JERSEY FRAUD PREVENTION FORUM NEWSLETTER NOV 2020

Message from the Chair

Welcome to the latest edition of the Jersey Fraud Prevention Forum newsletter. As the Coronavirus outbreak continues to impact many aspects of our lives, we want to take this opportunity to remind islanders to remain extra vigilant, especially when working from home and shopping online this Christmas.

Earlier this year, we reported on Covid-19 related scams targeting the island, including fake text messages claiming to be from the Government of Jersey and bogus testing kits. These scams are still out there.

With the majority of people still working from home, fraudsters are adapting the way they target their victims. Most recently, we have received reports of them posing as representatives from large reputable global companies, such as Amazon, Google and internet service providers to try to obtain banking or subscription details from local residents.

We recently announced that there had been a 73% drop in fraud and scam reports for the first six months of 2020. While this may appear positive, we appeal to islanders to report any instances of fraud, even if you don't fall victim yourself. By notifying us, our members or the Police, you could prevent someone else from being caught out.

Chief Inspector, Chris Beechey
Chairman of Jersey Fraud Prevention Forum

Local business targeted in £130,000 invoice scam

The owners of a local building company are warning other businesses to be extra vigilant after they were targeted in a sophisticated impersonation scam, which saw fraudsters intercept more than £130,000 in invoice payments.

The scammers hacked email correspondence between the business and its customers by diverting emails into a hidden email folder in the business' email account. The owners of the company only realised they had been scammed when a customer contacted them to say they had transferred funds, as requested, into the business' 'new' bank account.

Realising something wasn't right, the business owners and the customer acted quickly, informing the police, their banks and lawyers. Luckily, in this case, they were able to recover 100% of their money, however, some people aren't so lucky.

Commenting on the experience, one of the owners said: "I felt sick, distraught – I couldn't sleep through anxiety. But, now it's over, it's such a relief. I now feel more confident with my understanding of cyber security and the protection that's available."

For tips on how to protect your business from impersonation attacks and phishing, see page 2.

£1 million lost in fake transactions

In 2019, consumers that brought complaints to the Channel Islands Financial Ombudsman lost more than £1 million to authorised push payment scams. This is when fraudsters persuade victims to transfer large amounts of money upfront to their criminal accounts in return for goods and services that don't exist or the customer never receives. Scammers usually target their victims through scam text messages, also known as smishing.

If you are asked to make a bank transfer in advance of receiving a product or service, remember:

- Be wary of offers and goods that seem too good to be true
- Do your checks and make sure the people you are talking to are legitimate
- Always use a secure payment method
- Contact your bank immediately if you think you have been caught out.

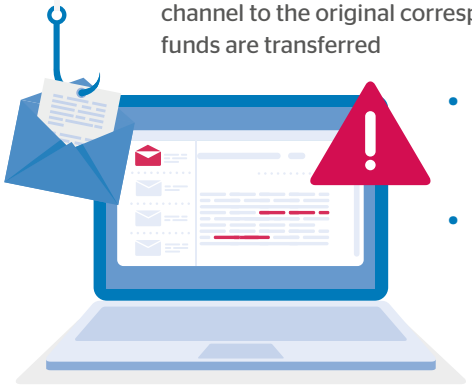
Report it!

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

Who's in your inbox?

When running your own business there are always risks, but your emails shouldn't be one of them. Here are some things you can do to remain vigilant against email scams:

- Invest in an email package and avoid using free email providers like Hotmail, Yahoo and Gmail for business correspondence
- Keep your folders organised and avoid having too many, so you can keep on top of any unwelcome emails
- Invest in the latest software and hardware (i.e. router) available for your business. Cyber security is so important, particularly as communications and payments are often made online
- Before making a payment to a supplier or asking a customer to pay an invoice, follow up and make sure the payment details are legitimate. Do this over the phone or by using another communication channel to the original correspondence, before funds are transferred



- Set up multi-factor authentication on your emails
- Engage an external cyber security provider to do an annual health check on your IT set-up.

Warning from the financial services regulator

Many islanders won't consider themselves investors, but anyone who has some money put aside and needs to make a decision about what to do with it is an investor. The Jersey Financial Services Commission is warning islanders to be extra vigilant if they are considering making or changing investments during the current economic climate.

In times of uncertainty, such as Covid-19 or the financial crash of 2007/8, we do unfortunately see trends of an increase in frauds/scams and also poor professional conduct within the finance industry, with people being mis-led into making high-risk investment choices that aren't suitable for their risk appetite.

When speaking to an investment professional, remember:

- Consider whether it sounds too good to be true
- Only invest what you can afford to lose
- Consider taking a trusted family member or friend with you for a second opinion
- Shop around, visit a few investment professionals to get the best deal for you.

Scammers don't do refunds or returns

With Christmas fast approaching, it's important that we don't rush our festive shopping. It's easy to get swept away with online offers, next day delivery promises and Black Friday sales. It's important that you don't give money or personal details to anyone you don't know or trust. However, if you do get caught out in a scam, there are some ways you could get your money back, depending on how you paid.

Bank card or PayPal

- Your card provider can request the seller's bank to refund the money. This is known as the chargeback scheme which is not a legal requirement and all card providers have different rules
- If you paid by debit card, you can request a chargeback regardless of the amount
- If you paid by credit card and the item cost more than £100 but less than £30,000, you might be able to claim under the Consumer Credit Act - this is known as a 'Section 75 claim'
- If the item cost less than £100 and you paid by credit card, you can't use Section 75, but you can use chargeback.

Bank transfer or Direct Debit

- Contact your bank immediately to let them know what's happened and ask if you can get a refund
- Banks may reimburse you if you've transferred money to someone because of a scam. This type of scam is known as an 'authorised push payment' (see p1)
- If you've paid by Direct Debit, you should be able to get a full refund under the Direct Debit Guarantee.

Continues on next page

Scammers don't do refunds or returns (cntd)

Money transfer service

It's unlikely you'll be able to get your money back if you've paid through a wire service such as MoneyGram, PayPoint or Western Union. However, there are other things you can do, such as reporting the scam to the States of Jersey Police and getting financial or emotional support from Citizens Advice Jersey.

Protect yourself when using a money transfer service by:

- Only sending money to someone you know
- Choosing a password that's hard to guess
- Not sharing your password with others.

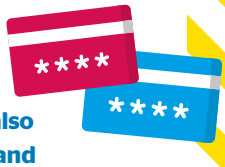
Game of spoof

Our telecommunications providers have seen a recent increase in scam calls and texts to islanders from fraudsters pretending to be from Amazon, Google, HMRC and "your internet service provider". Fraudsters are savvy and will often only make a couple of calls to local residents from of a range of numbers, instead of many calls from one specific number, which makes blocking these calls very difficult.

Airtel, JT and Sure are also receiving increased reports of spoofing. This is when scammers falsify the caller ID display to disguise their identity, so islanders think they are receiving calls from a local number, when in fact it's a scam. If you receive a suspicious call, always be cautious and return the call using a trusted number.

For example, if it's a caller claiming to be from your bank, end the call and call them back using the contact details on the bank's official website or the back of your bank card.

Mobile device malware



The island's telecommunications providers are also warning islanders to be alert to fraudulent calls and text messages being made/ sent from their devices. Airtel, JT and Sure have identified that customers' devices are being hacked by fraudsters and malware is being installed via seemingly innocent apps.

Scammers are then using the customers' service text bundles to send fake texts. These texts often go unnoticed as they don't always appear in call logs or sent messages and may not be charged for as they are included in a bundle.

Make sure you know how to check which apps have access to send text messages from your device – you might be surprised! If you're not sure how to do this, contact your phone provider or look for device specific instructions online.

International reports have highlighted that this issue is rarely seen on Apple iPhone devices but is more common on Android. On these devices, users are able to download apps from a variety of sources and therefore don't necessarily have the same level of security applied.

Gadget gifts that keep on giving

For many, the latest gadgets are at the top of the Christmas list, with those powered by an app or connected to the internet being the most appealing.

But you must remember that they can come with privacy risks that shouldn't be ignored. Gadgets that are internet-enabled provide a more personalised experience, by offering functions such as speech or image recognition. However, the devices also collect personal information, which is like gold dust for potential fraudsters.

Examples include: birthdate, name, physical location, account passwords, profile pictures and credit card information.

Continues overleaf →

Gadget gifts that keep on giving (cntd)

The Jersey Office of the Information Commissioner has the following advice:

- Do an internet search to see whether anyone has raised privacy and security concerns about the gadget before you buy it
- When a gadget asks for personal information, you don't have to hand it over. Consider using a fake name, birthdate and address
- Set a strong password
- Take a look at where your collected personal data is being stored. If it's on the gadget itself, it's less of a concern than if it's on a Bluetooth-connected app or uploaded to the cloud (think third-party server)
- Read the gadget's privacy policy. Understand how your data will be used
- Consider what kind of information the gadget collects. It could collect images, voice recognition and location data. Are you comfortable with this?

Covid-19 update

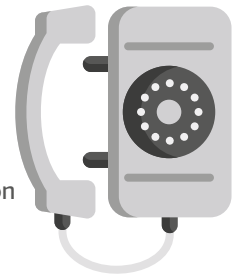
In our last newsletter, we focused on Covid-19 scams and unfortunately they are still happening. Fraudsters are always looking for the next vulnerability to exploit. In this new world with many people still working from home, we will no doubt see an increase in impersonation emails. This can include fake bills or fake invoices asking for speedy payment.

A simple internet search can give fraudsters all the information they need to falsify an invoice or bill. Pair that with a name that you know/recognise and a rushed phone call, and you could be persuaded into authorising a payment.

If you receive an invoice or bill you're not expecting, even if it contains the name of a business or person you know, make sure you check the details before making the payment. A quick call to the company or person requesting the payment could prevent you from transferring money straight to fraudsters.

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 the States of Jersey Police on (01534) 612 612. For more information on the Jersey Fraud Prevention Forum visit **www.fraudprevention.je**



Game - take five

Test your knowledge! Fill out our survey on Facebook to be in with a chance of winning a luxury La Mare Christmas hamper.

Black Friday webinar

On Thursday 19 November at 12:00 we will be hosting our second webinar for the public to learn more about current scams and frauds targeting the island.

This time we will be looking at online shopping scams ahead of Black Friday on 27 November and the festive shopping period. Learn more about the event and our panel by visiting our website.

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.