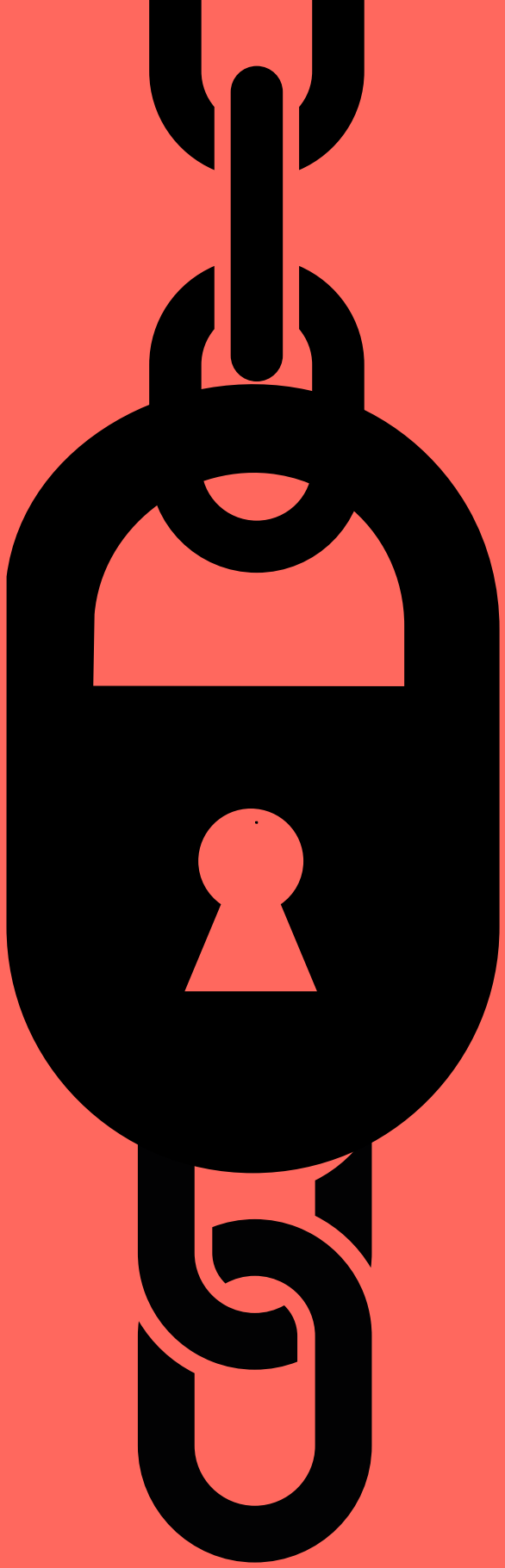

New Updated Edition

FRAUD PROTECTION TOOLKIT

The ultimate guide to minimising the risk of fraud

www.cumbria.police.uk

Introduction from Detective Inspector Jamie Eaton

Fraud not only has an impact on people - it also damages organisations and economies, eroding trust and financial security. The challenges are significant, however there are proactive steps we can take to mitigate fraud effectively.

The first step is to increase our awareness of fraud. This toolkit will provide a useful guide to recognising the red flags such as phishing and too-good-to-be-true offers.

Individuals and organisations must stay vigilant by questioning unsolicited communications and verifying information before sharing their most personal data.

Cumbria Police place great emphasis on fraud, taking both a targeted approach and prevention. We have a dedicated officer working with individuals and departments across the force to enhance their awareness. Please remember that being the victim of fraud is never your fault, fraudsters will use persuasive techniques.

To minimise the impact of fraud it is vital we adopt a multi-faceted approach that combines education and collaboration. We all have a role to play in creating a culture of vigilance, by staying vigilant and informed we can build a strong protection system to fraud and build trust.

Let's all take steps to tackle fraud and create a safer future. Please do take the time to read this useful toolkit and share with your colleagues.

Further information:

Please check out the #NoBlameNoShame Campaign by the National Trading Standards Scams Team to learn more about how criminals use manipulation in fraud. The national Stop! Think Fraud campaign also contains essential information by providing the tools and knowledge to recognise fraudulent behaviour and take action to stop and prevent it. Finally, please do share this booklet and the information within.

How to Minimise Fraud Risk

Have you been a victim of fraud?

NO → This guidance, if followed can still help to minimise your fraud risk.

YES → Please report the incident to both your financial provider and Report Fraud.

Next

Please start with pages 4 and 5 in order to secure both your personal and financial information and page 6 for recovering monies lost to fraud.
Next – Let's take some action to give you more control over the contact routes and minimise fraud risk

How was contact made with you?

Telephone	Mobile Phone/ SMS/Text Message	Social Media and Messaging Services	Email and Websites	Computer and Tablets	Post to & Direct at Home Address
Page 7	Page 8	Page 9	Pages 10	Pages 11	Pages 12-13

The more contact routes controlled,
the more the risk of fraud will be minimised.

Personal Information

Criminals will try to get hold of your personal information as it makes it possible for them to take out financial products like loans or credit cards and/or services in your name, leaving you liable for the cost.

- Treat your personal information like your house or car keys and never hand it over to strangers, recent acquaintances or anyone asking for your details where it is not strictly necessary.
- Always be mindful about what personal information you share online such as through any social media accounts.
- Only give out your personal information after very careful consideration. It is ok to reject, refuse or ignore any requests whilst you think it through.

Minimise fraud risk and control your personal information by:

- [ ] Check if identity fraud has been committed by checking all 4 UK credit reference agencies (Equifax, TransUnion, Crediva and Experian). For a fee all 4 reports can be checked at once at Check my File.
- [ ] Protect against identity fraud and from criminals using your personal details to apply for products and services in the future by applying for CIFAS Protective Registration which costs £30 for 2 years.
- [ ] Find out what to do if identity fraud is confirmed as being committed.
- [ ] Notify any relevant organisations where originals or copies (including photos) of documents/identification may have been provided (DVLA, HM Passport Office).

Safeguard your Finances

Criminals will try different tactics to get at your finances.
Warning signs for fraud include:

- Asking you to withdraw or transfer money to a different account.
- Asking you to reveal your full banking password or pin.
- Asking you to reveal your OTP (one time password).
- Asking you to buy jewellery/expensive items to help with a police investigation.
- Asking you to buy gift cards including iTunes gift cards.
- Sending a courier to collect money, cards or personal items.

! The Police or your bank will never ask you to do any of these things.

- Treat your bank cards, PINs and login details like your house or car keys and never hand them over to strangers or recent aquaintances .
- Keep all your financial information such as bank details, PINs and banking passwords safe.

Minimise fraud risk and control access to your financial information by:

- [ ] Report the fraud to your bank so cards and account numbers can be changed, and a refund can be discussed if applicable.
- [ ] Ensure that Report Fraud have been informed (Report Fraud do not investigate).
- [ ] Consider how a co-signatory on your account may reduce the scope for fraud.
- [ ] Consider how appointing a lasting power of attorney allows you more control over what happens to you and your finances in case of an accident or illness.

Recovering Monies Lost to Fraud

Please note that any decision to refund any monies lost to fraud lies entirely with the bank/financial institution concerned. Report Fraud or Police form no part of the decision-making process.

Fraudsters will often pose as being able to recover monies lost to fraud for an up-front fee which is known as Recovery Fraud, so please ensure that steps are taken to verify any route you may choose to pursue.

The Financial Conduct Authority also has information on Financial Investments.

Minimise fraud risk and control access to your financial information by:

- [ ] If money was transferred via bank transfer, please refer to What to do if you're the victim of a bank transfer scam - Which?
- [ ] If payment took place via credit card, please refer to Section 75 of the Consumer Credit Act - Which?
- [ ] If payment was made via a debit card, check to see if you can claim for a refund under a voluntary scheme called Chargeback using this letter template .Debit card payments and purchases are not covered by section 75 of the Consumer Credit Act
- [ ] If the payment was made via an online payment platform such as PayPal, Apple Pay or Google Pay check to see if you can make a claim under their dispute resolution process. Terms and conditions will apply.
- [ ] If a purchase took place via an online marketplace check to see if you are covered under any buyer protection scheme. Please see eBay UK - Buyer Protection Guide ,What is Buyer Protection? - Shpock and Buyer Protection (vinted.co.uk)
- [ ] Contact Citizens Advice to discuss how it may be possible to get your money back.
- [ ] Consider making a court claim or using mediation services Make a court claim for money - GOV.UK (www.gov.uk) (A claim to the small claims court may be done directly or via a solicitor).
- [ ] Consider using a Financial Advisor or Claims Management Company regulated by the Financial Conduct Authority (Check the Financial Services Register to ensure they are regulated. It is also possible to check to see if an individual or company is already known to the FCA (Financial Conduct Authority) for being unregulated Unauthorised firms and individuals | FCA).

Contact via Telephone

Criminals will use the telephone most often to contact potential victims. Warnings signs for fraud include:

- Threatening to arrest you if you do not do something such as withdraw cash or transfer money to pay a 'fine' or 'fee'.
- A recorded message asks you to call a number to 'claim a prize'.

! No genuine organisation/institution would ever use threats like this.

Minimise fraud risk and control this contact route by:

- [ ] Contact your service provider to discuss what call blocking solutions may be available.
- [ ] Request your service provider makes any landline numbers ex-directory.
- [ ] Discuss changing your telephone number with your service provider.
- [ ] Consider buying a handset with caller display so withheld/unrecognised numbers can be ignored.
- [ ] Register with the Telephone Preference Service to stop unsolicited and marketing calls. (Applies to mobile too)
- [ ] If scam/nuisance calls persist then consider buying an external call blocker. Trading Standards recommends truecall
- [ ] Report Nuisance calls to Information Commissioners Office who collate information for potential enforcement action.

Contact via Mobile Phone and SMS/Text Message

Criminals can make SMS messages and phone calls appear genuine.

- Never click on link provided in SMS messages or supply personal information, before taking steps to verify the source of the message.
- Visit Mobile phone fraud | Report Fraud for further information on keeping safe.
- Discover Date Safe Tips from the Online Dating Association to ensure a safe online dating experience.
- Learn more about Staying Safe from Romance Fraud in our e booklet.
- If you have been targeted with romance fraud, you may also find our Romance Fraud Practical Support Guide helpful.
- LoveSaid are an organisation who specialise in romance fraud prevention support and empowerment. Find out more at Resources-LoveSaid

Minimise fraud risk and control this contact route by:

Calls

- [ ] Block any unwanted numbers via your handset.
- [ ] Some handsets will enable specific numbers to be blocked. A service provider will be able to advise how to do this.
- [ ] Register with the Telephone Preference Service to stop unsolicited and marketing calls.
- [ ] Report spam calls by texting 'CALL' plus the number that called you to 7726. This will alert your service provider to investigate the number and potentially block it, if it is found to be a nuisance.

SMS/Text Messages

- [ ] Spam texts can be forwarded for free to "7726" which is run by Ofcom (This spells "Spam" on the telephone keypad).

Contact via Social Media and Messaging Services

Just like with phone calls and SMS messages, fraud criminals can make social media messaging appear genuine. Common frauds include:

Social media account takeover also known as 'social media account compromise' which can result in you being locked out of your own account, as well as fraud criminals taking over friend's account. Look out for unsolicited direct messages and odd posts from genuine contacts/friends on social media who may have had their account compromised.

A message claiming to be from your child seeking financial support for a fictitious emergency. This is also known as the 'Hi Mum and Dad' fraud which started on WhatsApp but has also spread to text messages. Always take steps to double check you are communicating with the person you think you are speaking to.

What is Sextortion:

Sextortion of a form of blackmail which involves threatening to publish sexual content about someone. This can include photos and videos someone may have shared in confidence or fraud criminals may claims to have faked content. This may be to extort money or force someone to do something against their will. This usually happens one of 2 ways:

- A threatening email claiming they have evidence of someone visiting an adult website and will threaten to disclose publicly unless a ransom is paid (often in Bitcoin).
- Sextortion via webcam/video call after photos or videos have been shared.

Contact the Revenge Porn Helpline if you have had images/videos shared without your consent.

Minimise fraud risk and control this contact route by:

- [ ] Secure e mail accounts and ensure social media privacy and security settings are set to manage your digital footprint.
- [ ] Recover-hacked-online-accounts by following this advice.
- [ ] Block unwanted contact/messages. For information about doing this on specific platforms, follow these links - Facebook, X/Twitter, Instagram, YouTube, Snapchat, WhatsApp, Discord, Google Chat (Previously Hangouts), TikTok, LinkedIn.
- [ ] Make use of the reporting facilities on each platform to report unwanted contact or untoward behaviour - Facebook, X/Twitter, Instagram, YouTube, Snapchat, WhatsApp, Discord, Google Chat (Previously Hangouts), Tiktok, LinkedIn.

Contact via Email and Websites

Fraudsters will often spoof email addresses and websites.

This means that an email address can be made to look as if it is from a genuine organisation when in reality it is from a web-based address (Gmail, Hotmail, Yahoo, etc.). Just because an e mail or website looks recognisable, it does not mean it is the genuine one.

- Make sure that your internet browser is not warning you that your connection is 'Not Secure' in the address bar. This may also be indicated by a crossed-out padlock icon. If you do see a locked padlock icon in the address bar, this means the connection to the website is secure. It does not guarantee that the website is legitimate or reputable.
- Always take extra steps to be certain before going ahead and never supply copies or photographs of personal documents to a stranger online or in response to a request out of the blue.

Minimise fraud risk and control this contact route by:

- [ ] Open the full email or hover your mouse over the display email to check the display and sender e mail address correspond. A mismatch is a good indicator of an email that should be treated as spam.
- [ ] Avoid clicking on links in that you have not checked out first. Report any suspicious e mails to the Suspicious Email Reporting Service by forwarding them to report@phishing.gov.uk
- [ ] Searching on the correct exact full website address can reduce the risk of ending up on a fraudulent website. Remember that the top results in search engines are sold as advertising space so the top result is not always the authentic website.
- [ ] Determine if a website is likely to be legitimate or a fraud by using by using the Check a website facility from Get Safe Online.
- [ ] Please see the 'Contact via Computer or Tablet' section (page 11) for further advice on how to secure your online presence.

Contact via Computer or Tablet

Create your FREE Cyber Action Plan on the NCSC website

The anonymity of the internet allows criminals to be whoever they want to be online. Just because someone says it is true, it does not mean that it is. If it sounds too good to be true then it probably is, however, it does not have to sound amazing to be a fraud.

- Use a Google or TinEye to carry out a reverse image search to see if an image has been stolen from elsewhere.
- Be sure to follow Key Cyber Protect Advice from the National Cyber Security Centre.

Minimise fraud risk and control this contact route by:

- [ ] Use a strong and separate password for your email - NCSC.GOV.UK
- [ ] Combine three random words to create a password that is 'long enough and strong enough' for all other accounts Three random words - NCSC.GOV.UK
- [ ] Save passwords in your browser: Password managers: using browsers and apps to safely store... - NCSC.GOV.UK
- [ ] Turn on 2-Step Verification (2SV) for your email: Turn on 2-step verification (2SV) - NCSC.GOV.UK
- [ ] Backing up your data: Backing up your data - NCSC.GOV.UK
- [ ] Install the latest software and app updates: Install the latest software and app updates - NCSC.GOV.UK

Advice for those concerned...

- [ ] Advice for those concerned a device has been infected: How to recover an infected device - NCSC.GOV.UK
- [ ] Find out how to use social media safely: Social Media: how to use it safely - NCSC.GOV.UK
- [ ] How to recognise and report emails, texts, websites, adverts, or phone calls that you think are trying to scam you: Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK
- [ ] Report a scam email by forwarding them to report@phishing.gov.uk

Contact via Post to Home Address

Criminals also use tactics to scam you by sending you fraudulent mail. Fraud warning signs can include:

- Mail that pressures you to respond by telling you that you need to 'act fast' or that 'an urgent response is required', particularly if this is to receive a pay-out or a prize.
- Find out more about different types of postal scams at Think Jessica

Minimise fraud risk and control this contact route by:

Post

- [ ] Opt out of the Open Voters Register which is available to anyone who wants to buy a copy.
- [ ] Remove your details from mailing lists by registering with the Mailing Preference Service
- [ ] It is possible to stop getting junk mail by following this guidance from The Citizens Advice Bureau.
- [ ] Report any scam mail you receive to Royal Mail
- [ ] Set up a Royal Mail Postal Redirection to your new address when moving to ensure your mail moves with you.
- [ ] Royal Mail can redirect mail in special circumstances where a power of attorney, deputyship or other similar legal authority exists.
- [ ] Set up a HM Land Registry - Property Alert for any property that could be at risk of fraud.
- [ ] Consider asking a relative or trusted friend to help you check and screen the post.

Contact via the Doorstep at Home Address

You may also get doorstep callers offering their services or products for sale. This can also include people posing as bank officials or couriers claiming to need to collect bank cards, cash, or jewellery.

Tactics may involve:

- You are asked or pressured to hand over money at the door
- You are asked or pressured to hand over bank cards, financial information, PINs, or withdraw cash.

The below tips will help you feel better equipped to deal with any unexpected doorstep callers:

- Say 'No' to doorstep callers. Many people worry about appearing rude if they say no to doorstep callers. It is always ok to say no thank you.
- Take time to think and talk to someone you trust outside the situation when you are asked to do something.
- Never sign on the spot if you are seeking trades persons– shop around. Get at least three written quotes to make sure you are not being ripped off.

Minimise fraud risk and control this contact route by:

Doorstep

- [ ] Install a 'no cold calling' sign. If a doorstep caller still knocks, then it is a good sign of when not to engage with someone.
- [ ] Discuss if a neighbour may help you screen visitors and install a sign directing doorstep visitors to this neighbour.
- [ ] Consider a CCTV (Closed Cicuit Television) camera in your porch (with a warning sign) or buying a smart/Ring doorbell (local Trading Standards can advise further in this area)
- [ ] Consider registering with the free support service offered by energy suppliers and network operators. The Priority Services Register can set up an identification and password scheme to help you identify if a doorstep caller is genuine.

Fraud Minimisation Checklist :

Minimise becoming a victim of fraud. The below checklist may help you keep track of any actions'

Useful Website Addresses

Cumbria Police fraud advice: https://www.cumbria.police.uk/advice/advice-and-information/fa/fraud/

Victims First: https://www.victims-first.org.uk/crime-info/guidance-and-support/fraud/

Victim Support: https://www.victimsupport.org.uk/

Report Fraud A-Z: https://www.reportfraud.police.uk/collection/a-z-fraud/

National Cyber Security Centre: https://www.ncsc.gov.uk

Stop! Think Fraud Campaign: https://stopthinkfraud.campaign.gov.uk/

National Trading Standards: http://www.nationaltradingstandards.co.uk

No Blame No Shame Campaign: https://www.friendsagainstscams.org.uk/news-and-updates/noblamenoshame-news-article

Age UK scams and fraud advice: https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/

Take Five to Stop Fraud: https://takefive-stopfraud.org.uk/advice/general-advice

Don't Be Fooled money mules advice: https://www.moneymules.co.uk

Citizens Advice: https://www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/

Useful Website Addresses By Page

Page 2 - D.I Wynn Introduction

#NoBlameNoShame Campaign: https://www.friendsagainstscams.org.uk/news-and-updates/noblamenoshame-news-article

Victims First: https://www.victims-first.org.uk/

Victim Support: https://www.victimsupport.org.uk/

Stop! Think Fraud Campaign: https://stopthinkfraud.campaign.gov.uk/

Page 4 - Personal Information

Identity fraud: https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft

Equifax: www.equifax.co.uk/Products/credit/statutory-report.html

TransUnion: www.transunionstatreport.co.uk/CreditReport/AboutYou

Crediva: www.crediva.co.uk/statutory-credit-report/

Experian: www.experian.co.uk/consumer/statutory-report.html

Check my file: www.checkmyfile.com

Protective Registration: https://www.cifas.org.uk/pr

What to do if identity fraud is committed: https://www.cifas.org.uk/services/identity-protection/victim-of-impersonation

DVLA: www.gov.uk/contact-the-dvla

HM Passport Office: www.gov.uk/passport-advice-line

Page 5 - Safeguard your Finances

Report Fraud: https://www.reportfraud.police.uk/

Lasting power of attorney: www.gov.uk/power-of-attorney

Page 6 - Recovering Monies Lost to Fraud

Recovery Fraud: https://www.actionfraud.police.uk/a-z-of-fraud/fraud-recovery-fraud

The Financial Conduct Authority: www.fca.org.uk/

Financial Investments: https://www.fca.org.uk/investsmart/5-questions-ask-you-invest

Victim of a bank transfer (App) scam: https://www.which.co.uk/consumer-rights/advice/what-to-do-if-you-re-the-victim-of-a-bank-transfer-app-scam-aED6A0l529rc

Section 75 of the Consumer Credit Act: https://www.which.co.uk/consumer-rights/regulation/section-75-of-the-consumer-credit-act-aZCUb9i8Kwfa

Chargeback: https://www.which.co.uk/news/article/chargeback-the-card-protection-banks-dont-tell-you-about-agxaE6A7oqwk

Letter template: https://www.which.co.uk/consumer-rights/letter/letter-to-make-a-chargeback-claim-aFAg65B543ik

Paypal: https://www.paypal.com/uk/webapps/mpp/paypal-safety-and-security

Apple Pay: www.support.apple.com/en-us/102335

Google Pay: https://support.google.com/googlepay/answer/7644016?hl=en

EBay UK - Buyer Protection Guide: https://pages.ebay.co.uk/buyerprotectionguide/

What is Buyer Protection?: https://www.shpock.com/en-gb/help/360015827897

Buyer Protection (Vinted.co.uk): https://www.vinted.co.uk/help/550-buyer-protection

Citizens Advice: www.citizensadvice.org.uk

Make a court claim for money: www.gov.uk/make-court-claim-for-money

Solicitor (Solicitors Regulation Authority): https://www.sra.org.uk/consumers/

Financial Services Register: www.fca.org.uk/firms/financial-services-register

Unauthorised firms and individuals (FCA): https://www.fca.org.uk/consumers/warning-list-unauthorised-firms

Page 7 - Contact via Telephone

Telephone Preference Service: http://www.tpsonline.org.uk

trueCall: https://www.truecall.co.uk/

ICO - Information Commissioners Office: https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/

Page 8 - Contact via Mobile Phone or Social Media/Messaging Services

Mobile phone fraud: https://www.actionfraud.police.uk/a-z-of-fraud/mobile-phone-fraud

Date Safe Tips: https://www.onlinedatingassociation.org.uk/for-consumers/date-safe/

Online Dating Association: https://www.onlinedatingassociation.org.uk/

Romance fraud guides:
https://crimestoppers-uk.org/getmedia/81014543-5933-4359-a319-b9a6b289ac96/Final-romance-fraud-e-booklet.pdf
https://data.actionfraud.police.uk/cms/wp-content/uploads/2024/10/Romance-Fraud-Support-Pack-National-Version-1.pdf

LoveSaid.org: https://www.lovesaid.org/

Resources - LoveSaid: https://www.lovesaid.org/resources

Telephone Preference Service: www.tpsonline.org.uk

Report spam calls: https://www.ofcom.org.uk/phones-and-broadband/unwanted-calls-and-messages/tackling-nuisance-calls-and-messages

Report spam texts: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls/

Page 9 - Contact via Social Media and Messaging Services

Hi Mum and Dad fraud: https://www.which.co.uk/news/article/notorious-hi-mum-and-dad-scam-spreads-from-whatsapp-to-text-message-an7N34c0gVbP

Threatening email: https://www.ncsc.gov.uk/files/sextortion-scams-infographic.pdf

Sextortion via webcam/video call: https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion

Revenge Porn Helpline: https://revengepornhelpline.org.uk

Secure e-mail accounts: https://www.actionfraud.police.uk/secureyouraccounts

Social media privacy and security settings: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Recover hacked online accounts: https://www.ncsc.gov.uk/files/Recovering-hacked-online-accounts-infographic.pdf

Block on Facebook: https://www.facebook.com/help/168009843260943

Block on X/Twitter: https://help.x.com/en/using-x/blocking-and-unblocking-accounts

Block on Instagram: https://help.instagram.com/426700567389543

Block on YouTube: https://support.google.com/youtube/answer/9482361?hl=en-GB

Block on Snapchat: https://help.snapchat.com/hc/en-us/articles/7012401093396-How-to-Block-a-Friend-on-Snapchat

Block on WhatsApp: https://faq.whatsapp.com/1142481766359885/?locale=en_US&cms_platform=iphone

Block on Discord: https://support.discord.com/hc/en-us/articles/217916488-Blocking-Privacy-Settings

Block on Google Chat (Previously Hangouts): https://support.google.com/chat/answer/9277792?hl=en-GB&co=GENIE.Platform=Android

Block on TikTok: https://support.tiktok.com/en/using-tiktok/followers-and-following/blocking-the-users

Block on LinkedIn: https://www.linkedin.com/help/linkedin/answer/a1344213/recognize-and-report-spam-inappropriate-and-abusive-content?lang=en

Report on Facebook: https://en-gb.facebook.com/help/171757096241231

Report on X/Twitter: https://help.twitter.com/en/safety-and-security/report-abusive-behavior

Report on Instagram: https://help.instagram.com/192435014247952

Report on Youtube: https://support.google.com/youtube/search?q=report&from_promoted_search=true

Report on Snapchat: https://help.snapchat.com/hc/en-us/articles/7012399221652

Report on WhatsApp: https://faq.whatsapp.com/1142481766359885/?helpref=-search&cms_platform=android

Report on Discord: https://discord.com/safety/360044103651-reporting-abusive-behavior-to-discord

Report on Google Chat (Previously Hangouts): https://support.google.com/chat/answer/9277792?hl=en&sjid=14249485753439872488-EU

Report on TikTok: https://support.tiktok.com/en/safety-hc/report-a-problem

Report on LinkedIn: https://www.linkedin.com/help/linkedin/answer/a1344213/rec-

Page 10 - Contact via Email and Websites

Suspicious Email Reporting Service: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email

Check a website: https://www.getsafeonline.org/checkawebsite/

Get Safe Online: https://www.getsafeonline.org/

Page 11 - Contacted by Computer or Tablet

Free Cyber Action Plan: https://www.ncsc.gov.uk/cyberaware/actionplan

Google Reverse Image Search: https://support.google.com/websearch/answer/1325808?co=GENIE.Platform%3DDesktop&hl=en&oco=0

TinEye: https://tineye.com/

Cyber Protect Advice: https://www.ncsc.gov.uk/cyberaware/home

National Cyber Security Centre: https://www.ncsc.gov.uk/

Use a strong and separate password for email: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

Password - 3 random words: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

2 Step Verification (2SV) for e-mail: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

Save passwords in browser: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

Backing up Data: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

Install latest software and app updates: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

Infected device advice: https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Use social media safely: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Recognising scam emails, texts, websites or phone calls: https://www.ncsc.gov.uk/collection/phishing-scams

Suspicious Email Reporting Service: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email

Page 12 - Contact via Post to Home Address

Think Jessica: www.thinkjessica.com/postal-fraud/

Open voters register: https://www.gov.uk/electoral-register

Mailing preference service: https://www.mpsonline.org.uk/

Stop getting junk mail: https://www.citizensadvice.org.uk/consumer/post/stop-getting-junk-mail/

How to report scam mail: https://personal.help.royalmail.com/app/answers/detail/a_id/303/~/

Royal Mail Postal Redirection: https://www.royalmail.com/personal/receiving-mail/redirection

Redirect mail in special circumstances: https://www.royalmail.com/sites/royalmail.com/files/2024-04/special-circumstances-redirection-application-form-april-2024.pdf

HM Land Registry Property Alert: https://www.gov.uk/guidance/property-alert

Page 13 - Contact via the Doorstep at Home Address

Doorstep callers: https://www.actionfraud.police.uk/a-z-of-fraud/bogus-tradesmen-fraud

Priority Services Register: https://www.ofgem.gov.uk/energy-advice-households/join-your-suppliers-priority-services-register

Designed by Corporate Communications CC6110_V4_0524

VICTIMS FIRST

Care | Empower | Recover

Report Fraud