



Fraud Counts Newsletter



December 2020



This Photo by Unknown Author is licensed under CC BY-SA-NC

Welcome to the first edition of the new look Fraud Counts newsletter from ASW Assurance

In future, Fraud Counts will be a briefer read and we will be publishing them more regularly.

This first new look edition is aimed at helping you to stay safe from fraudsters in the lead up to Christmas.



This Photo by Unknown Author is licensed under CC BY-NC

The twelve tips for Christmas

Christmas 2020 is going to be unusual because of COVID and we have already seen fraudsters exploit the pandemic in a variety of ways.

Whilst we can be certain the fraudsters will exploit the festive season and COVID, it remains to be seen exactly how they will do that.

From past experience, here's what we can expect - we present the twelve tips for Christmas, courtesy of West Yorkshire Police, Action Fraud, City of London Police, Get Safe Online and Cyberstreetwise.com.



This Photo by Unknown Author is licensed under CC BY-NC

LOOK OUT FOR FRAUDSTERS WHEN PURCHASING YOUR CHRISTMAS PRESENTS

Traditionally, this time of year sees fraudsters targeting individuals when they are spending money on presents and other Christmas preparations.

Sometimes peoples' guard is dropped because Christmas time is not "business as usual".

Suspicious of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence - 0800 028 40 60 or www.reportnhsfraud.nhs.uk





The twelve tips for Christmas

1. Online shopping fraud

- Wherever possible use online retailers/brands you are aware of and trust.
- Be especially careful when purchasing expensive items.
- Make sure you have adequate anti-virus software that will enable your computer to flag any untrustworthy sites.

2. Christmas e-cards

- If you receive an anonymous e-card, better to play it safe and delete the email as it could be infected.
- Use a reputable anti-virus product on your electronic device, making sure it is regularly updated and always turned on.
- If you believe your electronic device has been infected, switch it off and disconnect from the internet to prevent further information being stolen. For advice on free malware removal tools go to www.cyberstreetwise.com. Also, contact your bank and change passwords and usernames.

3. Auction fraud

- Always use recommended methods of payment rather than transferring money direct to a seller.
- Research the seller before you bid. If available, check their feedback but be mindful that this can also be falsified.
- Be cautious when buying from sellers abroad or private individuals. If you are in any doubt, back out of the sale.
- If you are collecting what you have bought, take someone with you or let someone know where you are going.

4. Holiday fraud

- Always pay with a credit card; if they don't accept credit cards, don't buy from them.
- Use companies that are ABTA or ATOL protected. Verify this protected status by contacting the Civil Aviation Authority.
- Research the internet and consider the reviews of the company/person you wish to use before booking your trip.

5. Loan and investment scams

- Authentic loan providers will not ask for an advance fee. If they ask for an advance fee just say no.
- Research any loan or investment companies online before making any financial commitment. Also make sure to read the terms and conditions.
- If the loan or investment opportunity seems too good to be true, it probably is.
- Never set up a loan or make an investment which starts with a cold-call. Always better to just hang-up.
- Go to www.fca.org.uk for a list of unauthorised firms and top tips on how to avoid dodgy investments.

6. Ticketing fraud

- Only look at tickets from reputable websites that are secure (showing a padlock) and, before buying, do an internet search for reviews on the gig/sporting event to see if anyone has fallen victim to a ticketing scam.
- Avoid entering your bank or credit card details on public or shared computers.



7. Donating to charity

- Visit the charity's website by typing the address into your browser rather than clicking on a hyperlink embedded in an email.
- Before you donate, check the website you are on is secure - the web address should begin with https:// (the "s" stands for "secure") and look for the padlock symbol.
- Do not respond to requests to donate through a money transfer company such as Western Union or MoneyGram.
- If you are still worried, a legitimate charity will advise you on other ways to give on their website or via a phone call.

10. Social media scams

- Do not have too much personal information on social media accounts which could allow your bank accounts to be compromised. Think particular about online quizzes that seem to be fun but include questions such as "what was your first car?" or "what was your Mum called before she got married". Take a moment to think whether your answers are also answers to your password reset questions on any online or bank/build society account etc.
- Be wary of installing add-ons to your internet browser as some can be used to extract personal and financial information from your search history.
- If you click on a social media advert do the necessary checks before buying anything from the website you land on.

8. Mobile malware/malicious apps

- Make sure you have the latest versions of software installed for increased protection.
- Only download apps from official app stores like Google Play and Apple Store and always check reviews and ratings as well as developer information before downloading a new app.
- Install anti-virus software and keep it up to date.
- Do not click on links in emails from unknown sources or visit suspicious websites on your new devices.

11. Dating fraud

- Guard your privacy when chatting online and be selective with the information you provide about yourself.
- Never send money or give credit card or online account details to anyone you do not know and trust.
- Trust your instincts, if something feels wrong take steps to protect yourself.

9. Money transfers

- Never send money transfer for online purchases.
- Wait the six or seven working days it takes for a cheque to clear before transferring any money or sending/ mailing any goods. Doing this will mean you don't lose anything even if the cheque bounces, proves to be fraudulent or is cancelled.
- Never send money in advance to obtain a loan or credit card or to pay for "processing fees" on lottery or prize winnings.
- Never provide your banking information to people or businesses you do not know and trust ensure they really are who they say they are.

12. Mobile payments




















- Do not save passwords or personal/financial data on your mobile device unless it is absolutely necessary and make sure the phone is passcode protected.
- If stolen, most mobile devices have the software to wipe all data from their memory remotely - learn how this works.
- Do not leave your Bluetooth on as cyber-criminals can hack into your device unnoticed. Also, install anti-virus software and check the security features.



OUR LOCAL COUNTER FRAUD TEAM

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact your Local Counter Fraud Specialist (LCFS) below.

	<p>Gareth Cottrell – Interim Counter Fraud Manager 01872 258057 or 07814 002364 gareth.cottrell@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  Royal Cornwall Hospitals NHS Trust  Cornwall Partnership NHS Foundation Trust  Cornwall Care 		<p>Tracy Wheeler - LCFS 01752 431378 / 07789 868568 tracy.wheeler2@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  University Hospitals Plymouth NHS Trust  Devon Partnership NHS Trust  Livedale Southwest
	<p>Shamaila Asghar - LCFS (maternity cover for Adele Rilstone) 07775 417508 shamaila.asghar@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  Torbay and South Devon NHS Foundation Trust 		<p>Alice Lee - LCFS 07813 540022 alicelee1@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  Devon CCG  Out of Hours Service Providers
	<p>Eli Hayes – LCFS 07920 284239 elias.hayes@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  University Hospitals Bristol and Weston NHS Foundation Trust  Bristol, North Somerset and South Gloucestershire CCG 		<p>Mo Jackson - LCFS 07824 606899 mo.jackson@nhs.net</p> <p>LCFS for:</p> <ul style="list-style-type: none">  Northern Devon Healthcare NHS Trust  Royal Devon & Exeter NHS Foundation Trust