OPERATION SIGNATURE

Protecting vulnerable victims of fraud

Online Holiday Fraud

Scammers are targeting online holiday booking and accommodation sites to scam unsuspecting customers into paying for accommodation that is not available or does not even exist.

What you need to know:

- Scammers will often ask for payment via direct bank transfer
- Scammers will use photos obtained from other legitimate sites. If unsure check photos with a reverse image search.
- Scammers may state they belong to a trade body or protection scheme (ABTA). Contact these schemes.
- Research the property and see if they have their own website.

Dating and Romance Scams

Scammers are using many legitimate dating and social media websites to scam individuals. They lower your defences by building an online relationship with you.

What you need to know:

- Be wary of giving out any personal information
- Scammers will often show glamourous photos of themselves to gain your trust. But how do you know it is them?
- Scammers will make conversation more personal to draw more information from you
- Once trust has been built scammers will try to change their means of communication to email, text and possibly phone.
- Scammers will target your emotions and get you to part with money (ie death of relative, stranded in a foreign country)
- Never send money abroad (via Moneygram, Western Union)
- Scammers will request you keep your online relationship a secret
- Scammers may ask you to accept money from them into your own bank account. By doing this you may be committing a criminal offence of money laundering

Ticketing Scams

Scammers are taking advantage of the demand for tickets by creating fake sites offering these sought after tickets.

What you should know:

- Scammers website will offer tickets that are sold out or not yet available
- You may receive tickets, turn up to an event and then be told the tickets you hold are in fact fake.
- Scammers may tell you a representative will meet you at the event and then not show up.
- Paying for tickets via credit card offers protection under the CCA.
- You may be able to find reviews for the website you are about to use.
- Remember the only way to avoid being scammed is to buy tickets from the promoter, venue box office or reputable ticket exchange site.

Online Shopping and Auction Fraud

Scammers are using online shopping scams because they can hide their identity using the internet

What you should know:

- Scammers will try to encourage you to leave a legitimate site to complete a sale. This could lose any payment protection the legit site offers.
- Scammers will often over emphasis words such as ‘authentic’ or ‘genuine’
- Never pay for a vehicle without viewing it and the relevant documentation first. You may be offered discount if you pay before seeing. Don’t!
- Just because a website say its .co.uk doesn’t mean it is based in the UK. Check phone numbers and addresses.
- Beware when selling items online. Scammers can enter a low bid and then using a different user log a high bid. Towards the end of bidding the high bid will be removed.
- Research sellers and bidders history. Also look at reviews for websites.

Internet Scams

Many internet scams take place without the victim noticing. Scammers may attempt to put programs on your computer that can steal, wipe or lock your data.

What you should know:

- Scammers can use the internet to promote fraud through unsolicited or junk emails known as spam. Always delete these emails.
- Any email you receive that comes from an unknown sender is likely to be spam.
- If you receive an email from an unknown source which contains an attachment (eg invoice). **DO NOT** open it. This may contain a virus
- Online market places can save you money. But they are also used by scammers. Scammers will try to steer you away from legit sites and request you use unusual payment methods.
- Websites can be very sophisticated. Make sure you do research before committing to any purchase
- Be care of bogus official looking websites, claiming to assist in applying for passports/driving licenses.
- **NEVER** give personal or financial details to anyone unless you know and trust them.

Protecting your computer

- Keep your security programs such as antivirus and firewall, up to date. Make sure your web browser and operating system are the latest version. If unsure contact a computer specialist.
- Be wary of opening links on unsolicited emails you may receive.
- Know how to verify secure web sites if making financial transactions. A padlock will appear in either the bottom left or right corner of the browser bar. Not the website.
- If you receive an email claiming to be your bank, think about whether it is genuine. Close the email, visit your banks website and contact them via your normal method.
- If its too good to be true, it normally is!