JERSEY FRAUD PREVENTION FORUM NEWSLETTER

APRIL 2019

Reports of scams and frauds received by the States of Jersey Police increased by 60% last year, compared to 2017.

Thankfully not all resulted in financial losses, with many islanders reporting scams in order to raise the alarm and help the Police issue appropriate warnings. That said, the total number of islanders who reported losing money unfortunately rose by 67% from 2017 to 2018.

Social engineering is constantly evolving and continues to be one of the top methods that criminals use to defraud the general public. Fraudsters are tricking islanders into providing their personal and/or financial details by pretending to be from trusted organisations such as banks, utility companies or the police.

It's thanks to islanders reporting instances of successful and attempted scams that we can form a better picture of how criminals are targeting the island. Please keep reporting because your information could prevent someone else from getting caught out. Working together we can make a stand against scams.

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

REPORT: (01534) 612 612 / PO Box 500 / scams500@police.je

£1 Million lost in bogus Bitcoin

An islander has lost £1.2 million by investing in a bogus bitcoin fund. An experienced investor in cryptocurrencies, the man was scammed by criminals who claimed to work for a legitimate company.

Over a period of time, the fraudsters tricked him into investing his life savings by giving him regular updates on the investment's 'performance' and taking a vested interest in his personal life.

Unfortunately, despite bank intervention, there was no way to recover his money. Police Constable Chris Ingham from the States of Jersey Police commented:

"Following this islander's huge loss, we're warning local residents to be extra vigilant when investing in cryptocurrencies or any investment that seems too good to be true and promises high returns with no risk.

Always get independent advice from a professional, and make sure the company you're dealing with is legitimate."

Deal or No Deal?

Brexit has been all over the media for months and fraudsters will be taking full advantage of the confusion and uncertainty that have surrounded it. It's important that islanders are aware and extra cautious about the risks associated with such a high profile political matter. Stop and think twice about what someone may be asking from you, particularly if they want your personal details "because of Brexit".

Following protocol

We are delighted to announce that Jersey is introducing the Banking Protocol, an initiative which aims to identify and protect potential fraud victims when they visit a bank or building society. Set up in the UK between the police, banks and Trading Standards, this rapid response scheme has led to more than 200 arrests and prevented more than £25 million in attempted fraud. It gives branch staff the means to immediately alert the police if they spot a fraud taking place. The Banking Protocol will be rolled out in the island later this year.

Nothing funny about Spoofing

Our telecommunications partners, Airtel-Vodafone, JT and Sure, are warning islanders to be extra vigilant after a number of customers recently reported falling victim to spoofing. This is when scammers disguise their identity by deliberately falsifying the information that appears on your phone's caller ID display.

Often fraudsters use numbers that are identifiable, for example a bank or credit card line, or our local Jersey area code of 01534. Unfortunately the telecommunications providers cannot block these types of calls as they are generated outside of the island, but recommend any customers who are being targeted should contact them. The most important thing to remember is not to give away your personal information to unexpected and unknown callers.

Scams of the heart

Falling for someone and then falling victim to their deception is hugely distressing. The cost of romance fraud is both emotional and financial.

Fraudsters prey on people's emotional vulnerabilities and trick them into parting with their money and personal information. Last year in the UK, victims lost a total of £50 million in this type of fraud, according to figures released by Action Fraud. To avoid financial heartbreak:

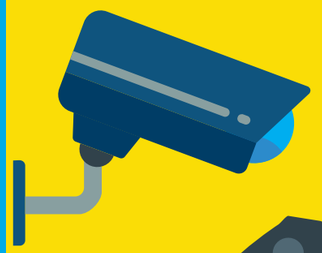
- Never rush into a relationship – get to know the person and ask questions
- Talk to your friends and family and be wary of anyone who wants to keep the relationship secret
- Never send money or share your bank details, no matter how long you've been speaking to them or the reason they give
- If you do decide to meet in person, make sure it's in a public place and let someone else know where you're going to be.

Sextortion

Fake blackmail sextortion scams are increasingly common. Typically, scammers send out thousands, or even millions, of identical emails claiming to have captured compromising videos, pictures or a person's internet search history.

The scammers threaten to publicise this information if they don't receive a "keep quiet" payment. The whole thing is a bluff, but the scammers bank on a few recipients being panicked into sending the requested money.

To make their false claim seem more plausible and increase their chances of success, scammers often include user passwords or phone numbers in their emails. They will have got hold of this personal information from previous data breaches where, perhaps unbeknown to you, you will have been compromised.



Don't be a loser

Online gaming can be great fun, but interacting with strangers comes with risks.

If you have responsibility for young people, it's important to have open and honest conversations with them about the potential dangers and risks surrounding playing online.

Equally, if you're a gamer yourself, you should bear in mind the following. Account hacking is becoming particularly prevalent with fraudsters gaining access to credit card and personal information. Gamers are also falling for phishing and spoofing attacks, where they get tricked into giving up their account and personal details when scammers pretend to be legitimate companies offering gaming currencies.

To avoid losing more than the game:

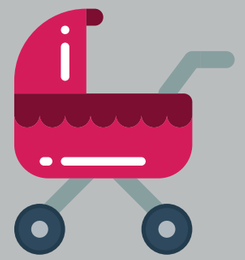
- Keep your machine clean with current computer security software and protect all devices with anti-virus
- Protect your online presence with strong account passwords and two-factor authentication as an extra layer of protection. Enable your privacy and security settings, limit how and with whom you share your information, and use an avatar (icon, image) rather than a photo
- Stay up-to-date, think before you act, and know how to block or report another user.

Close to home

If you are a carer, relative, friend or neighbour of an islander who might be vulnerable to scams, you might be the only person who can stop them falling victim. There are some common things to look out for such as lots of junk mail and calls from strangers, or perhaps the person becoming secretive about their finances.

You can help by reminding them not to give out their personal information, to speak to you before they reply to any offers or requests for payment, and to be suspicious about any claims they have won a prize. Also let them know not to be embarrassed to report a scam. It could prevent others from falling victim too. For more information visit **thinkjessica.com**

Don't be pushed



Last issue we warned islanders about authorised push payments. Paying in advance for fake goods and services is still a hot topic for our partner Jersey Trading Standards so once again we're reminding islanders about this scam. Basically, it's when fraudsters pose as genuine individuals or organisations and persuade victims to transfer money directly into criminal accounts. These payments are irreversible. In 2018 in the UK, close to 84,000 people lost a total of £354.3 million in these scams. To avoid being caught out when buying goods, make sure you do your research and be wary of any requests to pay by bank transfer. Contact your bank immediately if you think you've been caught out.

Block it

Do you get nuisance phone calls? You can register with the Telephone Preference Service which is a free national service for opting out of receiving unsolicited marketing and sales calls. It makes it illegal for companies to contact you if your number is on the central register. You can opt out by calling **0345 0700 707** or registering online at **tpsonline.org.uk**

While your local provider cannot block all nuisance calls, Airtel-Vodafone, JT and Sure advise you to let them know so they can try to minimise the impact.

Take a stand against scams

Do you want to join the fight against scams and frauds? Then why not become a Friend Against Scams? As part of a national initiative, the National Trading Standards is on a mission to recruit volunteers to tackle the lack of scams awareness by providing information and empowering people to take a stand against scams. Friends Against Scams encourages communities and organisations to take knowledge learnt about scams and turn it into preventive action.

There are now more than 21,000 Friends Against Scams signed up in the UK and Jersey Trading Standards is also a Friend. Why not become the first recruits for Jersey? By signing up, you will play a vital role in helping islanders spot, prevent and protect themselves from becoming victims of scams. Find out more and sign up here: **friendsagainstscams.org.uk**

Jersey's online fraud fears

According to Jersey's 2018 Opinion and Lifestyle Survey, 58% of islanders said they are worried about falling victim to a digital crime such as online fraud, cyber bullying or scams.

The results also show all ages of the population are increasingly concerned about digital crime, particularly the youngest demographic, rising from 29% in 2016 to 52% in 2018. Nearly three quarters of local residents feel the States of Jersey Police should be prioritising protecting islanders from digital crime.

Cryptic crime

If you find the words bitcoin, blockchain or virtual currency totally cryptic, don't worry - you're not alone. Cryptocurrency is the umbrella term given to digital currency of which Bitcoin has become the most talked about. It can be an alternative to money, credit cards and cheques. The 'crypto' element of cryptocurrency means the process is encrypted and designed to be confidential, anonymous and unbreakable between the buyer and seller.

Hot commodities in online trading, cryptocurrencies can be tricky to understand and aren't necessarily regulated by the Jersey Financial Services Commission. Fraudsters capitalise on people's limited knowledge and prey on their appetite to make money, promising unrealistic returns and no risk. Before you invest your money in crypto, or any asset for that matter:

- Take your time. Learn as much as you can about the investment. Don't be rushed into making a decision and be wary if you're being pressured
- Be vigilant and do your research. Always seek independent advice
- Don't assume it's the real deal. A professional-looking website doesn't mean it's genuine.

Look out for S.A.M

June is Scams Awareness Month (SAM)...keep your eyes peeled for helpful tips and advice on our Forum Facebook and Twitter pages for a chance to win some goodies!

Report it!

If you think you have been targeted by fraudsters or fallen victim to a scam, please report it to the States of Jersey Police on (01534) 612 612.

You can re-direct scam mail using the free postal service PO Box 500. Send any suspicious emails to scams500@police.je

Remember that if you are a victim of a scam, or an attempted scam, however minor, there may be other people in a similar position and your information could be vital.

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

Get Safe Online

Get Safe Online is the UK's leading awareness resource to help protect people, finances, devices and businesses from fraud, abuse and other issues encountered online.

Find out more:
www.getsafeonline.org

Let's talk

If you are a member of a group, club or organisation and you would like to learn more about frauds and scams, our Forum partners are available to present at seminars, talks and classes.

Get in touch with us to find out more by emailing FSCCommunications@jerseyfsc.org or calling (01534) 822008.

Members of the Jersey Fraud Prevention Forum

airtel vodafone · citizens advice · JERSEY CONSUMER COUNCIL · Jersey Bankers Association · Jersey CrimeStoppers. 0800 555111 100% anonymous. Always. Qi Finance Jersey Official Sponsor · 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.