JERSEY FRAUD PREVENTION FORUM NEWSLETTER

NOVEMBER 2022

Message from the Chair

Welcome to the latest edition of the Jersey Fraud Prevention Forum newsletter. So far during 2022, the States of Jersey Police have received a total of 83 reported frauds and scams. This year the biggest loss was with Bitcoin and crypto investment scams as islanders lost £176,450. Crypto is a new and emerging sector, and we remind islanders to treat it like any other sector and report any suspicions you have.

The second biggest loss the island saw this year was due to Romance Fraud, with islanders losing £130,500.

We know when it comes to matters of the heart it can sometimes feel embarrassing to come forward or to recognise that you have fallen victim. We want to remind islanders that we are here to help and that if you suspect you or a friend or family member has fallen victim that you can also speak to any of our Forum members.

Merry Christmas and remember to be vigilant!

Chief Inspector Chris Beechey
Chairman of the Jersey Fraud Prevention Forum

Jersey fraud victims in numbers

There have been a total of 83 victims of reported scams and fraud in Jersey in 2022, with a total loss of £403,902.

Some of the biggest scams include:

Bitcoin and crypto investment scams

£176,450

Banking scams
£35,417

Online shopping scams (Some examples include a pet purchase, a boat, false Ebay listings, and event tickets)
£19,942.00

Romance fraud
£130,500

WhatsApp scams
£7,149

Protect your personal data when shopping online

Online users should be aware of the risks which are more than just securing our credit card information. Here are some top considerations to protect your privacy and security when shopping online:

- Double-check URLs are legitimate
- Use strong and secure passwords
- Use a secure network when mobile shopping
- Use an official online shopping app if available
- Think before you click, especially with email links

Find out more on our website with the QR code.
Contact the Jersey Office of Information Commissioner by calling **716 530** or emailing **enquiries@jerseyoic.org**

Report it!

If you think you have been targeted by fraudsters or fallen victim to a scam and lost money, you should report it to one our members or the States of Jersey Police on 612 612.

Be careful who's messaging you this Christmas

Action Fraud has reported that there has been a £1.5 million loss due to WhatsApp scam messages posing to be from family and friends in 2022.

What it looks like

Hi Mum
This is my new phone number that old number can you delete. I have to look for a new phone.

Who are you?

My phone broke. I have to get it fixed or buy a new one...

Who do you think??????????????????????

How it works

Criminals claim to be a family member and will usually begin the conversation with "Hello Mum" or "Hello Dad."

They will say that they are texting from a new mobile number as their phone was lost or damaged.

They will go on to ask for money to purchase a new phone, or claim that they need money urgently to pay a bill.

The criminal will supply their bank details for payment, with some coming back on multiple occasions until the victim realises they've been scammed.

If you or a loved one has received this type of message, please report it!

Christmas parcel delivery scams might leave you in the cold

Islanders are being targeted by clone parcel deliveries from places like DPD, Royal Mail, and Amazon, stating that your package couldn't be delivered with a link to pay a re-delivery charge.

Fraudsters are always adapting how they target victims. We are now seeing messages encouraging victims to download an app. If installed, it can steal your banking details, passwords, and other sensitive information. The app also accesses your contacts.

Be scam aware and do not:

- Click on any of the links.
- Reply to the email or text message.
- Open the attachment as it may be a virus.
- Install any apps if prompted.

Instead:

- Use the official websites of delivery companies to track your parcel; check that the courier email address is legitimate by searching their website using a different browser.
- Ring the business by finding their phone number on their website - do not use the number or a link from the email.
- Delete the message without reading it if it is from someone you do not know.

International Fraud Awareness Week 13 - 19 November 2022

Come and see us for a free cupcake – it's NOT a scam!

We will be opposite Voisin on **Friday 18 November 12:00 – 14:00** to help raise awareness of frauds and scams for International Fraud Awareness Week.

Our Forum members will be on hand to chat, exchange fraud experiences and to provide guidance on fraud prevention. Sharing experiences helps to protect others.

How to stay jolly while online shopping

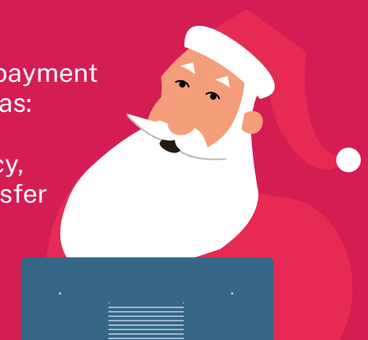
We all love a good deal! And the winter months are full of them: Black Friday, Cyber Monday, Christmas shopping and January sales. Online shopping has become a staple convenience in our modern lives and we are warning islanders to be extra careful.

If something looks too good to be true, you can:

- Visit websites of other retailers offering deals on the same product and do some price comparison shopping before you click "purchase."
- Look out for strange wording or spelling and grammar mistakes, as it's common for fake sites to be run out of countries where English isn't the first language.
- Type the website address into Google's Transparency Report to see the site's safety rating from Google.
- Use "Wayback Machine" site at www.archive.org to look up a website and see older versions of the website.
- Buy elsewhere - if a site asks you for information that seems too personal or unnecessary for the transaction; reputable sites will allow you to pay with secure methods, such as credit cards, debit cards or PayPal.
- Type the company's name and "scam" into Google and see if there are any complaints about the site or if others have reported it as a scam.

Here are the warning signs you should look for on shopping websites:

- Poor website design and broken English.
- Suspect domain name including extra word in the URL like "deals", "sales", "discounts."
- Recently established website especially for well-established brands.
- Bad reviews.
- non-standard payment methods such as: money order, crypto-currency, cash, wire transfer or a prepaid gift card.



Avoid scams when booking holidays

All you want for Christmas is... NOT giving your money away to fake holiday booking agents or clone hotel website owners. With the strong travel demand, scammers are exploiting new ways to target people by fraudulent payment instructions.

You might find out that you never booked that holiday after all and might never see your money again. In some cases, you might be charged an extortionate booking fee, which you will only learn about from your invoice or bank statement.

Protect yourself online when booking your holiday:

- Beware of fake emails, websites, texts, and social media posts.
- Never click on links that you're not expecting. Fraudsters design them to capture your personal information or infect your device with malicious software.
- If the offer seems too good to be true, it probably is.
- If you find accommodation on a third party website - it could be a scammer, encouraging you to pay through a fake website.
- Always check the reviews.

Report it!

If you think you have been targeted by fraudsters or fallen victim to a scam and lost money, you should report it to one of our members or the States of Jersey Police on 612 612.

Islanders to be vigilant as fraudsters prey on cost-of-living crisis

As the cost-of-living rises, scammers target people under financial pressures, who hope for financial assistance. This gives criminals a thriving environment, misleading individuals into falling victim to crime out of desperation. What to watch out for:

- Online investments and get-rich-quick schemes
- Energy bill rebates
- Business scam fraudulent marketing
- Social media flooded with fake investment adverts
- Fake charity requests
- Property rental scams
- Investment schemes promising high returns. Criminals are cloning websites of legitimate investment firms.

Don't get conned out of your bitcoin

This year islanders lost £176,450 to bitcoin and crypto investment scams. Bitcoin and crypto exist in different locations, are less regulated than other investments, instantly transferable and non-reversible.
Tips to prevent you becoming a victim:

- Never purchase cryptocurrencies without researching who created them, when, and what tech is behind them.
- Never respond to any unknown contact – check the official number.
- Never open hyperlinks or attachments from unfamiliar accounts. Scammers edit hyperlinks to make them look real. Always hover over any links or attachments to reveal the fake website URL.
- Always look for HTTPS in a crypto exchange wallet or URL, this indicates that the site has secured encrypted traffic.
- Always keep accounts separate. Never link crypto brokerage accounts to traditional bank accounts.
- Never log onto your accounts through public Wi-Fi.
- Always place a hold immediately on any transactions. If you receive notice of an unusual activity on your account - report it straightaway!
- Ignore requests to give out private cryptocurrency keys. They control your crypto and wallet access. No one will ask for them in a legitimate transaction.
- Ignore investors that say they can grow your money quickly.

A message for business owners who accept over £12,500 in cash

Local retailers need to be aware that they could, unknowingly, be used to launder money for fraudsters. If you are a retailer who deals with large sums of cash, you might be a target for money launderers. Follow our guide on how to protect your business from falling victim:

airtel vodafone · citizens advice · CERTJE The Cyber Security Centre for Jersey · Jersey Bankers Association · Jersey CrimeStoppers. 0800 555 111 100% anonymous. Always. · Jersey Financial Services Commission · JERSEY CONSUMER COUNCIL

JOIC Jersey Office of the Information Commissioner · Jersey Honorary Police · Jersey Post · JT · Government of Jersey · States of Jersey Police · sure.