Can you avoid the 12 frauds of Christmas?

citizens advice

Derby & Derbyshire age UK

DERBYSHIRE County Council
Improving life for local people

Derbyshire Police and Crime Commissioner
Protecting Communities, Fighting Crime

www.derbyshirescamwatch.org.uk

Online Shopping

Fraudsters will take advantage of this demand and have created bogus web-sites to advertise goods and services that are counterfeit or will not be deliv-ered.

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

Postal Fraud

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

Auction Fraud

Fraudsters also use Christmas as an opportunity to “sell” popular items, per-haps 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

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.

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.

Ticketing Fraud

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.

Phishing Emails

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.

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.

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.

Social Networking

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.

Holiday Fraud

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.

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.