JERSEY FRAUD PREVENTION FORUM NEWSLETTER

APRIL 2022

Message from the Chair

Welcome to the latest edition of the Jersey Fraud Prevention Forum newsletter. Since the beginning of the year, the States of Jersey Police have received reports of 19 scams which have resulted in monetary losses of almost £300,000, this is close to the total amount lost in 2021.

The biggest losses we have seen have been with an investment scam, cryptocurrency scam and an advance fee scam.

With new and emerging sectors like cryptocurrency becoming increasingly popular, we strongly advise that you approach these as you would any other financial investment. This includes speaking with family and friends, as well as relevant bodies before you invest. Remember, if something sounds too good to be true then it usually is.

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

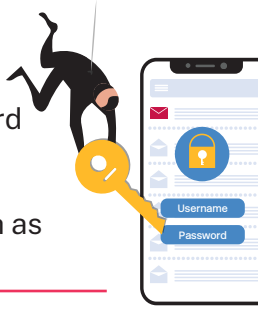
Chief Inspector Chris Beechey
Chairman of the Jersey Fraud Prevention Forum

Cyber threats from Russia

As the world witnesses the atrocities that are occurring in Ukraine, experts suggest that Russia and its sympathisers may respond to sanctions that have been put in place by using cyber-attacks. Although these are likely to target organisations rather than individuals, due to the interconnectivity of the world we live in, it is possible that an attack on a large organisation can affect more people than intended.

Additionally, as we've seen in the past, scammers like to use the fear and interest in these situations to prey on people. Here are some tips to help you stay safe:

- **Be on high alert** – beware of emails or texts asking for donations to the war effort. If you want to donate to any causes in support of the ongoing events, make sure you are donating to a well-known and trusted charity. For example: UNICEF or The Red Cross. You should only donate by going directly to their official website, rather than clicking any links in emails or social media posts.



- **Review your passwords** – expert advice is that password length is more important than password complexity. Choose passwords that are at least 12 characters long. Use three random words to generate strong but memorable passwords, such as "HorseRoadQueen".

- **Keep your software up to date** – make sure you install security updates on your computer when they become available. Also, keep your anti-virus software up to date. If possible, set it to update automatically.

- **Enrol in two-factor authentication** – this will provide you with an extra layer of security by requiring you to complete an extra step after entering a password. This usually works by asking for a verification code from your phone or email.

*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 (01534) 612 612.

Could you spot a romance fraud?

From userTodd246

Message

Hi Mary,

I saw your profile and had to message you, you're gorgeous.

Nice to meet you on here.
How are you, how is your day going?

I'm recently devorced, in the US military looking for a companion. If I found the right person I would definitely consider moving to where they live. What is your profession?

I'm running out of data. If you could send me some money to get more credit we can keep on talking. You can email me or get me on WhatsApp.

All my best,
Todd

Acknowledges distance and offers to relocate for love, playing on the emotions of the recipient of the message.

They will ask you for money so that they can keep talking to you this could be for data, flights or phone bills.

They may try to take your conversation onto another messenger service. This can be so they can hide their conversations and make it easier for monetary transactions.

Small spelling error

Download your go to guide to privacy!

When personal information gets into the wrong hands it can cause harm, embarrassment and distress.

The Data Protection (Jersey) Law 2018 helps to protect us by making sure organisations manage our personal information in a fair and lawful way. But as Islanders, we can all take steps to protect the information that identifies us.

The Jersey Office of the Information Commissioner's Privacy Toolkit is your go-to guide to privacy. It's packed with tips, definitions, explanations and guidance about how you can protect your personal information and learn more about your rights under the Jersey data protection law.

Download the JOIC's Privacy Toolkit at www.jerseyoic.org/itsallaboutyou/

Don't let your phone go roaming on holiday

If your phone is stolen while you're away on holiday, you should contact your local telecommunications provider immediately.

Many people think disabling the device is sufficient, but this does not stop fraudsters from using your SIM card in another phone and racking up huge bills at your expense. Forum partners Airtel Vodafone, JT and Sure are reminding Islanders to inform them about phone theft abroad, so they can disable the service as well as the device, preventing any extra unwelcome roaming charges. Helpful numbers:

Airtel Vodafone - 07829 700121
JT - 01534 882 882
Sure - 0808 1015 247

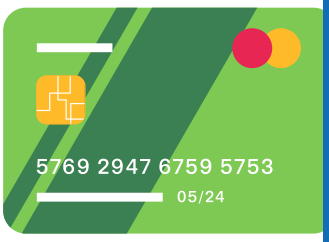
Advice from Action Fraud UK

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online or by contacting the Police.

Charity fraud



Islanders should be extra vigilant after reports of a Microsoft Messenger scam. We've been made aware of a scam where a fraudster befriended the victim over Messenger. They then claimed to be in Ukraine and said that they needed money for a taxi fare.

Given the disruptive times in Ukraine at the moment, the victim was willing to send them this money to help them out. However, this wasn't a case of a person in need, rather a fraudster playing on the goodwill of the victim.

Things to consider before making a payment:

- Do you know the person asking for money?
- Are they trying to rush you to make the payment?
- Has the request come out of the blue?
- If you're unsure if someone is genuine, we recommend asking a friend or family member or your bank to take a look at the request.

Cryptocurrency scams

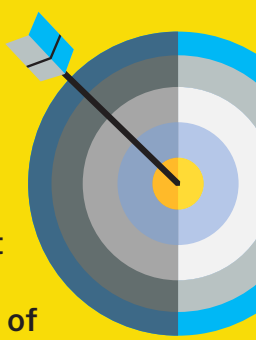
Investment fraud and scams are on the rise. Criminals are sadly exploiting the surge in popularity and excitement around cryptocurrencies to target unsuspecting would-be investors. In Jersey alone, this year we have seen losses of £64,000 in relation to Bitcoin and Cryptocurrency scams.

In order to help protect yourself from these types of scams, Take Five to Stop Fraud recommend looking out for these red flags:

- An aggressive or unrealistic marketing approach.
- Unclear company information on the website. For example, is the company registration number clearly stated?
- Lack of product or service clarity.

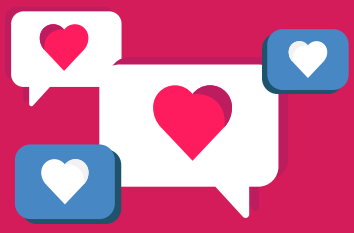
You can find more information on CyrptoUk and Take Five, Stop Fraud's websites.

*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.

Think before you swipe right!



This year so far Islanders have lost £10,000 to romance scams. In a recent cyber security report, Tinder and Plenty of Fish were the top two dating platforms often mentioned in romance fraud reporting. Fraudsters may also use social media or email to make contact.

Females over 40 were a common victim in romance fraud reporting, however, younger males were also targeted, mainly on platforms focused on 'hook-ups' and sexual interactions.

How romance fraud works

- Fraudsters create fake online profiles designed to lure the victim in. They may use a fictional name, or use the identities of real, trusted people.
- Typically they claim to be working overseas in countries suffering from a war or a catastrophe.
- They claim to be in these countries for military service, their profession (doctor or medic) or an aid worker. Their job helps them seem honest, trustworthy and professional.
- They might also try to move your conversation on to another app like WhatsApp, or ask for your email.
- They will then will introduce a situation where they need money quickly. This could be for a phone bill or travel expenses.

WhatsApp scam

Be careful of a WhatsApp scam where fraudsters pretend to be a family member, texting from a different mobile number asking for money. Between August and October 2021, the scam had been reported to Action Fraud in the UK 25 times and cost victims a total of £48,356.

How to check the message:
The best way to ensure the request is real is to ask the person they are claiming to be directly. This could be in person, or via the existing number you have for them. If you have any concerns or if you need to make a report, call the States of Jersey Police on 612612.

Members of the Jersey Fraud Prevention Forum

airtel | vodafone · citizens advice · Jersey Consumer Council · Jersey Bankers Association · Jersey CrimeStoppers. 0800 555 111 100% anonymous. Always. · Jersey Financial Services Commission

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