BOSS

Be Online Stay Safe

Media literacy online safety

Name:

Leeds
Older
People's
Forum

Samantha Haggart Digital Coordinator

Leeds Older People's Forum is a registered company in England and Wales (#CE023712) and a registered charity (#1191030)

Exercise 1: How strong are your passwords?

Strong passwords:

- Combine upper and lower-case letters, numbers, and special characters.
- Ensure uniqueness for each account.Avoid being easily guessable.
- Using strong passwords is crucial for maintaining the security of your online accounts.

Put a tick next to the strong passwords below and put an X next to the weak passwords

Password123		**123abc**	
Samsung12		**Rainbows12**	
123456		**Letmein**	
Helen1970		**Guest12**	
Phonecuppen13!		**Bookhookmouse12**	

Exercise 3: Visit “Password Monster website”

Type in different passwords and see how long they would take to crack by a hacker. You don’t have to use your own, you can use similar ones.

Do you need to change your passwords?

Spotting Misinformation

Misinformation refers to false stories or rumours that spread rapidly on the internet. It occurs when individuals share inaccurate information, whether unintentionally or intentionally. Just as in real life, it's crucial to exercise caution regarding what you believe or share online and to verify suspicious information. Misinformation can resemble 'fake news' or rumours, it is important to use critical thinking and rely on credible sources to distinguish between fact and fiction.

How to spot misinformation online

Use multiple sources: Always check information from more than one place. If different websites or experts say the same thing, it's likely accurate

Check the date: Make sure the information is recent. Old information might not be right anymore

Beware of ‘red flags’: Be careful of flashy, exaggerated headlines or websites. They might not be honest. Have you heard of ‘click bait’ headlines?

Think carefully: Use your own judgement. If something sounds unbelievable or strange, it might be wrong

Check the Contact Page: Look for a way to contact the website or the people behind it. Real websites usually have a "Contact Us" or "About Us" page

Be wary of images and videos: Be cautious about pictures and videos, could they be fake?

Believe in Your Instincts: If something feels too good or too strange to be true, be cautious and check more

Artificial Intelligence

Artificial Intelligence (AI) is technology that enables computers to perform tasks that usually require human intelligence. It's crucial in modern tech for things like voice recognition and self-driving cars, making machines more capable and independent.

Did you know…?

1. Smartphones use AI technology to improve camera quality and take better photos
2. Social media platforms use AI to personalise the content you see in your feed
3. AI is commonly used in weather forecasting to make accurate predictions
4. Smart thermostats use AI to learn your temperature preferences and adjust them automatically
5. Self-checkout machines at grocery stores use AI to scan and calculate the total cost of items
6. Modern cars often employ AI for features like adaptive cruise control and lane-keeping assistance
7. AI is used in medical diagnostics to help identify diseases based on medical images

Discussion questions:

1. Do you have AI devices in your home?

2. Is AI good or a threat, what do you think?

Potential threats from artificial intelligence:

Misinformation and Deepfakes: AI can be used to create convincing fake content, such as videos, news articles, which may spread false information or impersonate trusted individuals or organisations.

Phishing and scams: Cybercriminals can employ AI to write sophisticated and personalised phishing emails and messages, making it harder to distinguish them from legitimate communications.

Identity theft: AI-powered attacks can mimic someone's voice or even generate forged identity documents, making it easier for criminals to steal personal information.

Automated fraud: Fraudsters can use AI to automate fraudulent activities, such as fake reviews on e-commerce websites or automated customer service bots for scam calls.

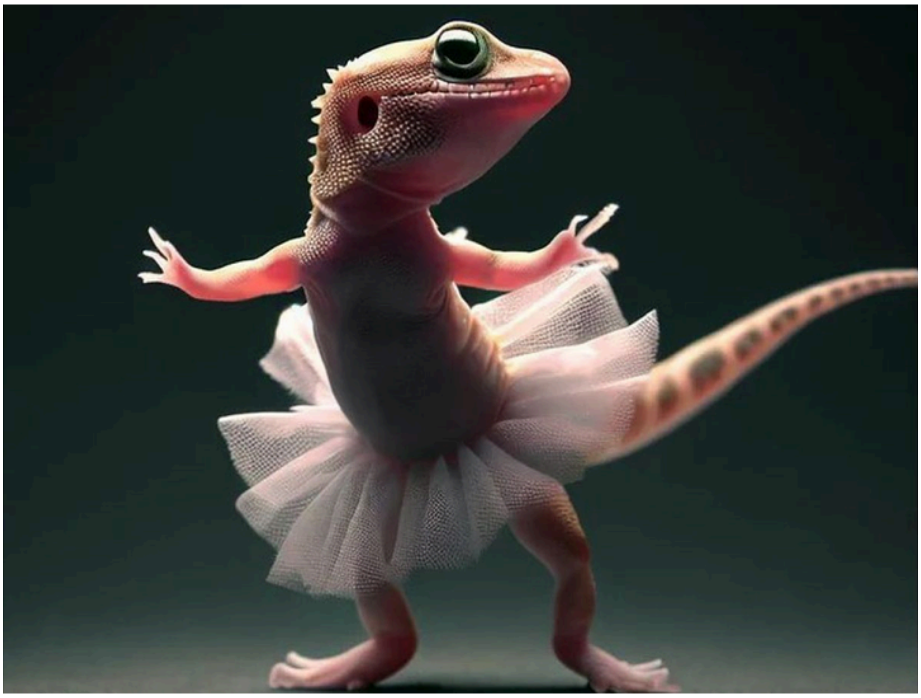
Voice impersonation: AI technology can learn and replicate someone's voice, making it possible for cybercriminals to impersonate individuals over the phone or through voice-based authentication systems, potentially leading to voice identity theft and fraud

Have you heard of any of the above scams?

Notes:

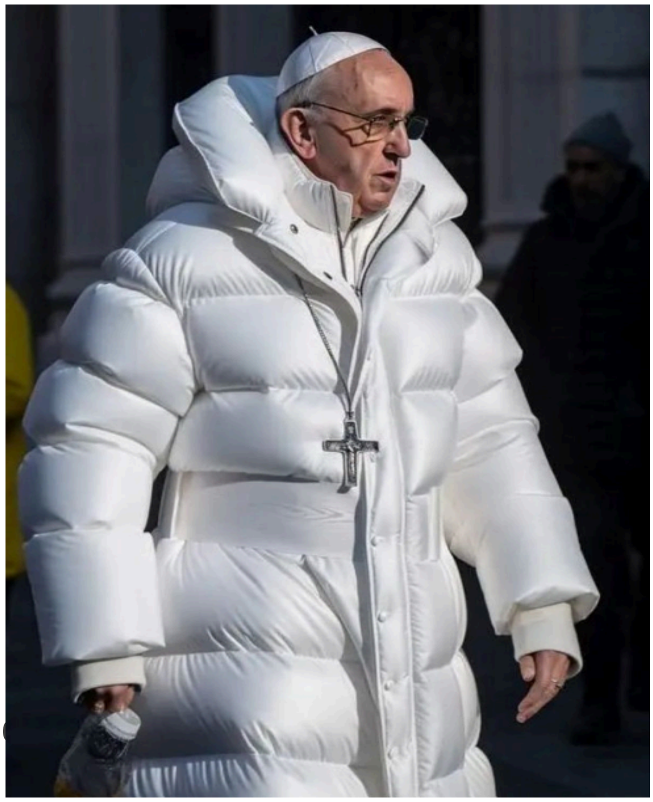
Can you believe what you see?

Take a look at these photos recently posted on Twitter



(Photos from Twitter)

This adorable lizard in a tutu is a mind-blowing fake



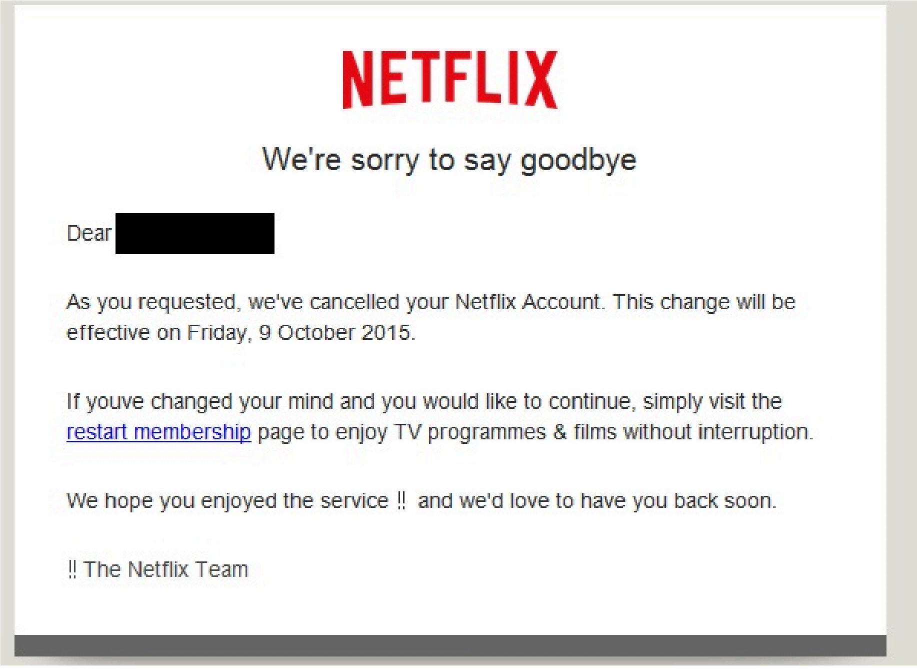
Pope out with a puffer jacket and water bottle.

Lots of people thought these were real and shared them with friends.

What would you have thought if a
a friend shared with you?

Common scams and how to protect yourself

1. Phishing emails/scam calls: Older individuals may receive emails or calls claiming to be from banks, government agencies, or even family members in distress. Always verify the legitimacy of such communication by contacting the company directly using a trusted phone number, not the one the caller gives you



NETFLIX

We're sorry to say goodbye

Dear [redacted]

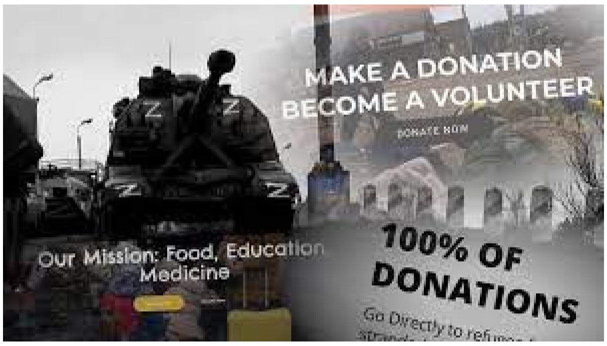
As you requested, we've cancelled your Netflix Account. This change will be effective on Friday, 9 October 2015.

If youve changed your mind and you would like to continue, simply visit the restart membership page to enjoy TV programmes & films without interruption.

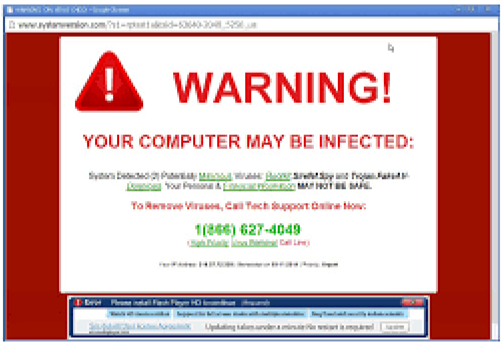
We hope you enjoyed the service ‼ and we'd love to have you back soon.

‼ The Netflix Team

2. Fake charities: Scammers often pose as charitable organisations, especially during times of crisis. Only donate to charities you know.



3.Tech support scams: Fraudsters may call claiming to be from a tech support team telling you your device is broken or hacked. Remember a scammer can't tell if your phone device has a problem. You would seek help, if needed, from a trusted professional.



WARNING!

YOUR COMPUTER MAY BE INFECTED:

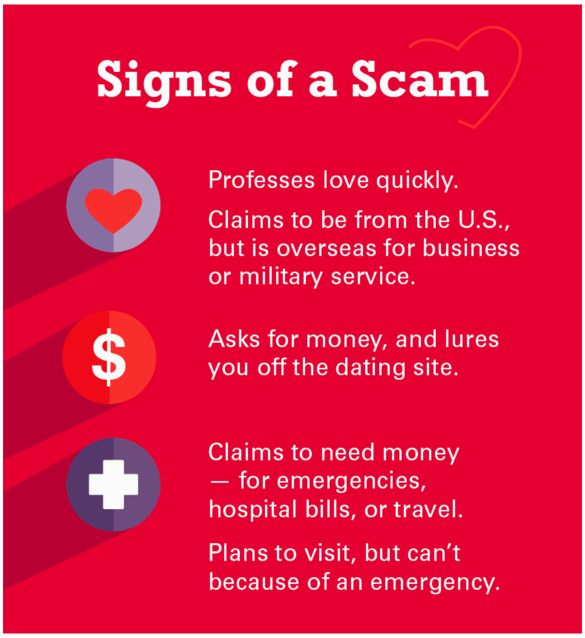
System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

(High Priority Virus Removal Call Line)

4. Romance scams: Individuals may be targeted on dating websites. Be aware of online relationships, especially if the other party starts asking for money or personal information.



Signs of a Scam

Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.

Asks for money, and lures you off the dating site.

Claims to need money — for emergencies, hospital bills, or travel.

Plans to visit, but can't because of an emergency.

5. Investment fraud: Always check unsolicited investment opportunities promising high returns. Consult with a financial advisor before making any significant financial decisions.

Over £63m was lost by victims of investment fraud who made reference to a social media platform in their report.

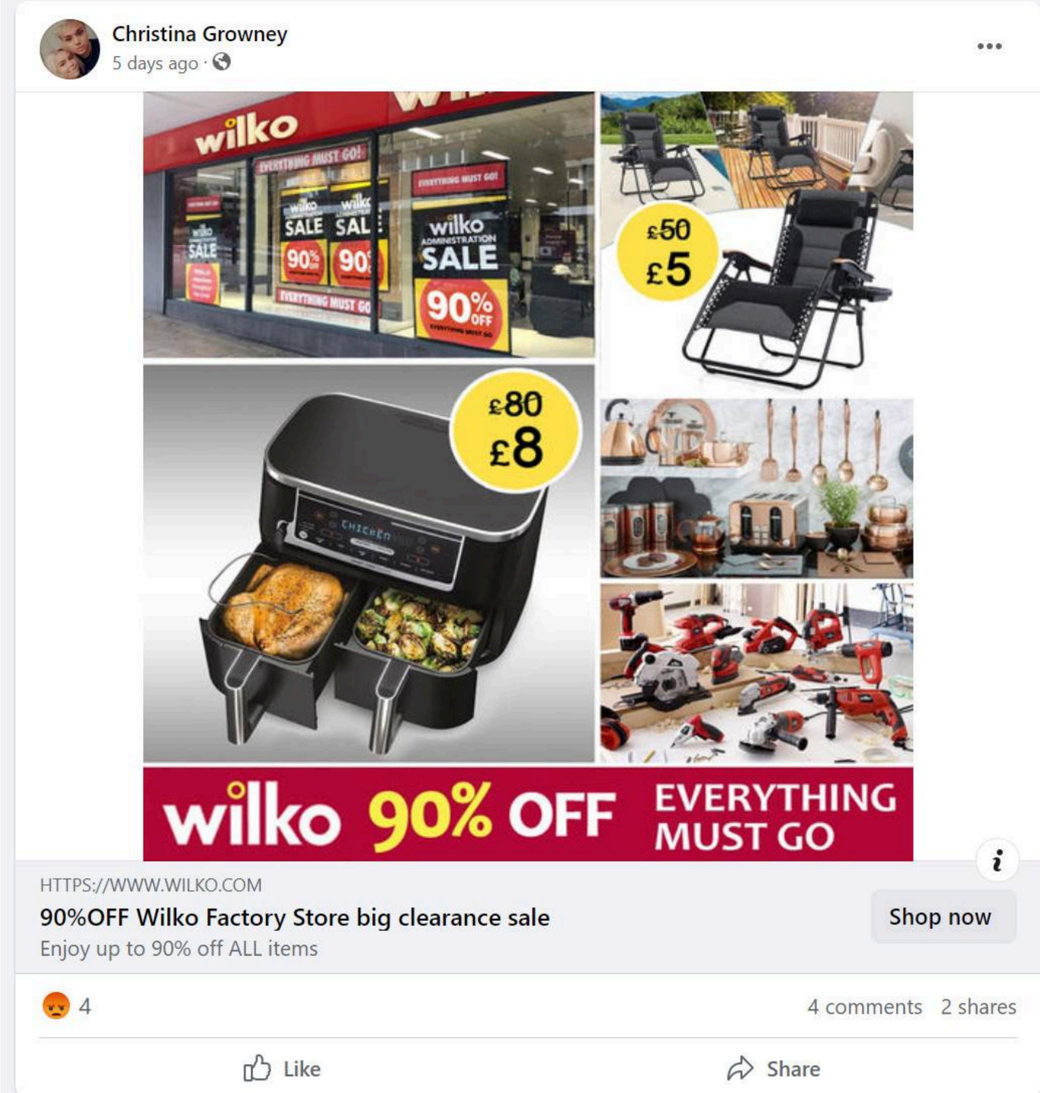
6. Door-to-door scams: Scammers may show up at your doorstep posing as utility workers or contractors. Always verify identities and contact the relevant companies directly to confirm the visit. Remember if you are not expecting anyone you do not have to open the door. Or get a chain fitted on your door.

TAKE A STAND AGAINST
DOORSTEP SCAMS
PROTECT YOURSELF FROM DOORSTEP CRIME.
IF YOU'RE NOT SURE DON'T OPEN THE DOOR.

7. Lottery or prize scams: Legitimate lotteries and contests don't require payment upfront. If it sounds too good to be true, it probably is.

8. Identity theft: Regularly check bank statements and credit reports for any suspicious activity. Using strong, unique passwords and being cautious with personal information can help prevent identity theft

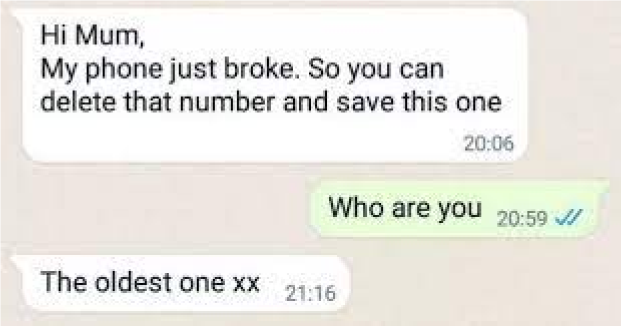
9. Social media scams: Be cautious about accepting friend requests or messages from unknown individuals. Scammers may use fake profiles to build trust and gather personal information. Also be aware of fake adverts like the one below offering huge discounts.



Christina Growney
5 days ago ·

HTTPS://WWW.WILKO.COM
90%OFF Wilko Factory Store big clearance sale
Enjoy up to 90% off ALL items

10. WhatsApp impersonation scams: If you receive messages on WhatsApp claiming to be from a relative in distress, requesting urgent financial assistance. Always check by calling the family member on the number you have or checking with other relatives before sending any money.



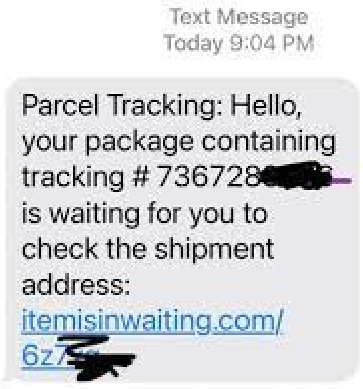
Hi Mum,
My phone just broke. So you can delete that number and save this one 20:06

Who are you 20:59

The oldest one xx 21:16

Messaging scams have been reported to Action Fraud 1,235 times between 3 February and 21 June this year and have cost people a total of £1.5million. (Source: This is Money)

11. Text message scams (Parcel/package scam): Scammers may send text messages claiming you have an undelivered parcel and provide a link for "redelivery" or payment. Do not click on suspicious links and confirm with the delivery company directly if you are unsure



Text Message
Today 9:04 PM

Parcel Tracking: Hello, your package containing tracking # 736728[redacted] is waiting for you to check the shipment address: itemisinwaiting.com/6z7[redacted]

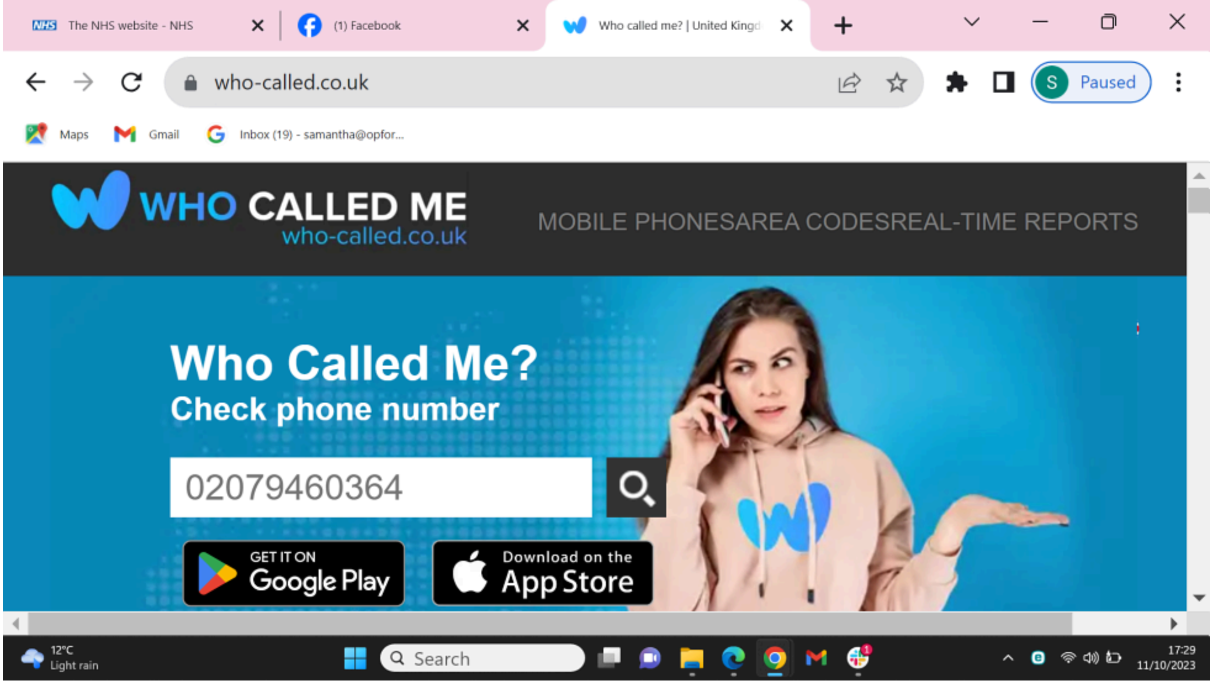
These scams often play on emotions or a sense of urgency. It is crucial to pause, take a step back, verify the information independently, and not rush into any decisions.

Who Called me? How to check scam telephone numbers

Telephone scams are becoming increasingly common, and it's essential to protect yourself from potential fraudsters. 'Who Called Me?' is a useful website that can help you check if a telephone number is associated with a scam. This handout provides step-by-step instructions on how to use the Who Called Me website effectively.

Step 1: Access the Who Called Me? website
Open your Google or Safari and go to the Who Called Me? website

Step 2: Enter the suspicious telephone number
In the search bar at the top of the page, enter the telephone number you want to check. Make sure to input the full number, including the area code.



Step 3: Click on the 'Search' magnifying button to begin the look-up process.

Step 4: Review the results
Who Called Me? will display information related to the telephone number you entered. The results may include details such as the number's type (e.g. scam, telemarketing, or legitimate), user-reported comments, and the number's overall rating based on user feedback.

Step 5: Examine user comments and ratings
Scroll down to see user-contributed comments and feedback.
These comments often provide valuable insights into the nature of the call, whether it's a scam, telemarketing, or a legitimate caller.

Step 6: Make an informed decision
Based on the information provided by Who Called Me? and user comments, make an informed decision about whether the telephone number is associated with a scam.
If the feedback and comments suggest a scam, exercise caution and consider blocking the number.

Additional Tips:

- Be cautious when answering calls from unknown numbers, especially if you suspect they might be scams.
- Consider registering your number on the National Do Not Call Registry (https://www.donotcall.gov/) to reduce unwanted calls.

Conclusion

Who Called Me? is a valuable resource for identifying potentially fraudulent telephone numbers and protecting yourself from scams. By following these steps and using the information provided on the website, you can make more informed decisions about the calls you receive and take steps to safeguard your personal information and finances.

Notes:

How to block scam emails, and text messages

Blocking scam email addresses can be an effective way to prevent further communication from scam companies. The exact steps to block email addresses can vary depending on the email service or client you are using. Here are some general guidelines:

How to Block emails
Find the email address from which the scam emails are being sent. This is usually displayed in the "From" field .

Gmail
Open the email, click on the three vertical dots (‘More options’) next to the reply button, and select ‘Block [sender's name]’.

Outlook
Right-click on the email, choose ‘Junk’, and then click on ‘Block Sender’.

Yahoo Mail
Open the email, click on the ‘More’ option (represented by three dots) near the top-right corner, and select ‘Block Senders’.

Write down how to block emails on your device below

How do you block scam/spam text messages on Android and iPhone?

Blocking spam text messages on Android and iPhone devices can help prevent further messages from a scam company. The steps to block text messages may vary slightly depending on the specific devicen. Here's a general guide for both Android and iPhone:

Blocking scam text messages on Android:

- Open the Messages app
- Locate the scam message
- Long-press the message: press and hold the scam message until a menu appears.
- Block the sender: look for an option like ‘Block’ or ‘Block number in the menu. Tap on it to block the sender's phone number.

Confirm the block: you may be prompted to confirm the action. Confirm the block to prevent further text messages from that specific number.

Note
The exact steps and options may vary depending on the Android device and messaging app you are using. If you are using a third-party messaging app, the blocking process might be different. Refer to the app's settings or documentation for specific instructions.

Write down instructions below for your phone:

Blocking scam/spam text messages on iPhone:

- Open the Messages app
- Locate the scam message
- Tap the "i" icon:
- Scroll down to find the option ‘Block this Caller’ and tap on it.
- A pop-up will appear asking for confirmation. Confirm the block to prevent further text messages from that specific number.

Note
On iPhones, you can also block numbers directly from the Phone app. Open the Phone app, go to the ‘Recents’ or ‘Contacts’ tab, find the number you want to block, tap the ‘i’ icon, and select ‘Block this Caller’.

By following these steps, you can block scam text messages on your Android or iPhone device.

Remember, scammers may use different phone numbers or tactics, so it's important to remain vigilant and not solely rely on blocking numbers.

Glossary of words

Name	Definition
Strong password	Passwords that include a combination of upper and lower-case letters, numbers, and special characters, are long, unique to each account, and not easily guessable.
Misinformation	False or misleading information shared online, resembling rumours or false stories that can spread quickly on the internet.
Fact checking	A method to verify the accuracy of information, essential for combating misinformation
Artificial Intelligence (AI)	Technology that enables computers to perform tasks requiring human intelligence, such as voice recognition and self-driving cars.
Identity theft	Unauthorised use of someone's personal information, often facilitated by AI-powered attacks.
Phishing	Cybercriminals using AI to craft sophisticated and personalised emails or messages to deceive individuals.
Deep fake	AI-generated fake content, such as videos and articles, that may spread false information or impersonate trusted individuals.
Smart devices	Devices enhanced with AI technology, like smartphones and smart thermostats, provide added convenience and functionality.
Disinformation	Deliberately false information spread with the intent to deceive.
Misleading headlines	Headlines that may not accurately reflect the content of the accompanying article, leading to potential misunderstandings.
Click bait	Sensationalised or misleading online content designed to attract clicks and views.