JERSEY FRAUD PREVENTION FORUM NEWSLETTER NOV 2021

Message from the Chair

Welcome to the latest edition of the Jersey Fraud Prevention Forum newsletter. We want to take this opportunity to remind Islanders to remain extra vigilant of fraud and scams during this festive season.

This year, the Police have received 52 reports of fraud and scams. This is the lowest number reported in the past five years. Although reports are down, we've still seen significant monetary losses with over £100,000 being lost to scams in 2021.

Fraudsters are always adapting to the way we do business and how we invest our money, that's why it is critical that Islanders pay attention to the warning signs and aren't afraid to ask questions when they are unsure if they are being scammed.

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

Chief Inspector, Chris Beechey, Chairman of the Jersey Fraud Prevention Forum

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.

Ho ho no! Scam calls are on the rise

The festive period is a time to be together, however, there are some people we want to KEEP OUT!

We have been notified of a number of scam calls trying to gain remote access to Islander's computers.

One of our Forum partners, the Jersey Consumer Council has seen this first hand.

How a scam call works:

- You receive a call out of the blue from someone claiming to be a computer-security expert from a legitimate company
- They'll say that your PC, laptop or tablet has been infected with malware and that they can help you solve the problem
- They will then trick you into installing malicious software that is able to capture sensitive data
- The scammer will then convince you to visit websites to download software that will allow them to take control of your computer remotely and adjust settings to leave your computer vulnerable.

Three common things to look out for are:

- Urgency – Scammers might give a time limit like 30 minutes to complete the check
- Coercion - they will say that they are there to protect you
- Pressure – The scammer will detail how dangerous it is if the victim didn't do what they said.

Covid snapshot

Covid has had an impact on many aspects of our lives, including how we are targeted by fraudsters. During the pandemic the National Trading Standards reported:

41% of scams involved fake government communications

33% surge in scams between April 2020 and April 2021

54% Of scams related to bogus delivery notifications

60% increase in scams via telephone calls

667% Rise in scams via unsolicited emails

How well does Santa know his scams? Can you connect the scam to the scenario?

A) When a victim is befriended on the premise of starting a romantic relationship by a scammer and persuaded to part with large sums of money

C) When a victim is asked to perform sexual acts which are allegedly recorded. The fraudster threatens to share the content unless the victim pays monies to the scammer

D) When a victim is contacted out of the blue and convinced to invest in schemes or products that are worthless or do not exist. Once the criminals have received payment, they cease contact with the victim

F) When a victim is contacted by a scammer stating they are calling from the victim's bank and that they are investigating the bank staff and money needs to be moved to a safe account – the scammer then has the victims entire bank balance

B) When a hacker gets into and monitors a business email account and sends fake emails to the business posing as a known supplier requesting payments to an account

E) When a victim is sent a DPD / Royal Mail e-mail stating that a parcel couldn't be delivered. The scammer sends a link to pay for a re-delivery charge – additional monies are then taken from the victim

Mandate Fraud

Telephone scam

Sextortion

Romance fraud

Investment fraud

Postal scam

Answers: A- Romance Fraud B-Mandate Fraud C-Sextorion D-Investment Fraud E-Postal Scam F-Telephone scam

Be careful when you treat yo' elf this Christmas

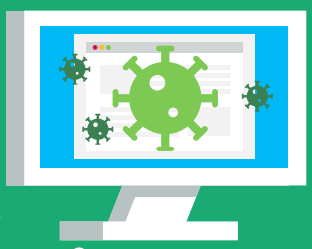
Online shopping is how most of us buy our Christmas presents and with the threat of delivery delays due to shortage of lorry drivers, we might feel pressured to buy NOW!

We're asking Islanders not to rush, remain vigilant and to remember, if something looks too good to be true, then it usually is.

We've also been made aware of scam calls claiming to be from Amazon. A reminder that big online retailers like Amazon won't ring you and ask for your banking details. If you think you're being pressured into something or if the call doesn't sound right, remember you are well within your rights to HANG UP!

Stop, Challenge, Report

Criminals spend hours researching their next scam, coming up with cunning ways to deceive unaware victims. If you're ever in doubt remember:



- **Stop:** Take a moment to think – does this seem genuine and should I speak to a friend or family member before parting with my money?

- **Challenge:** Never feel rushed, it's okay to say no.

- **Report:** If you think you're a victim of a scam, contact your bank immediately and call the police.

Shining a light on privacy

Twinkle, twinkle, little star

Have you thought where your details are?

Up above in clouds in the sky

Are they secured from prying eyes?

Twinkle, twinkle, little star

How I wonder how safe you are

When the Christmas gifts are shared

New smart phones and toys prepared

Signed up online to new privacy rules?

Old equipment factory settings restored?

Twinkle, twinkle, little star

How I wonder how safe you are

Protect your privacy and personal information, only share it with those you trust. For more information about your personal information rights check out the Jersey Office of the Information Commissioner's Privacy Toolkit: www.jerseyoic.org/privacytoolkit

For regular updates follow @JerseyOIC on Facebook, Twitter, LinkedIn and Instagram.

Who is sliding into your DMs?

It's always alarming when we get unsuspected messages sent to us via our social media accounts. Sometimes these people messaging us can have bad intentions and may want to con you out of money after making you fall victim to a romance fraud.

Three things to remember:

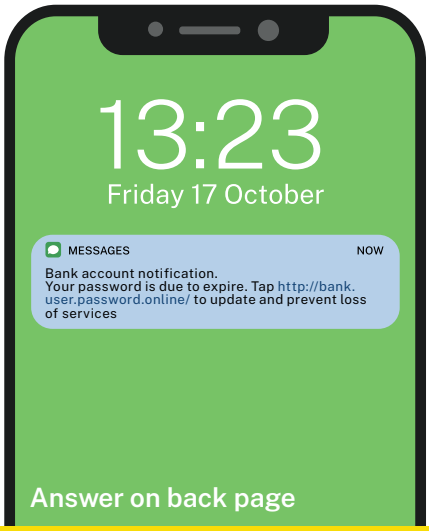
1. Speak to family or friends about who you are talking to.

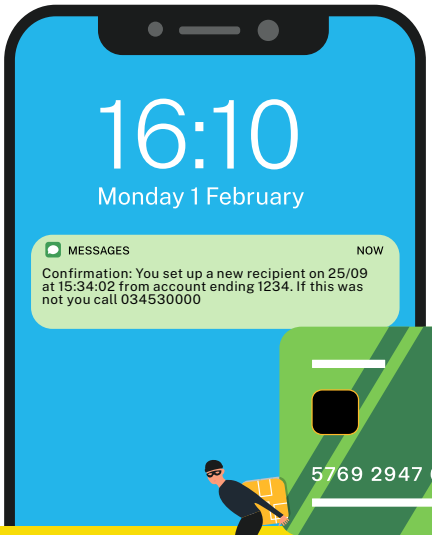
2. Don't send or transfer money, or take out a loan on the other person's behalf.

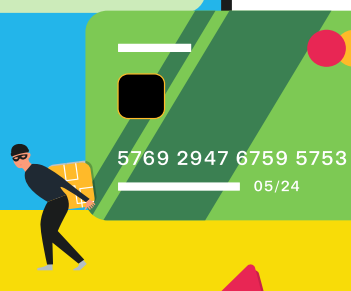
3. Don't allow the other person to access your bank account.

Spot the scam!

Text message scams can be very convincing, so it's important to know what to watch out for to stay ahead of the fraudsters. Choose out of these text messages which one is fraudulent.







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.

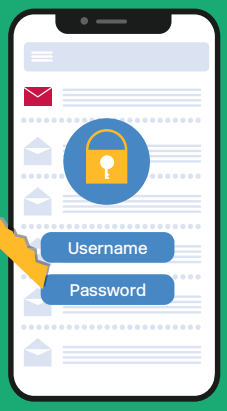
"Double-O-Fraud"

It has been a tactic of fraudsters for some time now to use current events or key calendar moments as subjects for phishing emails and other scams. For example, reports show that in 2020, phishing attacks increased up to 600% with many of the emails capitalising on the fear around COVID-19. For example, they would ask recipients to click on links or open attachments concerning such things as fake charities, incorrect vaccination information, and contact tracing.

Now, researchers are warning that fraudsters are taking advantage of the fact that, since the pandemic, some premieres of new films have moved online to streaming services rather than coming out at the cinema. For example, cybercriminals used the latest James Bond movie, No Time to Die, as phishbait. Researchers found malicious ads and phishing sites are claiming, falsely, to offer free access to the full movie. In some cases, the websites display a few minutes from the beginning of the movie, and then ask users to enter their credit card information to continue watching. However, after the user has registered for the movie, money is debited from their account, the payment (and associated data) ends up in the fraudster's hands, and the victim is left with no movie to watch.

As always, vigilance is key:

- Avoid links promising early viewings of films or TV series. Always check with your TV service provider, to ensure the authenticity.
- Only use official, trusted webpages to watch or download movies.
- Pay attention to the links in emails.
- Check the filenames that you are downloading. For example, a video file should never have a .exe or .msi file extension.



Wordsearch

A	V	G	J	B	V	E	C	J	V
S	C	A	M	C	K	X	Y	G	Q
F	Q	G	C	A	L	A	B	D	F
G	F	Z	N	Y	Q	B	E	S	R
Y	T	G	D	A	T	A	R	Q	A
K	S	N	X	Y	I	N	P	O	U
P	A	S	S	W	O	R	D	V	D
Z	N	Q	S	V	U	E	R	B	S
A	N	T	I	V	I	R	U	S	D
Q	S	M	I	S	H	I	N	G	N
L	N	S	E	C	U	R	I	T	Y

Answer to spot the scam!:
Green phone

Word list:

- Scam
- Fraud
- Smishing
- Data
- Cyber
- Password
- Security
- Antivirus

The JFSC hosted a webinar as part of World Investor Week.

If you would like to learn more about investor fraud you can catch up here:

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.