The Twelve Frauds of Christmas

National Fraud Intelligence Bureau

Hosted by

CITY OF LONDON POLICE

The National Fraud Intelligence Bureau (NFIB) is committed to preventing, detecting and disrupting fraudulent activities throughout the UK.

The NFIB has compiled a list of twelve frauds that we suspect criminals may use during this festive period.

We have created the "**Twelve Frauds of Christmas**" with the aim of highlighting these fraudulent activities, increasing business and community awareness, together with advice to help prevent you becoming a victim of crime.

If you have been a victim of fraud, now, or in the past, it is important that you report the matter.

You can do this by visiting the UK National Fraud & Internet reporting centre: **Action Fraud** – www.actionfraud.police.uk or **0300 123 2040**

National Fraud Intelligence Bureau **Hosted by** CITY OF LONDON POLICE

1. Online Shopping

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.
- 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.

2. Postal Fraud

During the festive period, you may receive additional letters and parcels to your address. However, not all these may be for you!

Fraudsters will purchase goods online and often utilise an innocent persons address to smooth the progress of the fraud. Once an item has been delivered to an address a person wearing a "official looking" clothing will approach the address and attempt to take possession of the package or parcel by stating it has been incorrectly delivered.

These parcels are purchased by means of fraudulent activity such as cloned credit card details, and your address used to cover the criminal's tracks.

How you can protect yourself:

- Ask for identification if you are approached by anyone attending your home.
- Do not let anyone inside your home, if you are suspicious in any way.
- Do not sign for anything you have not ordered or are you not expecting.
- Never accept or handle anything you deem suspicious.
- If in any doubt call the police.

3. Auction Fraud

Whilst the majority of online auction sellers are genuine there are some unscrupulous criminals who use auction sites to offer counterfeit goods or those that simply do not exist.

It is not until you received the goods, if at all that you discover them to be fake, of poor quality or unsafe to use.

Fraudsters also use Christmas as an opportunity to "sell" popular items, perhaps generally sold out on the high street, 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:

- 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.
- Check if the auction site provides insurance for the purchase.
- Be aware of the seller's delivery, warranties and returns policy before ordering.
- Never send prepaid voucher codes via email.
- Check the seller is authorised by the voucher issuer.
- If you are in any doubt at all, do not purchase from the seller.
- If it sounds to good to be true it normally is.

4. Holiday Fraud

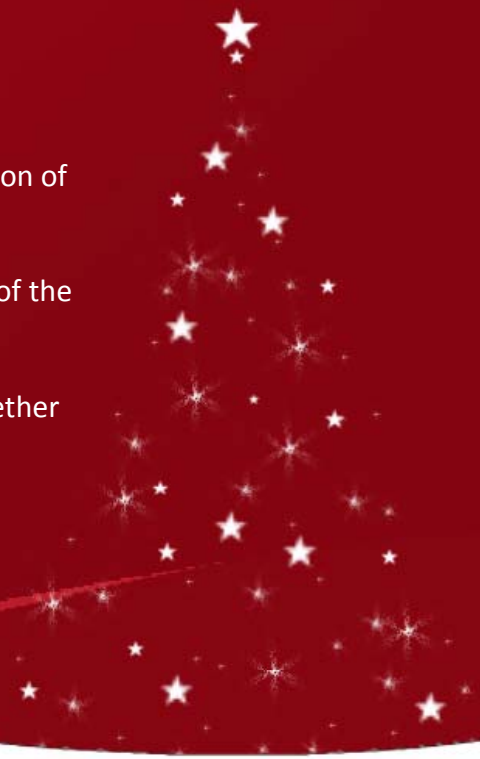
During the festive period, many people decide to book a bargain break and after the expense of Christmas be on the look out for a cheap deal.

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 who 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.
- Checks made with Companies House can help to futher 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.



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 fraudsters email may contain a virus. Once activated the file will imbed 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 considering 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.

6. Ticketing Fraud

From rock concerts, to sporting events, we are always keen for a day or evening out at the lowest price we can find. However, there are many bogus websites that advertise 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 only have one thing in their mind: Stealing your money.

How you can protect yourself:

- Always go to the official website to find a list of authorised sellers.
- Be cautious of previously sold out tickets that have appeared for sale.
- Research the company before you buy tickets.
- Never send prepaid voucher codes over the internet via email.
- Always check to see if the seller is authorised by the voucher issuer.
- Be cautious of telephone numbers starting 070 or 004470. These can be set up on the internet and answered anywhere in the world.

7. Phishing Emails

"**Phishing**" emails are designed to capture your personal information: including but not limited to bank details, addresses, passwords and usernames, basically any information that can be used to commit fraud and steal your money.

Criminals will send out emails pretending to be from genuine organisations such as banks. The email will usually advise you that your account details need to be verified for security reasons, and to do this you will need to click on a link.

The link will then take you a webpage controlled by the fraudsters, and that has been made to look like the company they are trying to impersonate. Once you submit these details, they are in the hands of a criminal.

How you can protect yourself:

- Reputable companies will not ask for personal/financial information via email.
- Never send any personal information to the sender.
- Make sure you have a 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.

8. Social Networking

Social media allows people to connect with each other all over the world and this ability to connect comes to special prominence during the festive period. Users are able to write blogs, talk about personal experiences and share information with friends, relatives and followers.

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.
- 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 messages truthfulness.
- Be careful about installing third party add-on programs. Again, these can be used to compromise personal information and your computer.
- Try 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.

9. Cash Point Fraud

The use of card traps, skimming and PIN devices, are common methods that fraudsters will use to steal your financial details and commit fraud.

CARD TRAPS - These are devices that are placed on the ATM slot and will "trap" your card inside.
SKIMMING DEVICES - These capture your card details when you place your bank card into the ATM slot.
PIN DEVICES - These devices are placed on top on the original keypad and are designed to capture you PIN.
PINHOLE CAMERAS - These are placed in a position on the ATM, which will enable the fraudsters to record your PIN number as you type it onto the keypad.
SHOULDER SURFING – Suspects may stand behind you and record you typing your PIN into the ATM.

How you can protect yourself:

- If available consider using cash point machines inside banks, rather than on the street.
- Always be mindful of who is around you.
- Always inspect the cash point before you inserting your card.
- If you suspect anything contact Police and the bank immediately .
- Do not attempt to remove the device.
- Report any suspected misuse to your issuer immediately.

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 at 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.

11. Card Not Present Fraud

When using debit/credit card payments for goods and services, the fraudsters will use various techniques to steal and duplicate this method of payment, such as “skimming” at the point of sale, using a secondary device, or via Malware on the victims computer.

Criminals will use your card details to order items online, via the telephone, and by mail order. There is no face to face contact with the transaction. The fraudster can use your card details remotely, from anywhere in the world once they have the details.
Card Not Present Fraud is the most common type of fraud in the UK.

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. A secure website should begin with “https”. The “S” stands for secure. The browser should also normally have a small padlock located on the address bar confirming this.
- 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 and eye on your card to avoid skimming and check your statements regularly.
- If you have not done so, ask your card provider about “3D secure” and how to sign up to it .

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.

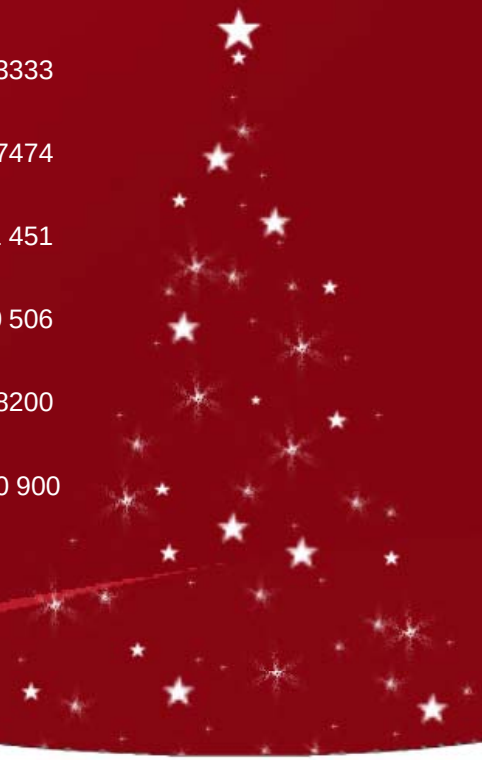
Compromised data can then be used to facilitate crime or sold onto other criminals, who will use it to commit fraud.

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 antivirus software many new smart phones will have the facility to install antivirus software to prevent attacks
- Check with the manufacturer or your provider for specific instructions about virus software and security features. It will protect your data getting into the wrong hands, which may be used by criminals.

Useful Contacts

The National Fraud Intelligence Bureau: UK fraud intelligence Gateway to prevent and detect crime	www.nfib.police.uk	0207 601 6999
ABTA: Travel companies trade body	www.abta.com	
Citizen's Advice Bureau: Free independent & confidential advice	www.citizensadvice.org.uk	0844 111 444
Crimestoppers: Reporting crime anon	www.crimestoppers-uk.org	0800 555 111
Get Safe Online: Advice on how to protect against Cyber crime	www.getsafeonline.com	
Insurance Fraud Bureau: Working to prevent insurance fraud	www.insurancefraudbureau.org	0800 4220 421
Office of Fair Trading: Enforces consumer protection	www.oft.gov.uk	0300 123 3333
PhonepayPlus: Regulates premium rate numbers in the UK	www.phonepayplus.org.uk	0207 940 7474
Retailers against Crime: UK retail membership consortium	www.retailersagainstcrime.org	01786 471 451
The Trading Standards Institute: Enforces consumer related legislation	www.tradingstandards.gov.uk	0845 4040 506
UK Payments Administration: Information about making payments in UK	www.ukpayments.org.uk	0203 217 8200
Victim Support: Charity providing info to victims of crime	www.victimsupport.org.uk	0845 30 30 900



National Fraud Intelligence Bureau

Hosted by

CITY OF LONDON POLICE