

JERSEY FRAUD PREVENTION FORUM

NEWSLETTER

APRIL 2023



Message from the Chair

Welcome to our Spring edition of the Jersey Fraud Prevention Forum newsletter.

Since our last publication in November, the States of Jersey Police have received 36 reports of fraud and scams, which have resulted in monetary losses of £606,250. This unfortunately is the highest loss within a 4-month period that we have ever observed.

Investment scams continue to cause concern, including cryptocurrency, bitcoin, and banking scams and frauds.

We strongly advise all readers to be extra cautious when approaching financial investments. Always consider speaking with family and friends, as well as official advice bodies before you invest. Remember, if something sounds too good to be true, then it usually is.

We are pleased to observe that our recent campaign on romance fraud awareness appears to have had a positive impact on the number of reported cases.

New types of fraud being seen now include event ticket and pet purchase scams. Always do your research on the source you are planning to buy from.

Sadly, after challenging times for hospitality during Covid, the Cyber Emergency Response Team (CERT) have been dealing with an email hacking case within the industry that has resulted in a series of related frauds.

Frauds are becoming increasingly more sophisticated in their nature and scope.

If you think you may have been a victim of a fraud or scam, notify the Forum, its members, or the Police.

We look forward to seeing you at the Jersey Boat Show, where members of the Forum will be joining forces with Crimestoppers. Please come and see us.

Chief Inspector Chris Beechey
Chairman of the Jersey Fraud Prevention Forum

Scams targeting islanders

Investment/Bitcoin/Cryptocurrency Scam - £510.502

The victim is convinced to hand money over to a scammer as an 'investment.'
Many of these scams involve investments in cryptocurrencies such as Bitcoin, as well as NFTs.

Banking Scam - £68,862

Scammers use various techniques to get the bank account details of victims, and then use these details to steal money from the victim.

Mandate Fraud - £5,087

Scammers defraud victims by convincing them to change the details of a regular payment, direct debit or standing order.

Romance Fraud - £4,000

Scammers forge romantic relationships with victims, primarily online. They will then use this relationship to gain money from the victim.

Pet Purchase Scam - £1.525

Scammers falsely advertise pets to defraud a victim.

Online shopping / Ticket Scam - £924

Scammers falsely advertise products and services online to defraud victims. A particular case in Jersey involved a ticket to a music festival.





Get-rich-quick scams

If it looks too good to be true, it probably is!

You might be attracted to online cryptocurrency investments with a promise of high returns. However, this winter, islanders lost £510,502 to investment scams, the majority of which involved cryptocurrency.

Watch out for:

- · Adverts promising high returns and little to no risk
- · Strangers offering unexpected investment opportunities
- · Pressure into making an investment or demanding personal details
- Unclear company information on the website i.e. no company registration number
- Lack of product or service clarity
- Hard-to-understand pitches with a promise of outsized returns, often with spelling and grammar errors

Protect yourself:

- Check the FCA Register online to confirm the firm you are dealing with is authorised
- Check the FCA Warning List online for firms to avoid
- Only use the contact details on the FCA Register, not the ones given by the firm directly
- Seek advice from a financial advisor before making a significant financial decision

www.fca.org.uk

Scammers are using the rising cost of living to defraud people

Scammers are using the cost-of-living crisis to their advantage. Be careful who you give information to. Scammers might claim to be from the Government, giving money to help people who are of pension age, disabled, or on a low income. Always make sure you know exactly who you're talking to. You can do this by hanging up, and calling back any agency or company, on the number they list on their website.

Some of the most common fraudsters try to get money and information from you:

- Pretending to be from the government or HMRC offering help
- Offering a fake investment or financial 'get rich quick' scheme
- Offering rebates and refunds
- Pretending to be from your bank
- Pretending to be an online retailer, like Amazon
- Pretending to help with medical costs or insurance
- Offering help with energy bills

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.



Do you belong to (or run) an association or club in Jersey? Have you ever thought about how the information they have about you, is being kept safe? It's a question that we should all be thinking about by instinct.

If your personal information fell into the wrong hands, it could be a problem for you. Jersey OIC has a super new Community Lead ready and willing to help groups of people understand how to protect personal information.

Sophia Bird has joined Jersey OIC and is keen to meet with community groups to offer guidance (and have a cup of tea and a chat!). So, if you are running a club or association or belong to one that might like Sophia to pop in, why not give her a call on **01534 716530**, or email her **s.bird@jerseyoic.org**.

Jersey OIC's top tip for April

Think twice before sharing your personal information with anyone, in person and online.



Advice on cyber security from Jersey's Cyber Emergency Response Team (CERT)

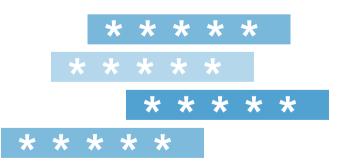
You can also get advice about cyber security by calling **01534 500 050** or emailing **hello@cert.je**.

CERT.JE is run by security experts who can advise on risk and provide expert assistance in the case of a cyber security incident.

They are responsible for promoting and improving cyber resilience and reducing the risk and impact of major cyber incidents amongst Jersey citizens, businesses and community organisations, as well as public services and the Island's critical national infrastructure.

CERT.JE has recently supported issues ranging from nation state cyber-attacks to ransomware and personal social media account takeovers, as well as providing advice on topics such as securing home computers, websites and using online services. You can report security incidents to **incidentreports@cert.je.** Please remember CERT.JE is not a law enforcement service and cyber-crimes should still be reported to States of Jersey Police on **612 612**.





Be wary of charities scams

Scammers are preying on your compassion and goodwill. Locally, we saw scammers calling for donations after the Pier Road tragedy. Other scammers have used the invasion of Ukraine, the Turkey-Syria earthquake and even animal shelters, to get money, or personal information, from people.





Watch out for rogue traders

Trading Standards give free and confidential advice to consumers to help resolve any disputes, but taking some simple steps in advance can ease the process and help your project run smoothly.

Trading Standards are warning Islanders to avoid being taken advantage of when employing traders:

- Never pay cash upfront to traders, especially those who cold-call looking for work.
- Know who you are dealing with. Are they registered with JFSC?
- Ask for a quotation, not an estimate, and get a written contract with timescales and the cost, including GST.
- Where possible get more than one quotation so you can judge if the price is fair.
- Pay by credit card to give you extra protection if anything goes wrong.



Don't be a Money Mule keep your bank account to yourself

Did you know you could be committing a crime if you let someone else use your bank account? You can face criminal charges, fines and imprisonment. You could even be helping someone commit crimes such as drug dealing, people trafficking or even terrorism.

Cases of Money Mules reported in Jersey

- Social media platforms We have seen posts saying "contact me if you want to make legit money." These posts usually target children and young adults, who may not know what they're doing is illegal.
- Romance scams Not all romance scams will ask for money directly. Some have asked victims to allow transfers through their bank accounts.
- Property rental scams Criminals have been reported using money mules in property rental scams. Once they scam a victim pay out of an illegitimate property fee, they will give the money to a Money Mule, to transfer to a different country.

How to protect yourself

- Never give out your bank, personal or security detailsit could be closed, and you may find it difficult to open another bank account or obtain a mortgage in the future.
- Never send money to, or receive money from, people you don't know!































