JERSEY FRAUD PREVENTION FORUM NEWSLETTER

NOVEMBER 2023

The JFPF will be at Charing Cross, on **Wednesday 15 November** as part of Fraud Prevention Week. Come along between **11am and 3pm** to speak to our members and get advice on how to avoid being scammed.

Think Christmas - Think Data Protection

As the festive season approaches, safeguarding your personal information is paramount. Follow these top tips to protect yourself this Christmas:

1. Shop safely - Stick to reputable websites and apps for online purchases and avoid clicking on suspicious links.

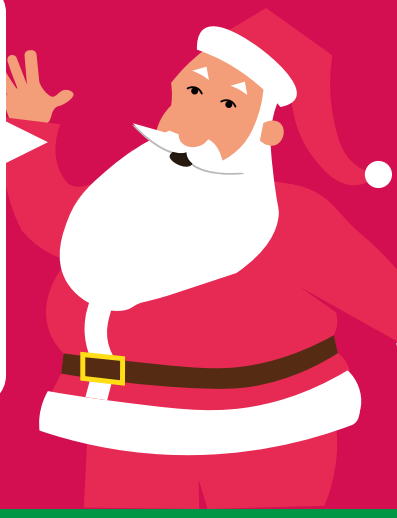
2. Be mindful on social media - Limit sharing sensitive personal information like travel plans and adjust privacy settings to control who sees your posts.

3. Beware of scams - Stay vigilant against e-Christmas card scams and fake emails. Avoid opening attachments or links from unknown sources.

4. Secure your devices - Update your devices and apps regularly to ensure you have the latest security patches. Use strong, unique passwords and enable two-factor authentication.

5. Avoid public Wi-Fi for sensitive transactions - Public Wi-Fi networks are often unsecured. Refrain from conducting financial or sensitive transactions when connected to public Wi-Fi.

Enjoy a safe and secure Christmas, keeping your personal information protected. If you have any concerns about the way your personal information has been used, contact the Jersey Office of the Information Commissioner on **01534 716530** or email **enquiries@jerseyoic.org**



Islanders lose over £2.5m to scams between April and August

From just April to August, there have been 91 victims of fraud in Jersey (87 individuals and four businesses). People aged 71 - 90 make up a quarter of these victims. According to the UK National Crime Agency, 86% of fraud goes unreported. These numbers only show a fraction of the picture.

Invoice and mandate scams - **£2,001,725**
Investment scams - **£258,713**
Banking impersonation scams - **£172,901**
WhatsApp impersonation scam - **£45,400**
Facebook scams - **£28,005**
Romance scams - **£16,500**
Online employment scams - **£11,538**
Debit/credit card fraud - **£8,470**
All other scams - **£8,007**
Holiday booking scam - **£6,000**
Tax scams - **£3,627**
Property rental scams - **£1,800**

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

Protecting yourself this Christmas

Fraudsters and scammers can target us in many different ways, but there are some key habits you can use to protect yourself and your personal information:

1. Have you been contacted out of the blue with an unexpected request or asked to take urgent action? If so, ask yourself if it passes the "makes sense test" and proceed with caution, these are some of the most common ways fraudsters and scammers will try to steal your information and money.

2. Are you being asked to click on a link to provide details or to take action? Stop, think about what you are being asked to do, and double check if the request is genuine. Web links and phone numbers can be easily spoofed to appear genuine, but they will actually take you to fake websites or call centres.

3. Dating online? Never send money to a person you have not met face-to-face and who you know to be genuine. Romance scammers will try and encourage you into helping pay for an urgent bill, to help them with travel costs to come and see you, or they will trick you into an investment opportunity which is too good to be true.

4. Is it too good to be true? Always consider this whenever you are shopping online or if you are looking to invest. Scammers will try and trick you into believing that an item is sought after or that it is a good deal, or that an investment will give you greater returns with little or no risk.

5. Seeking a rental property? Never pay a deposit or the first month's rent for a property without meeting the landlord or agent in person. This meeting should be at the property you are looking to rent. This is a perennial and persistent issue on Jersey and one that all Islanders need to be aware of. It's also one which Islanders continue to lose large amounts of money to.

Channel Islands Financial Ombudsman joins the Forum

What is the Channel Islands Financial Ombudsman's (CIFO's) general approach when receiving complaints about frauds and scams? CIFO generally receives complaints of this type when the financial service provider (FSP) has refused or is unable to refund the customer the money they lost.

These challenging cases mean both the customer and the bank are considered victims. CIFO will look at the circumstances of each complaint to decide what is fair and reasonable for both parties. Some of the evidence CIFO may examine is whether a customer authorised a payment, if not, the FSP should refund the total value lost.

If the customer authorised the payment CIFO may examine what the FSP could reasonably have been expected to do to prevent the loss, and whether the customer's conduct was objectively reasonable in the circumstances. CIFO may also examine the adequacy of the FSP's security processes and procedures. For example:

- Have the FSPs provided fraud/scam guidance on their websites?
- Does the FSP produce warnings when consumers attempt certain transactions to prompt them to verify the transaction information being inputted?
- Has the FSP addressed the consumer's complaint in a timely manner?
- Do the FSPs have awareness of the type of fraud/scam?

For more information, please visit our website **www.ci-fo.org**. CIFO has also published the below case study which illustrates this issue.