NOT **EVERYONE** IS AS NICE AS **YOU**...

The 12 Online Frauds of Christmas

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE

NOT **EVERYONE** IS AS NICE AS **YOU**...

The City of London Police is committed to preventing, detecting and disrupting fraudulent activities throughout the UK.

Working with the National Fraud Intelligence Bureau (NFIB), Get Safe Online and Action Fraud, we've created the twelve online frauds of Christmas that we suspect criminals may use during the festive period. These have been compiled with the aim of highlighting these fraudulent activities and increasing business and community awareness, together with providing advice to help prevent you from becoming a victim of this type of crime. See Getsafeonline.org for further advice and guidance.

If you are unfortunate enough to become a victim of fraud, it is important that you report it. You can do this by visiting Action Fraud – the UK's first national fraud reporting centre. It provides a single point of contact for fraud victims, where they can both report a fraud and seek guidance and advice. **www.actionfraud.police.uk** or call them on **0300 123 2040**.

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE

NOT **EVERYONE** IS AS NICE AS **YOU**...

1. Shopping Online

Consumers have increasingly turned to the convenience of online shopping, sitting in front of their computers and ordering items from the comfort of their own homes.

Fraudsters will take advantage of this demand and have created bogus websites to advertise goods and services that are counterfeit or will not be delivered.

Items advertised on these bogus sites as genuine will be fake, of poor quality and/or unsafe to use.

In many cases the fraudster will have no intention of sending you anything in return for your money.

How you can protect yourself

- If possible use online retailers/brands you are aware of and trust
- Be cautious when dealing with sellers in other countries
- Check 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
- For major brands always go to the official website to find a list of authorised sellers
- If you are in any doubt do not purchase from the seller

NOT **EVERYONE** IS AS NICE AS **YOU**...

2. Auction Sites and Auction Fraud

Auction sites, such as eBay or Gumtree, are a popular way of buying presents. Whilst the majority of auction sellers are genuine, there are some unscrupulous criminals who use auction sites to offer counterfeit goods or those that simply do not exist.

Fraudsters also use Christmas as an opportunity to "sell" popular items such as smartphones, gadgets and "designer" clothing at low prices designed to catch your attention. In reality, the chances are that the goods offered for sale do not exist and that you will receive nothing in exchange for your money.

How you can protect yourself

- Remember to always use recomended methods of payment for the site rather than making direct payments to a seller
- Research the seller before you bid. If available, check the seller's feedback, be mindful though that this can be falsified
- Be cautious when dealing with sellers abroad or private individuals
- Be aware of the seller's delivery, warranties and returns policy before ordering
- If you are in any doubt at all, do not purchase from the seller
- If you're going to pick up your purchases in person, take someone with you or let someone know where you are going

NOT **EVERYONE** IS AS NICE AS **YOU**...

3. Email Links and Attachments

We've all received emails urging us to click on a link to receive a special offer, or open an attachment containing some great news, or to "confirm details". Sometimes, these are from reputable online stores and banks, but often they are scams and could lead you to reveal your personal details or download malware. If in doubt, delete the email and don't pass it on.

How you can protect yourself

- Reputable companies will not ask for personal/financial information via email
- Never send any information to the sender
- Make sure you have suitable anti-virus software protection installed
- If you receive an email asking you to verify details, and are unsure if it is real, contact the company direct to confirm if it is genuine
- Do not respond to or open attachments from unknown sources
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email
- Do not make purchases or charity donations in response to spam email
- Don't click on 'remove' or reply to unwanted email

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE

NOT **EVERYONE** IS AS NICE AS **YOU**...

4. Holiday Fraud

During the festive period, many people decide to book a bargain break and, after the expense of Christmas, be on the look out for a cheap deal.

Fraudsters will advertise fake holidays via websites or social media, offering cheap "too good to miss" deals, you may even receive a random telephone call or text offering a last minute deal.

If the holiday and price sound too good to be true it usually is.

How you can protect yourself

- Use reputable companies which are members of ATOL, or ABTA protected. Verification of protected status can be completed by contacting the Civil Aviation Authority, The Association of Independent Tour Operators, or The Travel Association (ABTA)
- Checks made with Companies House can help to further determine the legitimacy of the firm
- You should be suspicious if the company encourages you to pay with cash
- If you are told the company does not accept credit cards, you should consider whether you wish to book with them

NOT **EVERYONE** IS AS NICE AS **YOU**...

5. Electronic "E-Cards"

Christmas cards are not only sent by post these days, but also by means of email via an "e-card". Many are genuine; however fraudsters have used this platform to create their own cards. This is one card you do not want to open.

The fraudster's email may contain a virus. Once activated the file will embed itself into your computer – all without your knowledge.

This malware works inside your computer collecting personal data, financial information, passwords, usernames together with tracking your usage. The collected information will then be forwarded to the fraudsters, enabling the fraudulent use of your details.

How you can protect yourself

- If you receive an e-card, check to see where it has come from. If it is from someone anonymous, you should consider deleting it from your inbox as it may be infected
- Use a reputable anti-virus product, that provides you with suitable protection against this type of software and make sure it is updated regularly and is always turned on
- If you believe your computer has been compromised, switch it off and disconnect from the internet. This will prevent any further information from being sent to the criminals
- Contact your bank and consider changing passwords and usernames to prevent any of your accounts from being compromised

Do not use the compromised computer until the virus has been removed.

NOT **EVERYONE** IS AS NICE AS **YOU**...

6. Social Networking Specials

Social networking sites are increasingly used by fraudsters to spread their scams too. So again, if you see a post promising a free giveaway or cut-price offer that seems too good to be true, think twice before you follow it.

Beware that fraudsters also have access to social media, and will use it to obtain and collate personal information about you. They will use this as an opportunity to steal your identity and use the information to commit criminal activities.

How you can protect yourself

- Never openly advertise personal or financial details on social media
- Check your privacy and account settings and limit your page to only those whom you wish to access it. Beware of privacy settings being reset following site updates
- Be suspicious of messages asking for money. Hackers will use compromised accounts to send messages pretending to be friends or colleagues, asking for financial support. If you receive suspicious messages like this, contact your friend or colleague immediately via other means to check the legitimacy of the message
- Be careful about installing third party add-on programs. Again, these can be used to compromise personal information and your computer
- Do not to post information such as your birth date, your first pet, or school as these are normally included in security questions to reset your password. Fraudsters may use these answers to access your account via the "Forgot Password" link

NOT **EVERYONE** IS AS NICE AS **YOU**...

7. Donating to Charity Online

The season of goodwill is traditionally a time when charities actively seek donations.

Most collections and appeals are authentic and legitimate, but unfortunately fraudsters can exploit people's charitable nature and steal money which the donor thinks is going the help the charity. One of the most common ways of doing this is online. Do not stop donating money to the good cause of your choice. Instead, take a few simple precautions to protect yourself, and your chosen charity, against online fraud.

How you can protect yourself and donate safely

- Visit the charity's own website by typing the website address into the browser yourself, rather than clicking on a hyperlink embedded in an email
- Before you donate any money, check that the website you are on is secure. There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register
- If you receive unsolicited emails from charities you have never heard of or have no association with, do not respond and do not click on links contained in them. Report them to Action Fraud and then delete them
- Do not respond to requests to donate through a money transfer company such as Western Union or MoneyGram, as this is a tactic commonly used in scams
- Ensure that the charity is genuine before divulging personal details, or debit/credit card or online banking information
- When supporting disaster relief abroad, you could consider donating via the Disasters Emergency Committee website
- If you are still in any doubt, a legitimate charity will happily advise you on other ways to give on their website or via a phone call
- If you think you may have given your account details to an impostor or bogus charity, contact your bank immediately

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE

NOT **EVERYONE** IS AS NICE AS **YOU**...

8. Making Payments for Presents and Services Online

Using the internet to make payments for Christmas presents or to utility, phone, credit card, insurance and other companies saves considerable time and effort. There are, however, risks associated with online payments and you need to take care when making them.

How you can protect yourself

- Remember that paying by credit card offers greater protection against fraud than with other methods
- Double check all details of your payment before confirming
- Before entering payment details on a website, ensure that the link is secure
- When making a payment to an individual use a secure payment site such as PayPal – never transfer the money directly into their bank account
- Check the website's privacy policy
- Always log out of sites into which you have logged in or registered details. Simply closing your browser is not enough to ensure privacy
- Keep receipts – electronic or otherwise
- Check your bank statements regularly to keep track of what's going out of your account
- Check credit card and bank statements carefully after payment to ensure that the correct amount has been debited, and also that no fraud has taken place as a result of the transaction
- Ensure you have effective and updated anti-virus/anti-spyware software and firewall running before you go online

NOT **EVERYONE** IS AS NICE AS **YOU**...

9. Transferring Money

An authentic 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 "two days before Christmas" never transfer money into the seller's account, you may never see the goods or your money.

As well as Christmas time, there are many situations in which you may be asked to transfer money to other people – whether it is travel, education, family emergencies, or family support.

There are a number of long-established, highly respectable money transfer services commonly used for this purpose. Like many legitimate services, however, fraudsters can use them to take advantage of unsuspecting people by getting them to transfer funds for products and services that do not exist.

How you can protect yourself

- Never send a money transfer for online purchases
- Never send funds from a cheque in your account until it officially clears—which could take weeks
- Never send money in advance to obtain a loan or credit card
- Never send money to someone you have not met in person
- Never send money to pay for' taxes' or 'processing fees' on lottery or prize winnings
- Never provide your banking information to people or businesses you do not know
- Never send money for an emergency situation without verifying that it is a genuine emergency
- Never open an attachment from, or click on a link in, an unsolicited email claiming to be from a money transfer service

NOT **EVERYONE** IS AS NICE AS **YOU**...

10. Voucher Fraud

An increasingly popular method of paying for goods and services is that of pre-paid cash vouchers or electronic money designed to allow consumers to make purchases online without using a debit or credit card. Each voucher will have a unique serial number or code that can be used to purchase items from an authorised online retailer.

Criminals will attempt to fraudulently obtain these voucher codes. An example of a common method would be:

Fraudsters will infect your computer with a type of virus known as "Ransomware" which will lock your computer and then pretend to represent a trustworthy organisation such as the Police, claiming you have committed an offence. A message will ask for payment to release, with only one option of using a voucher, via an online link.

How you can protect yourself

- Only use voucher codes with authorised partners that are officially recognised by the issuer
- Never email, or give out a voucher code over the telephone, unless you are sure of the recipient
- Treat your vouchers as if they were cash
- Never purchase vouchers from third parties or unauthorised distributors
- If you are in any doubt about the use of the vouchers, check with the issuer
- There is a risk that your identity details could be compromised. Fraudsters could steal your identity and use it to access your personal finances or obtain goods or finance from alternative sources

NOT **EVERYONE** IS AS NICE AS **YOU**...

11. 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 high profile sporting events? It's natural to want to find a special day or evening out at the lowest price we can find. However, there are many bogus websites that advertise these artificial deals.

Fraudsters will normally offer extremely cheap deals that are very appealing and are in high demand at events that have already sold out. The tickets advertised do not exist and the criminal will have only one thing on their mind – stealing your money.

How you can protect yourself

- If shopping online, always remember to log out of any websites where you have entered your card details
- Only purchase goods and services from reputable websites that are secure.
- Avoid entering your bank or credit card details on public or shared computers
- Do not use an insecure WiFi connection. This may allow other users to compromise your computer
- Make sure you have adequate anti-virus software that will enable your computer to flag any untrustworthy sites
- Always keep an eye on your card
- If you have not done so, ask your card provider about "3D secure" and how to sign up to it
- Don't click on 'remove' or reply to unwanted email

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE

NOT **EVERYONE** IS AS NICE AS **YOU**...

12. Mobile Payments

The use of mobile devices has become more prevalent over the years with the introduction of smart phone technology and applications. Many of us use these devices to purchase goods and services, together with payment transfers.

Data is usually stored in the memory, and may be compromised if the device has been subject to a "hack", or if your telephone is stolen.

Compromised data can then be used to facilitate crime or sold onto other criminals, who will use it to commit fraud.

How you can protect yourself

- Do not save any passwords, personal or financial data onto your mobile device, unless it is absolutely necessary
- Make sure your mobile device is password or passcode protected
- Most mobile devices have the software to wipe all data from the device's memory remotely if it is stolen – learn how this works
- Do not constantly keep your Bluetooth facility on. There is a chance criminals may hack into your device unnoticed. Additionally, insecure WiFi can pose a risk as data can be intercepted if not encrypted
- Consider the use of anti-virus software many new smart phones will have the facility to install anti-virus software to prevent attacks
- Check with the manufacturer or your provider for specific instructions about anti-virus software and security features. It will protect your data getting into the wrong hands, which may be used by criminals

NOT **EVERYONE** IS AS NICE AS **YOU**...

And finally .....

There's a saying "If it seems to be too good to be true, it probably is." This is especially true of the internet, so if you find or are emailed about a bargain that seems just too cheap, it could well be a scam, the item is fake, it doesn't match the description or it simply doesn't exist. If the seller doesn't check out, check out of the website!

USEFUL CONTACTS

The National Fraud Intelligence Bureau
UK fraud intelligence gateway to prevent and detect crime
www.nfib.police.uk

Crimestoppers
Reporting crime anonymously
www.crimestoppers-uk.org **0800 555 111**

Get Safe Online
Advice on how to protect against Cyber crime
www.getsafeonline.org

Acton Fraud the UK's first national fraud reporting centre. It provides a single point of contact for fraud victims, where they can both report a fraud and seek guidance and advice.
www.actionfraud.police.uk **0300 123 2040**

Victim Support
Charity providing information to victims of crime
www.victimsupport.org.uk
0845 30 30 900

Office of Fair Trading
Enforces consumer protection
www.oft.gov.uk

ABTA
Travel companies trade association
www.abta.com

Citizen's Advice Bureau
Free independent & confidential advice
www.citizensadvice.org.uk
0844 111 444

Insurance Fraud Bureau
Working to prevent insurance fraud
www.insurancefraudbureau.org

PhonepayPlus
Regulates premium rate numbers in the UK
www.phonepayplus.org.uk

Retailers against Crime
UK retail membership consortium
www.retailersagainstcrime.org

The Trading Standards Institute
Enforces consumer related legislation
www.tradingstandards.gov.uk

UK Payments Administration
Information about making payments in UK
www.ukpayments.org.uk

For information and advice see our website
www.cityoflondon.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

CITY OF LONDON POLICE