# JERSEY FRAUD PREVENTION FORUM NEWSLETTER

APRIL 2021

## Almost £400k lost to fraud and scams in the last six months

**The States of Jersey Police received more than 50 reports of frauds and scams between August 2020 and March 2021, which saw islanders lose nearly £400,000.**

These frauds included romance fraud, mandate fraud, property rental scams, sextortion, banking scams and parcel delivery scams.

Forum Chair, Chief Inspector Chris Beechey, is asking Islanders to remain vigilant and to report these scams to the Police:

"Working with our members and different organisations, we try our best to return lost funds to victims, but sometimes unfortunately this doesn't happen.

That's why it is so important that Islanders stay alert to sophisticated scams and let us know if they think they have been targeted.

The second lockdown has again limited our social interactions, which has led to changes in the types of frauds and scams being reported to us. Being cut off and isolated from our usual social networks can make us more vulnerable to fraudsters.

We hope our newsletter will raise awareness and better equip Islanders to detect and report these crimes. If you think you are being or have been targeted, contact the Police and your bank as soon as possible."

## 100% increase in reported scams and frauds

**According to the States of Jersey Police, so far in 2021, they are receiving on average 12 reported scams and frauds each month. This is almost double the number reported in 2020, where in the first half of the year, there were on average seven each month.**

If you think you have been targeted by fraudsters or fallen victim to a scam and lost money, you should report it to your bank and the States of Jersey Police on (01534) 612 612. For more information on the Jersey Fraud Prevention Forum visit fraudprevention.je

## Types of scams targeting Islanders

**Parcel delivery scam**

DPD / Royal Mail email stating parcel couldn't be delivered with a link to pay a re-delivery charge. Additional money is then taken from the victim's account.

**Sextortion**

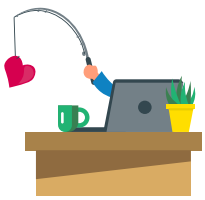
Scammers blackmail victims by threatening to share video content or photos of them of a sexual nature.

**Mandate fraud**

An employee is tricked into changing a regular payment ie a bank transfer after receiving a request over email from a colleague/supplier. But it's a fraudster impersonating the contact...

**Bank account scam**

Victim receives an urgent call claiming to be from their bank and investigating bank staff. They tell the customer to move their money to a safe account. But it's the scammer's account.



**Romance fraud**

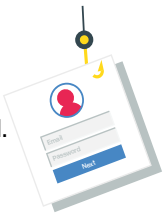
Emotional fraud when scammer pretends to be in relationship with victim then extorts large sums of money.

**Property rental scam**

Victims pay deposits for fake rental properties listed in Jersey.

**Amazon account scam**

Customer is told their Amazon account has been compromised. Scammer obtains bank details then clears their account.



# Hang up - don't be held up

**A customer of a local bank recently avoided handing over all the funds in their current account to fraudsters thanks to their bank's swift action.**

The customer received a call from a fraudster who claimed to work for the National Crime Agency and was investigating staff at the bank.

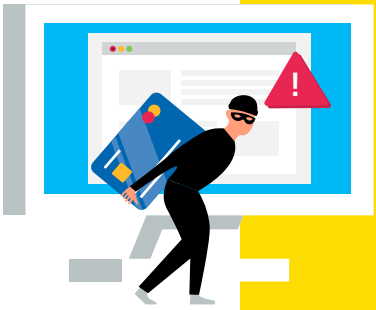
The fraudster convinced the customer that their account was at risk and that they needed to move their funds to a new 'safe account'. The customer gave the fraudster access to their computer and the fraudster then transferred money to their account. The bank flagged the transaction as suspicious and stopped it.

The fraudster then told the victim to call the bank's fraud team and advise that the payment was genuine. The customer had a lengthy discussion with the bank who identified that the customer was being targeted by a fraudster.

On this occasion, the bank was able to successfully prevent the customer from falling victim, but not everyone is so fortunate.

**Remember:**

- **If you're contacted by someone you've never heard of, whether it's a company or an individual, the chances are it's a scam.**
- **If you're asked to give an immediate answer, hang up. Scammers want you to part with your money immediately, so they'll say things that may make it difficult for you to say no.**
- **If you're asked for personal details such as your bank account number and PIN number, this is a sure sign it's a scam. Reliable companies or your bank would never ask for this information.**
- **If in doubt, hang up.**



# Where have you sent your rent?

**We've seen Islanders lose thousands of pounds to rental scams in the last seven months. This is when fraudsters post adverts for rental properties they do not own and get potential renters to send deposits in advance of viewings.**

The fraudsters put pressure on people to pay upfront to secure the property, claiming they've been inundated with interest. Some fraudsters even set up viewing appointments then don't turn up.

The adverts are very convincing, using pictures and addresses from legitimate Jersey property websites and the names of local people as the contact.

**Stay savvy:**

- **Don't send money to someone claiming to be a landlord or an agent until you have viewed the property and can verify the advert is genuine.**
- **Be wary of adverts that seem too good to be true. For example, cheaper rent and deposit charges than other properties of a similar size, or extra benefits (such as a swimming pool) that aren't usually available in the same price range.**
- **Be sceptical if you're asked to transfer funds via a money transfer service such Western Union.**

# Stop cyber criminals profiting from your business

No matter the type or size of your business, it's likely that some element of your work is carried out online. The threat of cyber criminals keeps increasing, which means that businesses need to put controls in place to reduce the risk. The following controls are a good place to start:

- **Understand what you have –** Identify your critical assets (for example your computer systems or payment machines) and conduct a risk assessment against them. This will help you understand and prioritise what security you need.
- **Incident management –** Put an up-to-date and tested incident response plan in place. This will help minimise potential loss of money and time by containing and managing any incidents that arise.
- **Staff training and awareness –** Teach your staff how to recognise phishing scams - what to look out for when working remotely and what to do if they identify an incident or data breach.
- **Access control –** Only give employees access to the data and services they need to do their job. This reduces internal risks and the impact of a data hack or breach.
- **Patch management –** Install updates as soon as they are available. Cyber criminals look for businesses who are slow to update their systems to exploit vulnerabilities.
- **Secure configuration –** Remove or disable unnecessary functions. Default set-ups for many devices, software, and services are often extremely open. This is particularly important for businesses using Cloud services.

# A delivery you aren't expecting

**Islanders have recently been targeted by a scam email claiming to be from DPD about a delivery. The email claims that DPD tried to deliver a parcel and now want to reschedule delivery, but there's charge....They include a link in the email for the recipient to make the redelivery payment. These scammers use 'spoofing' to make their correspondence with you look legitimate.**

According to Action Fraud, UK residents lost £242,000 to this particular scam between June and December last year.

DPD won't ask for a redelivery charge and have three genuine email addresses: dpd.co.uk; dpdlocal.co.uk; and dpdgroup.co.uk.

**If in doubt about any correspondence, remember:**

- **Check the 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 all messages without reading them if they are from someone you do not know. If you open it by mistake and it has an attachment, do not open the attachment as it may be a virus.**

# Spot the difference? How to identify a clone firm

**According to the UK's Financial Conduct Authority, consumers lost nearly £78 million after investing in fraudulent finance clone firms between January and December 2020.**

Clone financial firms are set up by scammers using the name, address and registration number of real companies. Locally, these real companies would be regulated by the Jersey Financial Services Commission (JFSC).

Typically clone firms offer investments in products such as bonds, shares, foreign exchange and cryptocurrency that are non-tradable, worthless, overpriced or even fictional. Some clones offer services to get a loan or charge a fee in advance to recover money from previous investments.

Fraudsters send potential investors marketing materials linking to websites of legitimate firms. They cold-call or make contact by email or social media and try to get Islanders to invest.

**Protect yourself from clones:**

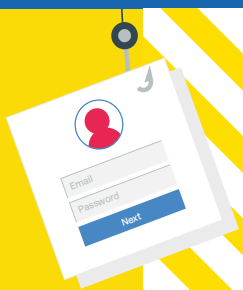
- Remember: if it sounds too good to be true, it probably is.
- Decline unsolicited investment offers whether made online, via social media or over the phone.
- Be wary if you've been asked to pay upfront.
- Always check the JFSC's list of regulated businesses to make sure you're dealing with a licenced firm. Also check the JFSC's warnings and public statements.
- Check business addresses by searching the Registry on the JFSC's website.
- Check telephone numbers, websites and email addresses by researching the firm and looking out for subtle differences.
- Get impartial advice before you invest.

# Know your rights with your personal data

Sharing your personal information can make life easier and more convenient. But, if it's not protected correctly or used in the right way, it can also be a gold mine for fraudsters. That's why it's important to control how and who has access to your data.

The Data Protection (Jersey) Law 2018 gives you rights over your personal information. These rights cover requesting copies of your information, knowing how your personal information is being used, requesting your information is erased, and objecting to its use in certain circumstances. In short, staying in control of your data!

For more information, guidance and templates about your personal information rights, visit the Jersey Office of the Information Commissioner's website jerseyoic.org and click 'FOR INDIVIDUALS' or call the JOIC team on (01534) 716530. For updates, follow JOIC on Facebook, Twitter, LinkedIn and Instagram.




# 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 your bank and the States of Jersey Police on (01534) 612 612.**

**For more information on the Jersey Fraud Prevention Forum visit fraudprevention.je**

# Don't get caught out by lockdown love

## The States of Jersey Police have reported an increase in romance frauds in the Island.

**Romance fraud** is defined as scamming someone out of money or personal information by pretending to want a relationship. Scammers dupe people into sending money to them, by gaining their trust and convincing them that they are in a genuine relationship. They use language to manipulate, persuade and exploit, so that requests for money do not raise alarm bells.

Requests for money might be highly emotive, for emergency medical care or transport costs to visit the victim. However, sometimes the scammer will subtly obtain personal information, to commit identity fraud.

According to the Online Dating Association, more than **23 million** people across Britain used dating apps during the initial lockdown. This type of fraud often starts with online dating websites, but quickly switches to social media or texting.

UK Finance reported a **20%** increase in bank transfer fraud linked to romance scams in **2020** compared to **2019**.

**Action Fraud** also reported an increase in romance fraud in 2019 and 2020, with people losing **£68m** in dating scams last year alone. The Covid-19 pandemic has added to the problem - lockdowns and restrictions on our social lives have led to more people seeking companionship online.

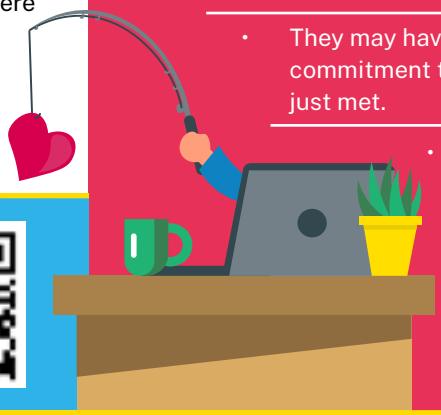
Many victims do not report romance scams because they are embarrassed or ashamed. But for those who do, there is some recourse. In 2019, the Banking Protocol was set up, where banks agreed to a voluntary code where if someone "has taken reasonable care and has any element of vulnerability" they are more likely to receive a refund.

## How to stay safe

- Don't share any personal or family details.
- Don't send or transfer money, or take out a loan on the other person's behalf.
- Don't allow the other person to access your bank account.
- Don't hand over copies of personal documents e.g. your passport or driving licence.
- Don't invest money on the other person's advice.
- Check if the person is using fake images on their dating profile by doing a reverse image search on a search engine. Ask a friend or family member to help you if you don't know how to do this.
- Always contact your bank immediately if you think you have been scammed. Report it to the States of Jersey Police on (01534) 612 612.

## Signs a loved one may be involved in a romance scam

- They may be very secretive about their relationship or provide excuses about why their online partner has not video called or met them in person.
- They might become hostile, angry, and withdraw from conversation when you ask about their partner.
- They may have very strong emotions and commitment to someone they have only just met.
- They may have sent, or are planning to send, money to someone they have not met face-to-face. They may take out loans or withdraw from their pension to send money.



**We want to hear from you - scan the QR code to take part in our 2021 spring newsletter survey.**

### 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 Post · JT · Government of JERSEY · sure.

To the best of our knowledge, the information contained in this newsletter is accurate and reliable as of the date of publication. However, we do not assume any liability for the accuracy and completeness of the above information.