CITY OF LONDON POLICE
National Policing Lead For Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

It's Christmas time, stay safe online

GET SAFE ONLINE .org

CYBERSTREETWISE.COM

CRIMESTOPPERS
0800 555 111
Call anonymously with information about crime

The 12 online frauds of Christmas

In the countdown to Christmas millions of people living across the UK will go online to buy presents for friends and family, search for holidays, book tickets for a big gig or send an electronic Christmas card.

What many do not realise is the hidden threat we now face from criminals online. They are targeting internet shoppers with scams which, on the surface promise to save them time and money, but in reality only deliver festive heartache and misery. Tens of thousands of people sadly fell victim to an online fraud in the weeks leading up to last Christmas and even more are at risk of suffering the same fate this year – being left hundreds, and sometimes even thousands of pounds out of pocket with no presents to give on the big day and their electronic devices corrupted with a computer virus.

To make life as difficult as possible for the cyber fraudsters, the **City of London Police**, which is the National Policing Lead for Fraud, and supported by **Get Safe Online**, **The Home Office**, **Crimestoppers**, **National Trading Standards** and **Victim Support** is running 'The 12 online frauds of Christmas' campaign. Together, we are raising awareness of the major internet threats and providing top tips on how to surf and shop safely, which will help ensure everyone gets to enjoy a very merry Christmas.

And if you do unfortunately fall victim to an online fraud, please report to Action Fraud on **0300 123 2040** or at **www.actionfraud.police.uk**.

For more online crime prevention advice go to **www.getsafeonline.org** or **www.cyberstreetwise.com**

1 Online shopping fraud

In 2014, 74% of all adults have purchased goods or services online, and this December around 50% of UK citizens are expected to use the internet to buy more than half of their Christmas presents. However, buyers need to be aware that fraudsters are looking to take advantage of this massive demand by creating bogus websites to advertise counterfeit goods and services that are often poor quality/unsafe, or items that will never be delivered.

Top tips to protect yourself

- If possible use online retailers/brands you are aware of and trust. For major brands always go to the official website to find a list of authorised sellers.
- Check the delivery, insurance, warranty and returns policy.
- 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

An increasing number of Christmas cards are being sent via email. Many are genuine; however, be aware that cyber-criminals are creating their own versions, which you do not want to open. The email may contain a virus (malware) that will embed itself onto your electronic device – all without your knowledge – and then collect personal data, financial information, passwords and usernames which can then be used to commit fraud.

Top tips to protect yourself

- 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.

Auction fraud

Auction sites, such as eBay or Gumtree, are a popular way to buy Christmas presents. Whilst the majority of items on sale are genuine, there may also be some items for sale that are either counterfeit or do not even exist. Fraudsters use the festive period as an opportunity to 'sell' popular items such as smartphones, gadgets and 'designer' clothing at low prices on auction sites. Please tread carefully before making a purchase. In reality, the chances are that the goods do not exist or what you receive will be a pale imitation of the legitimate version.

Top tips to protect yourself

- 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 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.

Holiday fraud

During or just after the festive period many people are keen to take a few days away, often in search of some sunshine or snow. With the expense of buying Christmas presents most will be going online on the look-out for a deal. However, it is important to be aware of fraudsters advertising fake holidays on websites or social media. These often come in the form of cheap 'too good to miss' package trips, bargain-booking offers for villas and ski chalets or calls and texts offering tempting last-minute deals.

Top tips to protect yourself

- Always pay with a credit card; if they don't accept 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

There is an increase in online loan applications at this time of year as people seek to cover the costs of the festive period. Fraudsters will exploit this opportunity by intercepting applications to legitimate lenders or by creating their own bogus company websites. You may also be tempted to put your money into an investment scheme which promises high returns and low/no risk.

Top tips to protect yourself

- 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

Creating wonderful memories is a part of the magic of Christmas and what better present to give than tickets to a rock concert or a sporting event? However, there are many bogus websites offering fake tickets. A tried and trusted formula for fraudsters is to offer cheap deals for tickets to events that have already sold out. In reality the tickets do not exist and anyone who tries to buy one will end up losing their money and a memorable day or night out.

Top tips to protect yourself

- 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.
- Make sure you have good, up-to-date anti-virus software on all your electronic devices.

7 Donating to charity

The festive period is traditionally a time when charities seek donations. Most collections and appeals are legitimate but be aware fraudsters are looking to exploit our charitable nature and steal donations. One of the most common ways of doing this is online.

Top tips to protect yourself

- 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.

8 Mobile malware/ malicious apps

Many people will be getting smartphones or tablets for Christmas. Cyber-criminals are constantly developing new ways to infect these devices through malicious apps or through infected websites/URLs. Although most malware is found on the Android operating system there have also been recent cases of strains being developed for Apple's iOS.

Top tips to protect yourself

- Make sure you have the latest version 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.

Money transfers

An authentic online seller will ask you to pay by card on a secure payment page, or occasionally by cheque. However tempted you are because 'it's the last one in stock' or it's 'two days before Christmas', never transfer money directly into the seller's bank account. As well as at Christmas time, there are many situations where you may be asked to transfer money to other people and there are a number of respectable services you can use. But be aware fraudsters are also looking to cash-in by persuading people to transfer money for products and services that do not exist.

Top tips to protect yourself

- Never send a money transfer for online purchases.
- Wait the six or seven working days its 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.

Social media scams

Most of the adverts placed on networking sites such as Facebook and Twitter are genuine. However fraudsters are also advertising give-aways and offers in the hope that people will click on these bogus adverts and be redirected to a website full of scams. Cyber-criminals may also be on the hunt for personal details which can be used to steal people's identities and commit fraudulent transactions.

Top tips to protect yourself

- Do not have too much personal information on social media accounts which could allow your bank accounts to be compromised.
- 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.

11 Dating/romance fraud

Many singletons will be making a New Year's resolution to find their ideal partner and signing up to an online dating website. This can be a great way to find true love but you also need to be on the lookout for fraudsters trying to win your affection and then asking for money to pay for them to visit you or help out with a family problem. Do not listen to promises of repayment – better to sever contact and look elsewhere.

Top tips to protect yourself

- 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.

12 Mobile payments

More and more people are using mobile devices, especially smartphones to make purchases. Data is usually stored in the phone's memory and may be compromised if the device is 'hacked' or stolen.

Top tips to protect yourself

- Do not save passwords or personal/financial data onto 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.

NATIONAL TRADING STANDARDS
eCrime Team
Protecting Consumers
Safeguarding Businesses

FCA
FINANCIAL CONDUCT AUTHORITY

victim support
find the strength