Information NOW

Information for people in Newcastle upon Tyne

Cyber crime, online fraud and scams

Online or cyber crime is carried out on the internet. Be wary of any request for your personal information or bank details to protect yourself and your data.

If in doubt, don't click any links in text messages or emails that you receive, even if they look genuine. Don't give your passwords or bank details to anyone. If you receive an unexpected phone call you can hang up, look up the public telephone number for the organisation and call them yourself.

Read on for more information about online crime, how to spot it and what to do if you're targeted.

Scams on your doorstep

Read more on our **fraud and scams article.**

If someone knocks at your door: **if you are not sure – don't open the door.** If you know and trust your neighbour you can ask a neighbour for help. Or contact **CityLife line** for help. This is coordinated jointly by the Council with the statutory sector. This Citylife Line is a safe way to get your essential supplies – food, prescriptions and hygiene products.

You will not be asked to pay for a Covid19 vaccine. Vaccinations may be arranged with your GP or **through the GOV.UK website**

Cyber crime

North East Regional Cyber Crime Unit (NERCCU) works to protect our communities from serious and organised crime. Their website has specialist advice and guidance around cyber crime prevention whether you're a business, organisation or individual. They have free training sessions and online resources. They can help you if you've become a victim of online crime. **Read more on how to report an online crime here.**

There are different types of cyber crimes that are referred to as:

- **Phising scams:** where an attacker tries to trick you into clicking a bad link that will download malware, or take you to a fake website. It can take place by email or text message. The attacker is trying to get you to reveal personal or sensitive information, such as passwords, email addresses, bank details. All of which can be used to steal money or sell your personal data on to other criminals.

- **Vishing scams:** or ‘voice phishing’ is where a fraudster uses recorded voice messages, phone calls, online messaging or text messages to try to trick you into giving them your financial information like your PIN number, card or bank details and Digipass code. This data could also be used to steal identities or sell your personal data onto other criminals
- **Smishing** scams: is a form of phishing but sent via text. Phone providers allow you to **report suspicious text messages** for free. If you forward a text, your provider can investigate the origin of the text and take action, if found to be malicious.
- **Quishing** is a type of phishing attack that uses QR codes to trick people into visiting a malicious website or downloading a virus-filled document.

Don’t enter your personal bank account details and don’t click on phishing emails that may embed malware software.

Five to Stop Fraud **Take Five is a national campaign** offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

Stay safe on the internet

The NCSC has launched a **Cyber Aware campaign** to help the public stay secure on the internet. Read their top tips to tackle and protect you from the growing cyber threats. Included in this is a new suspicious email reporting service**,** helping the public to fight back against phishing. To find out more about this new service and for tips on the 6 most essential protective behaviours, visit their website.

If the worst happens and you are a victim of a scam or if you think you have been targeted contact **Action Fraud – report Fraud & Internet Crime**

Online bullying, stalking and harassment

Cyber stalking is online harassment and similar to cyberbullying it can be carried out by email, text message and social media post.

How to report an online crime.

Protecting your image online

Revenge porn helpline supports adult victims of intimate image abuse who live in the UK. They provide advice, guidance and support with helping to remove intimate content which has been non-consensually shared online.

Stop NCII.org is a free tool designed to support victims of Non-Consensual Intimate Image (NCII) abuse

How to spot an online scam

1. **Check the sender of the email is who they say they are.** Read it slowly. Often the email sender may be misspelt slightly to trick you into thinking it's your bank, email provider, HMRC, internet provider, Microsoft, a company you've bought something from like Amazon, Ebay or Apple
2. **Look out for spelling errors or incorrect grammar.** A real company is usually very careful with how they write emails.
3. **Does the email or text or phone ask for immediate action?** Be very wary if so. You do not need to respond immediately
4. **Check the link is genuine before you click it.** Hover over any links when using a desktop computer, or press and hold the link on your phone/tablet to see where the link is trying to take you. If it doesn't match or it's an unknown address, do not click the link

Report phishing and scams

Be wary of emails or text messages that ask you to click a link, open an attachment, log in to any system, give your personal details or to view or download files.

If you receive a phishing email you can report it. Forward phishing emails to **report@phishing.gov.uk.** Do not click any links or open any attachments. If you receive a phishing or scam email at work, follow any of your organisation's IT policies too.

If you have been a victim of online crime report it to **Action Fraud**

Scams to be aware of

Fake company emails, texts or calls

Scammers may try to contact you pretending to be a company who you're normally in contact with. Hoping that you click on the link they send or open an attachment. They are trying to install a virus or spyware on your device to track your activity and take your log in details. Or take you to a fake website and get you to give them your personal information.

Be very wary of any emails, calls or texts that you are not expecting and follow the tips above on how to stay safe. Some examples of companies that scammers may pretend to be:

- **Attached files:** don't open any attachments sent with an email that you were not expecting. It may look like an invoice, image, bill or credit note
- **Your phone company:** BT, 02, EE, Virgin, Sky,
- **Parcel delivery company DPD, Hermes or Royal Mail** asking you to pay for a postage costs or to confirm delivery of your parcel
- **HMRC:** to pretend that you have an unpaid tax bill, refund, or threaten further action
- **Pensions or National Insurance:** to pretend that you have an unpaid tax bill, refund, or threaten further action
- **Any online shopping provider** may contact you about a fake unpaid bill, refund, special offer or free gifts. Such as Amazon, supermarkets,
- **Your email provider:** such as Hotmail, Office Outlook, Yahoo, BT Internet, Sky, Apple, iPhone

- **Your energy provider:** For example, British Gas or Shell. They may try to contact you about switching suppliers, outstanding payments or threaten further action
- **Your bank:** will never ask for your password or the 3 digit security number on the back of your card. If contacted, don't click any links or give your details over the phone. Visit to their website directly and contact them yourself.
- **NHS Coronavirus vaccinations:** Do not follow or click on suspicious text messages with a link to a booking site which mimics an NHS page. Never give your personal details including bank account numbers.
- **NHS Test and Trace service:** Fake text messages may arrive asking you to click a link to complete your personal details, saying you've been in close contact with someone who has tested positive for corona virus. Texts are now more for information, for close contacts. If you have registered a positive covid test result you will be contacted by test and trace. Follow the tips above about **how to check that a link is genuine**
- **Fake charity appeals and crowdfunders:** There are many worthy causes to support at this time, but be sure you are sending your money to the right organisation and not a fraudulent account. Check the **Charities Commission website.** Visit **Prevent Charity Fraud** for help and support to keep your charity safe.
- **Travel companies** such as Easyjet customer details have been compromised – beware of any unexpected communications from them
- **TV Licensing:** Send their emails from donotreply@tvlicensing.co.uk . They always include your name in their emails. They will never:

  - email you to tell you that you're entitled to a refund
  - offer you a discounted TV Licence
  - ask for your card details to take a missed payment before they asked you to sign in and identify yourself using your licence number, surname and postcode
  - ask for your mother's maiden name
  - ask for your date of birth (unless you're 74 or over and applying for a free TV Licence)
  - **Read more about what to look out for from TV License scams on their website.**

- **Offers that are too good to be true:** Be suspicious of free gifts, discounts or investments that sound too good to be true. Check the company is on the **FCA register.**
- **WhatsApp Scams:** You may be contacted by someone pretending to be a friend or relative, who has 'lost their phone'. This means you don't have their phone number saved in your phone. They may ask a favour, as they've lost their phone and need some money. Don't send any money to them. Try contacting your friend or relative on their usual phone number or email address and check if they're ok.
- **Pets:** Always buy pets from a reputable breeder or adopt from a shelter. You should see the animal before you pay.

Artificial intelligence and staying safe online

Artificial intelligence (AI) can be used to create realistic images, video, audio and writing. The AI programs can be trained to copy someones text messages or email writing style or voice, this is then used for targeted scams.

Deep fakes create fake video and audio of a person using AI. One type of deep fake scam involves the use of AI voice cloning tools, to copy the voice of a loved one, a family member, or even a well-known figure. They claim to be in distress or facing an emergency situation and urgently ask for money, payments or ask for sensitive information to help them via phone call or voicemail.

- Listen for unnatural pauses or a distorted voice quality, as these could be signs of pre-recorded messages or voices being created live by typing a script.
- If you have suspicions and you know the person, try contacting them on another phone number, social media or send a message to confirm they are on the phone to you.
- To protect yourself from phone scams, you could also create a codeword you agree to say or ask them to say, that isn't shared with anyone else. This can help you be sure it is their voice on the phone.

Deep fakes have also been used to create fake sexual images or embarrassing images of somebody to blackmail them. This should be reported in the same way as mentioned above in the protecting your image online section.

Protect your personal information

Be careful what personal information you post on social media. Fraudsters trawl online platforms for data like your name, address, email, phone number, place of work, health issues and date of birth. They can use this information to target or impersonate you to commit fraud. Or they may try to befriend you to gain your trust then ask for your help.

Make sure you use secure passwords and don't send money to people you don't know on the internet.

Safe video conferencing

Only download software from reputable brands such as Apple or Google Play or from the official website of the provider: such as **Skype.com** or **Zoom**

- Make sure your password cannot be matched with your other passwords for email and apps.
- Set up 2 step authentication
- Make sure you know how a meeting is recorded so you can spot the signs
- Don't post on social media – invite by email to keep the meetings private and avoid "bombing" (see below)
- Keep your software and devices up to date to maximise security

When arranging your video call, set up a password. Only send the joining instructions and log in details to the people you want to join your conversation. To avoid 'zoom bombing', where an uninvited guest joins your call. This is a risk when setting up a public video call, or posting the log in instructions online where others can see them.

Use secure browsers

Look for the padlock symbol or https:// next to the website address in your browser to check that the website you're using is secure. If the padlock is locked the website is secure. This is very important when using online banking, buying goods online or using any website where you are giving your log in and password details.

When you click a link on a website to visit another site, or from an email or text, look for the padlock symbol or https:// to make sure you are going to a secure site.

Some websites are set up as 'spoof' or malicious sites that look genuine but can allow a malware or a virus to be planted on your computer. Malware is any software intentionally designed to cause damage to a computer, server or computer network. A wide variety of types of malware exist, including: computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware. This could allow a fraudster to watch your online activity and harvest your personal data including passwords, giving them access to your emails and online accounts.

How to report and block malicious social media accounts

To report and block a Facebook profile

- click on the … on the person's cover photo and select Find Support or Report Profile
- then select the option that best describes the account
- click at the top right of Facebook and choose Settings
- click Blocking in the left side menu, select the person you want to block and click Block name

To report and block an Instagram profile

- tap **…** (iOS) or **…** (Android) in the top right of the profile. Tap Report and follow the instructions
- tap **…** (iOS) or **…** (Android) in the top right of the profile. Tap Block/Unblock

To report a Twitter profile and to block a Twitter profile

- select the overflow icon on the profile you want to report **…**
- then select Report and select the type of issue you'd like to report
- click the more icon on their profile page **…**
- then select Block from the menu. Click Block to confirm

To report and block spam emails on Google/gmail

- on your computer, go to Gmail.
- open the message, and click report spam near the top of the page !
- on your computer, go to Gmail and open the message. In the top right, click More **…**
- click Block sender

Support for victims of online crime

The Cyber Helpline support victims of cybercrime and online harm. Chat to their chatbot and get immediate advice on how to deal with your cyber security issue. If you need more help, it will pass you onto one of their volunteer cyber security experts.

- Read our article on **fraud and scams**
- Read **bogus callers**.
- Read **ways to report crime and community safety issues**.

Victim Support (VS) helps people affected by crime and traumatic events. They provide individual, independent, emotional and practical help to you to cope and recover from the effects of crime.

Action Fraud where you can report online fraud or crime using their telephone helpline or website.

Last updated: December 7, 2023

Useful Organisations

Northumbria Police

Website: www.northumbria.police.uk

Telephone: 101

Action Fraud – report Fraud & Internet Crime

Website: www.actionfraud.police.uk

Telephone: 101

Safe Newcastle

Email: safenewcastleadmin@newcastle.gov.uk

Website: https://www.safenewcastle.org.uk/

Telephone: 101

Get Safe Online

Website: www.getsafeonline.org

Telephone: 101

Prevent Charity Fraud

Email: info@fraudadvisorypanel.org

Website: https://preventcharityfraud.org.uk/

Telephone: 020 7920 8637

Address: Chartered Accountants' Hall , EC2R 6EA

North East Regional Cyber Crime Unit

Website: https://nerccu.police.uk/

Telephone: 020 7920 8637

The Cyber Helpline

Website: https://www.thecyberhelpline.com/

Telephone: 020 7920 8637

Address: Room 2, 1st Floor, TN13 1DB

Revenge Porn Helpline

Email: help@revengepornhelpline.org.uk

Website: https://revengepornhelpline.org.uk/

Telephone: 0345 6000 459

Stop NCII.org

Website: https://stopncii.org/

Telephone: 0345 6000 459

Victim Support

Website: victimsupport.org.uk

Telephone: 0808 16 89 111

Financial Conduct Authority (FCA)

Email: consumer.queries@fca.org.uk

Website: www.fca.org.uk

Telephone: 0800 111 6768

Address: 25 The North Colonnade, E14 5HS

Related Articles

Fraud and scams

Getting online and using digital equipment

Ways to report crime and community safety issues