neighbours or relatives to check whether the unexpected callers are genuine.

For further information and to download the cards, visit the PSNI website.

www.psni.police.uk/news/campaigns/nominated-neighbour-scheme

Challenge Five:

Inform two people of the password scheme offered by NI Water and NIE Networks. The password scheme helps support vulnerable people living in our community and the pre-agreed password helps the home owner identify if the caller from NI Water or NIE Networks is genuine.

NI Water Tel: 03457 440088
NIE Tel: 03457 643 643

www.niwater.com/customer-care-register
www.nienetworks.co.uk/help-advice/vulnerable-customers

Challenge Six:

As a unit, become Friends Against Scams by completing the online learning.

The Friends Against Scams initiative has been created by the National Trading Standards Scams Team to tackle the lack of scam awareness by providing information about scams and those who fall victim to them. It aims to protect people and prevent them from becoming victims of scams by empowering communities to "Take a Stand Against Scams". It encourages people to talk about scams and share scam awareness messages more widely among their communities.

Friends Against Scams encourages people to take the knowledge learned and turn it into action. Anybody can join Friends Against Scams and make a difference in their own way. For more information and to become a Friend Against Scams, please visit the following website.

www.friendsagainstscams.org.uk

7. Consumer Scenarios And Discussion

Activity Seven

Challenge:

Here are four scam scenarios. Divide into groups and give each group a scenario to discuss and decide what to do. Discuss the groups' answers and invite others' views.

Time:

15 minutes

Scenario One:

Mrs Connor loves entering competitions through her weekly subscription gossip magazine. Out of the blue, Mrs Connor receives an exciting letter informing her that she has won £1 million in the lottery. In order to claim the prize fund, Mrs Connor has to provide her credit or debit card details to an address in Australia to pay £50 to cover the cost of posting the winnings.

GROUP TO DISCUSS

- Do you think Mrs Connor is entitled to claim the £1 million?

Scenario Two:

Paul receives a phone call from his financial institution informing him that his account has been compromised and that, as a matter of urgency, he needs to transfer his money into their head office account. They are very sympathetic and want to ensure that they are looking after their customer. They ask Paul to confirm his sort code and account number.

GROUP TO DISCUSS

- Discuss whether Paul should respond to the phone call.
- What advice could you offer to Paul?

Scenario Three

Kim receives a phone call from a computer company stating that her computer has a virus and that they are ringing her to fix the problem over the phone. Kim is worried that she is going to lose all her family photographs and will not be able to use her computer to go online.

GROUP TO DISCUSS

- What advice would you offer Kim?
- What should Kim do now?

Scenario Four

Sam receives an email link with information about a 70% discount on the newest smart phone. He is looking for a new phone and thinks this is a great bargain. However, he has never used this online retailer before and has never heard of them.

GROUP TO DISCUSS

- Discuss whether Sam should proceed with this 'bargain'
- What would you do in this situation?

SCENARIO ONE ANSWER

RIP UP THE LETTER AND DO NOT REPLY!

Under no circumstances should Mrs Connor reply to this scam letter, nor should she even think about providing her credit or debit card details to claim this so-called 'prize'. This is a scam and you should never have to pay anything to claim a prize, not even the cost of a stamp. The best advice to give Mrs Connor is to bin the letter. Consumers can contact the Mailing Preference Service to reduce/stop unsolicited mail at www.mpsonline.org.uk or call 020 7290 3310. This is a free service and no company should charge for this service.

SCENARIO TWO ANSWER

HANG UP IMMEDIATELY AND DO NOT ENGAGE WITH THIS CALLER!

Paul should immediately hang up the call as no financial institution will ever ask you for your PIN or your online password. It is easy to panic in situations like this but no financial institution will ask you to confirm your sort code and account number. Under no circumstances should Paul give any personal or account details or transfer money. In this instance Paul should hang up, call a friend to ensure the line is clear, and then call his financial institution on its official customer service number to discuss the call he has received. Consumers can contact the Telephone Preference Service to reduce/stop unsolicited sales and marketing telephone calls to their mobile or home number at www.tpsonline.org.uk or 0345 070 0707. This is a free service and no company should charge for this service.

SCENARIO THREE ANSWER

HANG UP IMMEDIATELY AND DO NOT ENGAGE WITH THIS CALL!

Genuine computer companies do not make unsolicited phone calls to help fix your computer. Under no circumstances should Kim give any personal or account details or transfer money. Consumers can contact the Telephone Preference Service to reduce/stop telephone calls at www.tpsonline.org.uk or 0345 070 0707. This is a free service and no company should charge for this service.

SCENARIO FOUR ANSWER

DELETE THE EMAIL AND DO NOT REPLY!

Never click on links or files in emails unless you are sure of the source. Do your research before buying from a website you have not used before. Check reviews or previous customers' feedback.

Check The Consumer Council website www.consumercouncil.org.uk and search for 'Your Guide to Shopping Safely Online' which provides guidelines and tips on how to stay safe when shopping online, protecting your rights and protecting your parcel deliveries.

8. Role Plays

Activity Eight

Challenge:

Time:

10 minutes

Role Play a telephone and/or doorstep scam scenario.

Create a scam scenario between a consumer and scammer, where the scammer is trying to take money from the consumer.

Divide into groups of two, with one playing the role of the consumer and the other playing the role of the scammer pretending to be from your financial institution, or someone calling to your property to sell you something. They can act out the scenario to the other members.

Tips/Advice:

- Stop and think: Is the person genuine?
- Just because they sound professional and say they are from the financial institution, doesn't mean they are.
- What scare tactics is the scammer using to persuade you to transfer your money?
- Telephone scammers will often ask you to call another number to prove they are from the organisation they claim to be from. However, they then stay on the line. Check the number is genuine and call a friend first to ensure the line is free.
- Your financial institution will never phone you to ask for your PIN or your online banking password.
- Your financial institution will never phone you to ask you to transfer money to a new account because of suspected fraud on your account.
- Your financial institution will never come to your home to collect cash, your PIN, payment card or chequebook if you are a victim of fraud.

Tips/Advice:

- Ask for ID as bogus callers can pretend they are from the council, a charity, or a gas, electricity or water supplier.
- Look out for a doorstep trader warning about your home needing repairs.
- Never hand over a cash deposit or go with the trader to the bank to take money out.
- Is the doorstep seller trying to sell something or pressurise you into buying something straight away?
- Stop and think: Don't make the decision to buy anything or sign up to anything on the doorstep.

9. Be a Scam Detective

Activity Nine

Challenge:

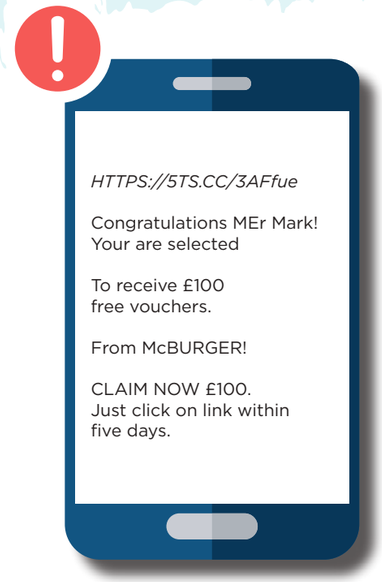
How to spot an email scam, mail scam and a text message scam.

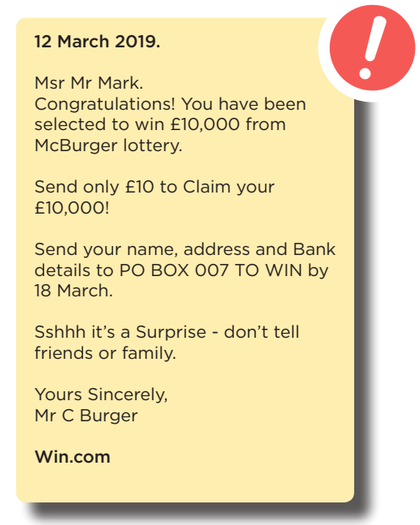
Time:

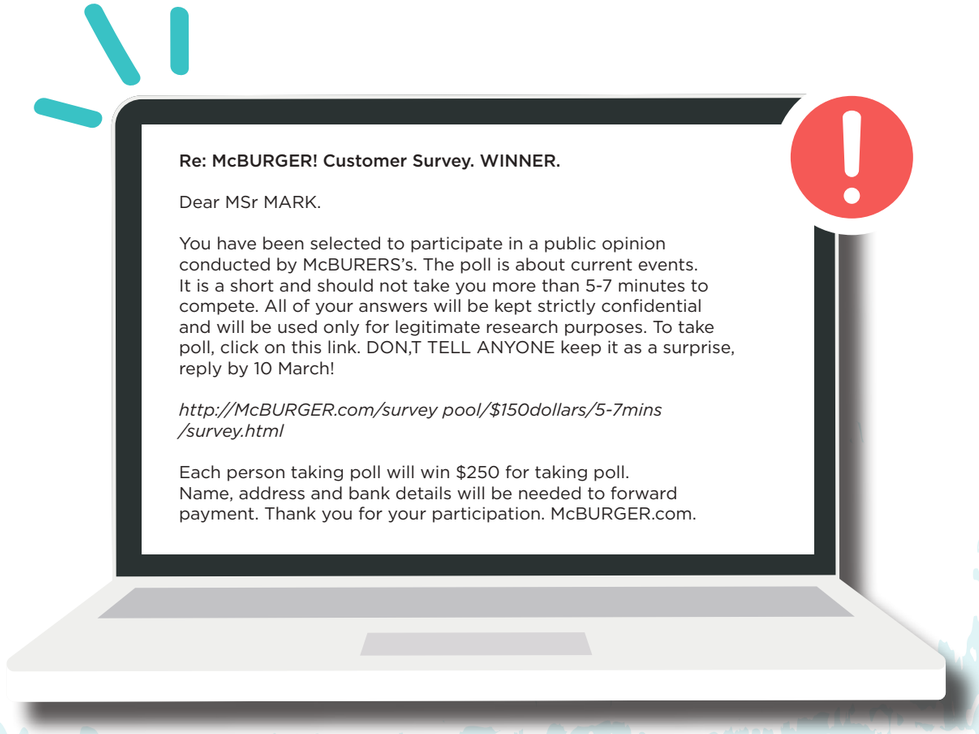
10 minutes

Read the following different types of scams and identify the different ways scammers try to trick you out of your money.

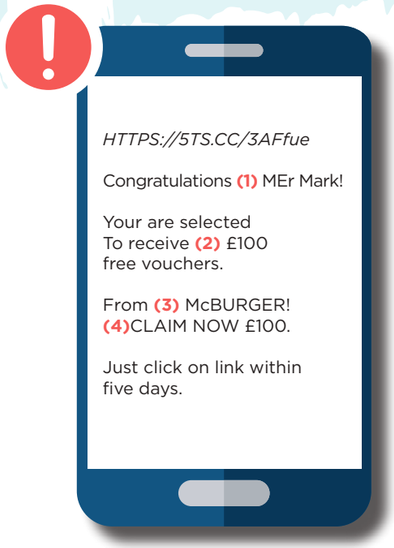
Divide into groups, with each group getting a copy of the three different scams. See how many things each group can identify before revealing the answers.







Activity Nine

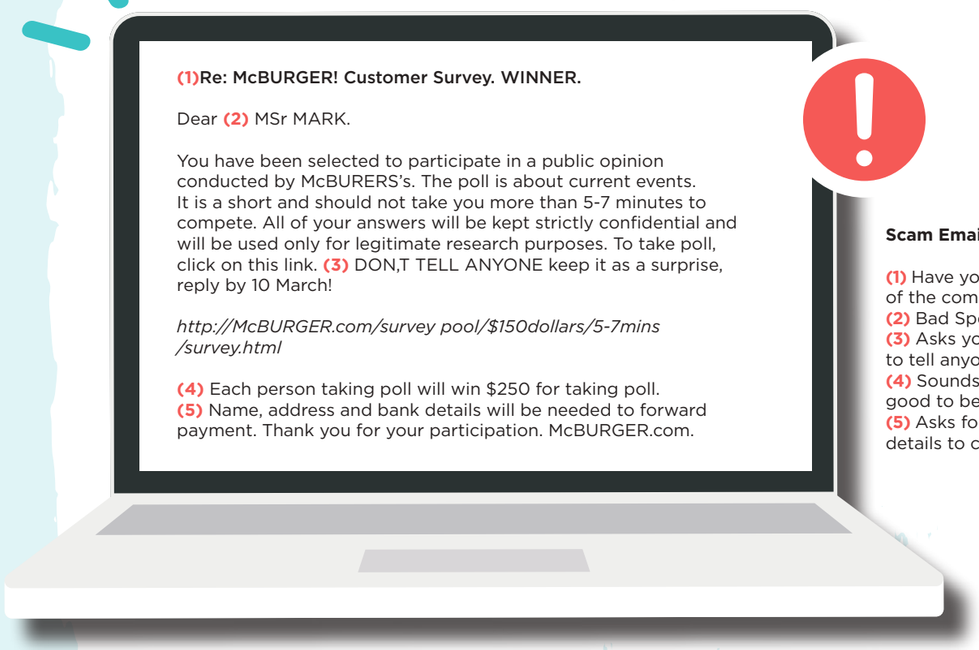


Scam Text Checklist

(1) Bad Spelling
(2) Have you entered the competition?
(3) Have you heard of the company?
(4) Puts you under pressure to reply quickly

Scam Letter Checklist

(1) Bad Spelling
(2) Prize is too good to be true
(3) Have you entered the competition?
(4) Asks you to send money to claim your prize
(5) Asks for personal details
(6) Uses a general address like a PO Box
(7) Puts you under pressure to reply quickly
(8) Asks you to keep it a secret
(9) Have you heard of the company?



Scam Email Checklist

(1) Have you heard of the company?
(2) Bad Spelling
(3) Asks you not to tell anyone
(4) Sounds too good to be true
(5) Asks for personal details to claim prize

10. Lights, Camera, ACTION!

Activity Ten

Challenge:

Make a three-minute advertisement about scams.

Divide into groups and decide together who your audience is and what your key messages are in order to make an advertisement to help consumers become more aware of scams.

You can use your mobile phone to record your advertisement and show it to other members. You may wish to share the advertisement on your organisation's website and social media platforms.

Time:

20 minutes

Tips/Advice:

Identify what key messages you want to get across.

Make the advertisement eye catching and engaging by thinking of a scenario to explain a particular scam, or you may wish to talk about several scam messages.

You may wish to use the 'Never, never, never' principles as part of your advertisement.

Suggested Equipment:

Laptop/tablet/ computer or mobile phone with a recording facility.

11. Be A Roving Reporter For The Day

Activity Eleven

Challenge:

You have been asked to write a front-page newspaper article on scams. You may wish to draw the newspaper template or this can be photocopied from the booklet. (Appendix 3).

Or you can decide to be a reporter for a local television station where you are interviewing a member of the public who has been scammed.

You may wish to become the television's news reader reporting on the different types of scams.

If you have written a front page newspaper article, show it to the rest of the unit.

Divide into groups of two and decide together who your audience is and what your key messages are to help consumers become more aware of scams. Each group will be asked to deliver these messages to the rest of the unit.

What scams will you decide to explain and what advice will you give?

You may wish to display your newspaper article in your meeting place hall or your community centre.

Materials:

Scissors, colouring pencils, crayons, pens, markers and paper.

12. Protecting Your Debit Cards

Activity Twelve

Challenge:

Have a group discussion about protecting your debit card and account from fraud.

Time:

10 minutes

Points for discussion

- Your financial institution will never phone to ask for your PIN or your online banking password;
- Your financial institution will never ask you to transfer money to a new account because of suspected fraud on your account;
- Your financial institution will never call at your home to collect cash, your PIN, payment card or chequebook;
- Do not reply to emails claiming to be from your financial institution asking for personal details or passwords;
- Do not write down your PIN code, online or telephone passwords;
- Do not give your PIN number to anyone. Your financial institution will never phone you to ask for your PIN or your online password;
- Always cover the keypad when typing PIN codes;
- Check to see if anything looks unusual or suspicious about the cash machine; and
- If the cash machine appears to have any attachments to the card slot, cash slot or keypad, do not use it. If possible, alert staff working in a nearby financial institution or call the PSNI on 101.

As part of the group discussion, ask everyone if there are things they would do differently from now on.

13. Shopping Safely Online

Activity Thirteen

Materials:

Two different colours of paper/card for each participant.

Challenge:

Time:

15 minutes

Have a group discussion about how to shop safely online by asking the following questions.

Using two different colours of paper/card, give each person one card of each colour. One of the cards will have the word ‘Yes’ on it and the other card the word ‘No’. Each person then has to hold up the card that shows the actions they currently take.

What do the results tell us about shopping safely online? As part of the group discussion, ask everyone if there are things they would do differently from now on.

1. Do you look out for the ‘https’ in the website address? (the ‘s’ stands for secure)
a. Yes
b. No

2. Do you check for the padlock icon in the browser bar before you make a payment?
a. Yes
b. No

3. If you are buying from an online retailer or a company you haven’t bought from before, do you research it first to check independent reviews of the business/product/service?
a. Yes
b. No

4. Do you click on web links sent to you in an email that directs you to a website?
a. Yes
b. No

5. Do you check for any delivery restrictions or additional costs for delivery to Northern Ireland before you are about to make a payment?
a. Yes
b. No

6. Do you use public Wi-Fi zones/hubs to buy goods online, for internet banking or to share personal information?
a. Yes
b. No

Points for discussion:

Observing what we do and don’t do can hopefully help us think of our future actions and stay safe when shopping online.

14. Passwords

Activity Fourteen

Challenge:

Time:

15 minutes

Have a group discussion on passwords that people use when online. Use the following prompt questions to help with the discussion, or have an interactive game by asking the questions.

Game:

Get everyone to stand in the middle of the floor and ask the following questions. The last person or people standing are password savvy!!!

START THE GAME WITH ‘SIT DOWN IF…’

- You use your name/age/birthday/pet’s name/best friend’s name/mum’s name/the word ‘password’ or the numbers ‘123’ to form your password?
- You don’t change your password on a regular basis?
- You don’t vary your passwords across different platforms and accounts?
- You don’t use a password with at least eight characters or a combination of numbers, upper and lower case letters and keyboard symbols?

Discussion Point One...

What do the results tell us about setting passwords? As part of the group discussion, ask everyone if there are things they would do differently from now on.

Ask the group to come up with some top tips on how to be more password savvy.

Discussion Point Two...

Have a group discussion on the need to limit what information/photos we put on different social media platforms. Dangerous people use fake profiles in an attempt to be-friend you. Scammers will try and take information such as your name, age, location or interests, and may ask for inappropriate photographs or in some instances, ask to private message you.

Ignore all emails, messages and requests and speak to a member of your family for further advice.

Ask the group to come up with some top tips on how to stay safe online on different social media platforms.

15. Scam Quiz

Activity Fifteen

Challenge:

Divide the group into pairs and give each pair a copy of the quiz to see how scam aware they are.

Time:

15 minutes

Discuss the correct answers together.

1. What organisations should you report scams and bogus callers to?

A. The PSNI and your local Council
B. Action Fraud and Citizens Advice
C. Action Fraud or the PSNI

2. Who is it ok to share your PIN with?

A. Your gran
B. Your best friend
C. Your financial institution
D. None of the above

3. You receive a text from your financial institution advising you that your account has been compromised. It refers you to a link asking you to enter your personal and account information. What should you do?

A. The text looks very official and you are worried about your account. You should update your account information using the link.
B. You should not reply to this text at all.

4. You are playing an online game and someone you befriended in the game wants to send you some credits so you can progress to the next level. They have asked for your credit or debit card details to process the credits so that you can progress with the game. What should you do?

A. Ignore the request, block the account and report it to Action Fraud.
B. As you are friends on this game, send them your credit or debit card details so you can progress to the next level.

5. Your friend sends you a request from a different profile on a social media site. What should you do?

A. Contact your friend another way and make sure the new account is genuine.
B. Accept their request. They probably made a new account.

6. You receive an email from your music store app stating that you are due a refund for a song purchase. They have sent a link so you can claim the refund.

A. You look forward to this refund from the music store app. Click on the link and fill in your details to receive this refund.
B. Ignore the email and report it to Action Fraud.

7. You see a ticket for a music artist you really like on a website. The tickets are usually £40, but this website is selling them for £15. What should you do?

A. Beware! If the price is too good to be true, it probably is. You could be buying a fake ticket.
B. Snap it up! That sounds like a great deal.

8. You receive an email from HMRC which explains that you are due a tax rebate. HMRC asks for your account details to process the tax rebate. What should you do?

A. Let them know your details. This looks legitimate.
B. HMRC will never email you to tell you that you are due a tax rebate. If in doubt, find the official number from another source and contact HMRC.

9. You receive an email about a competition saying that you have won a large sum of money and that you should reply straight away to claim. You have been asked to provide your credit or debit card details to release the money. What should you do?

A. Send your information straight away. You don't want to miss out on the prize.
B. If you haven't entered a competition - you can't win it. If the email has a sense of urgency and is asking for your credit or debit card details, there is a good chance it's a scam.

10. You receive a text message from your mobile phone network asking you to update your personal details. There's a link for you to use in the message. What should you do?

A. This message may be fake. Contact your mobile phone provider to discuss the text message before providing any personal information.
B. Update your information. You want to make sure you're being billed correctly.

Activity Fifteen

SCAM QUIZ ANSWERS

1. ANSWER C

You should report scams to Action Fraud on 0300 123 2040 or report bogus callers to the PSNI on 101.

2. ANSWER D

Whilst we are not saying that your gran or a friend would steal money from your account, it is good to get into the practice of not sharing your PIN with anyone, even people you trust. Your financial institution will never ask for your full PIN number. Your PIN is personal to you and only you.

3. ANSWER B

Your financial institution will never contact you asking you to transfer money if your account has been compromised. This includes asking for information about your PIN or online password.

4. ANSWER A

Under no circumstances should you provide your personal or account information to anyone, despite the attraction of progressing to the next level in a game.

5. ANSWER A

Some scammers will set up profiles on social media pretending to be one of your friends or family members. If they already have an account, make sure that the new one is genuine by contacting them another way.

6. ANSWER B

The best advice is to ignore these type of emails. These scammers pretend to be from a well known music store app and after clicking on the link, victims are prompted to enter additional personal information and credit or debit card details.

7. ANSWER A

Be aware of fake websites selling tickets, because you have no consumer rights if something goes wrong or the tickets turn out to be fake. You could end up losing your money.

8. ANSWER B

Under no circumstances should you reply to this type of email because HMRC will never contact you in an email about a refund of taxes.

9. ANSWER B

Scammers will try and entice you with a fabulous prize for a competition that you haven't even entered. Do not reply to these types of emails.

10. ANSWER A

Do not reply to this text message. The best advice is to ignore these types of text messages.

16. Spot The Scam

Activity Sixteen

Challenge:

How many different types of scams can you spot?

Time:

10 minutes

Friends Against Scams Spot the signs - House task

Give each person the house task sheet and ask them to find all the signs in the house.

Ask participants to mark all the signs they can see.

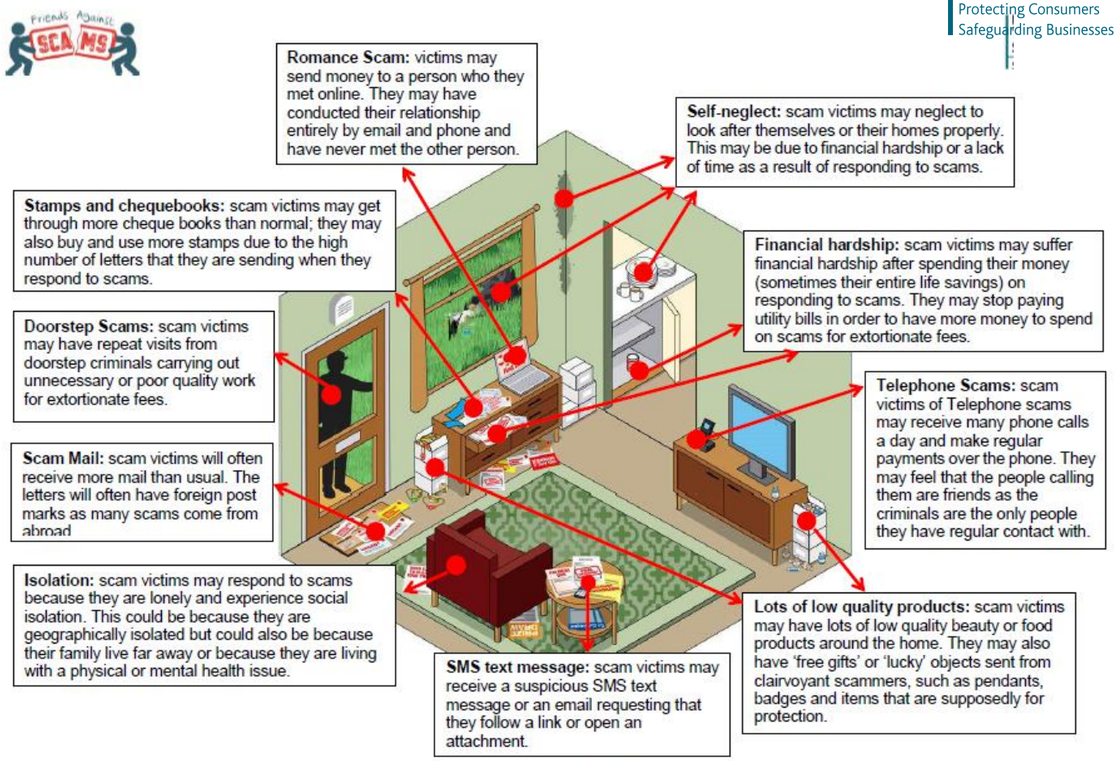
Go through the answers by asking them to shout out what signs they have found and why they think this might be a sign of a scam.

Go through any remaining answers and have a group discussion about the different types of scams.

Spot The Signs

Spot The Signs Answers

NATIONAL TRADING STANDARDS
Protecting Consumers
Safeguarding Businesses



#FriendsAgainstScams
www.friendsagainstscams.org.uk

EVALUATION

Tell us what you thought of the Scamwise Champion activities.

1. AFTER COMPLETING THE ACTIVITIES, HOW WOULD YOU RATE THE PARTICIPANTS' KNOWLEDGE OF SCAMS?

No Understanding — Excellent Understanding

1 2 3 4 5

2. HOW WOULD YOU RATE THE ACTIVITIES?

Poor — Satisfactory — Good — Very Good — Excellent

1 2 3 4 5

3. DO YOU HAVE ANY RECOMMENDATIONS TO IMPROVE THE ACTIVITIES?

4. ARE THERE ANY ADDITIONAL COMMENTS YOU WOULD LIKE TO MAKE?

Please complete and return by post or email to your organisation, along with the badge and certificate order form.

BADGE AND CERTIFICATE ORDER FORM

Please send me ___ badges

Please send me ___ certificates
to be delivered to:

Name of unit: _____

Leader's name: _____

Leader's address: _____

_____

RESOURCES

If you would like any of the following resources and information leaflets, please contact The Consumer Council on 0800 121 6022 or email us at contact@consumercouncil.org.uk

	QUANTITY
THE LITTLE BOOK OF BIG SCAMS	_____
SCAMS – KNOW THE SIGNS... TO STOP THE CRIME	_____
HOW TO SPOT SCAM MAIL	_____
SCAM TEST	_____
COLD CALLING STICKERS	_____
YOUR GUIDE TO SHOPPING SAFELY ONLINE	_____

Name of unit: _____

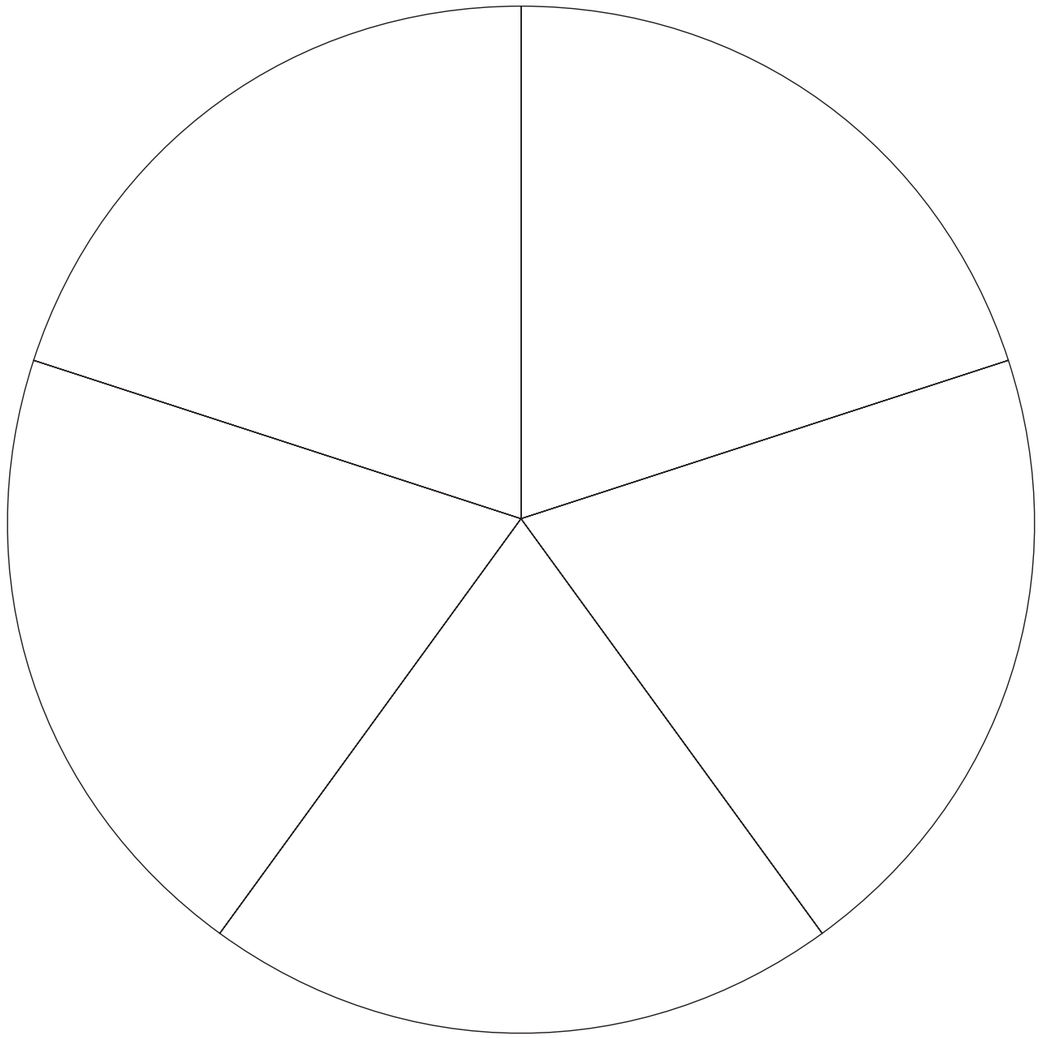
Leader's name: _____

Leader's address: _____

_____

APPENDIX 1

Poster Wheel Design



APPENDIX 2

Bookmark - Scam Test

If you can sp●t a scam, you can st●p a scam

Stay 4 steps ahead of a scam by using this **scam test**

- **S**eems too good to be true
- **C**ontacted out of the blue
- **A**sked for personal details
- **M**oney is requested

ScamwiseNI

nidirect.gov.uk/scamwiseni

scamwiseNI PARTNERSHIP

APPENDIX 3

Newspaper Template

DATE:

INSERT YOUR HEADLINE HERE

PICTURE:

ARTICLE HEADLINE

MAIN ARTICLE TEXT:

SCAMWISE LOGO:

The Consumer Council has produced this resource on behalf of the ScamwiseNI partnership. The ScamwiseNI partnership is made up of more than 30 statutory, commercial, voluntary, community, charitable and uniformed youth organisations.

The ScamwiseNI partnership would like to thank all partner organisations for their contribution towards the development of this resource. The ScamwiseNI partnership would also like to thank the uniformed youth organisations for supporting this initiative.

For more help and information visit
www.nidirect.gov.uk/scamwiseni and www.facebook.com/scamwiseni