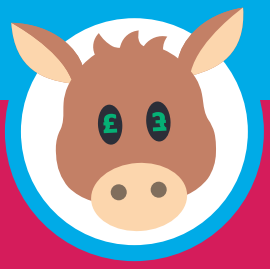
JERSEY FRAUD PREVENTION FORUM NEWSLETTER NOV 2019

Welcome to the latest edition of the Jersey Fraud Prevention Forum newsletter, a publication we hope continues to provide relevant information and useful hints and tips to help protect islanders from the ever-increasing risk of frauds and scams. All of our Forum partners continue to report a surge in both the volume and complexity of attempts to de-fraud our community and unfortunately the number of people reporting losses is also rising.

One of our biggest concerns currently is 'financial grooming', whereby trusting islanders are being deceived into handing over their life savings to people they have built a relationship with who are in fact fraudsters. In this issue we aim to raise awareness about this worrying trend so that residents are forewarned and will hopefully avoid falling victim to these criminals. We hope that you find our newsletter useful and that you have a 'safe' end to 2019.

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



Warning after catfishing hooks £350k

Islanders have lost hundreds of thousands of pounds in the first ten months of 2019, as reported cases of romance fraud and catfishing rise. Although the States of Jersey Police believe this figure is likely to be far higher with many incidents going unreported.

Catfishing and romance fraud see victims being lured into fake relationships by fraudsters using convincing profiles and deceptive stories.

Detective Chief Inspector Chris Beechey commented: "In most of the cases we're seeing, islanders are being targeted online via dating websites. Scammers seek out and exploit their vulnerability and loneliness, they secure their trust and then they steal their money with devastating financial and emotional consequences for the individuals concerned." The Forum is reminding islanders to always make sure they know who they're communicating with online and to never give out personal information or transfer money, unless they are absolutely sure who the person is.

If you have fallen victim to romance fraud or catfishing, report it to the States of Jersey Police on (01534) 612 612.

Is your child a 'money mule'?

In the last two years the number of under 21s allowing their bank accounts to be used for money laundering in the UK has nearly doubled, according to figures from Barclays.

Cash-strapped university students in particular are becoming lucrative new targets for fraudsters looking for 'money mules'. Lured in with offers of earning extra cash with 'no strings attached', most young people, often with financial worries, are 'groomed' online via social media to launder criminals' dirty money.

More and more Jersey students are heading to university in the UK so the Forum is warning about the risks of getting caught up in this criminal activity. Apart from having problems in the future with opening bank accounts and applying for credit cards and phone contracts, they could also be looking at a hefty prison sentence. To avoid falling victim, the Jersey Bankers Association is advising young people to:

- Never share bank account details or give access to accounts
- Be wary of unsolicited offers of earning easy money
- Speak to family, friends or a tutor if you're approached
- Remember it's potentially a crime to let someone else use your account
- If it's too good to be true, it probably is

For more advice visit getsafeonline.org & moneymules.co.uk

Christmas toys - naughty or nice?

Tech toys and gadgets may be high on many children's Christmas lists this year, but unfortunately they can present online security and privacy issues for families. Toys that connect to the internet can be fun and offer interactive play and education but many contain microphones, speakers, cameras, GPS tracking and sensors to capture and process data, which hackers can access.

Before you buy, here's some simple advice from Forum partner, the Jersey Office of the Information Commissioner:

- Do your research to see whether anyone has raised privacy and security concerns about the toy
- Check the manufacturer's privacy policy so you understand what information the toy collects, how it will be used and where it is stored. If it's on the toy itself, it's less of a concern than if it's on a Bluetooth-connected app or uploaded to the cloud
- Check how you set up, manage and enable parental control settings
- Talk to your children about playing safely, using strong passwords and not sharing personal photos and information
- Make sure you are comfortable buying a toy that sends emails to your child or connects to social media accounts

Hi, I'm calling from HMRC...

Our local telecommunications providers, Airtel, JT and Sure, are seeing a surge in the number of customers being targeted by fake callers pretending to be from HMRC, the Microsoft helpdesk and other reputable organisations. Unfortunately, many islanders are being caught out by either sharing their personal info or transferring money to fraudsters.

If you think you've received this type of call, you should contact your provider with details of the time of the call and the number. Your provider will then aim to trace the call and try to block it, if possible. Equally if you think you've fallen victim, you should contact the States of Jersey Police.

Juice jacking

Discovering that your phone is out of battery is a real inconvenience when you're out and about. Plugging into a public charging kiosk or wall outlet for a quick charge up may seem like a good idea but you could become the victim of a juice jacking attack.

Juice jacking is when hackers intercept charging points so they can inject malicious malware onto your device and steal your phone's data, photos, emails and messages. This is because both power and data can pass through the charge cable.

Juice up your phone safely by:

- Buying a small portable charger or power pack so you can charge up anytime, anywhere
- Avoiding USB charging at public spots and opting for an electrical outlet instead
- Investing in a "power only" cable to prevent data transmission
- Turning off your phone before plugging it into a mobile charging station - it's more difficult for hackers to access.

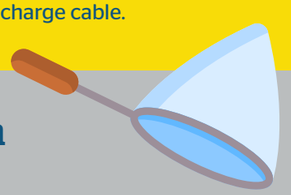
Protect your pension pot

Pension scams can be hard to spot and can be devastating for the victim. Scammers convince people to transfer their savings to a new scheme or release some of their money by making attractive but very fake offers. Usually scammers contact people out of the blue offering high returns and too good to be true deals.

If you're approached:

- Don't accept unexpected pension offers from cold callers. Do your research first
- Watch out for offers of high returns, complicated structures and unregulated investments
- Make sure you know who you're dealing with before you change your pension arrangements
- Don't be rushed or pressured into making a decision
- Talk to friends, family or an expert for impartial advice.

Caught in the net ...



Every issue we remind Islanders about the risks of phishing emails, as they continue to trawl local businesses and people. The Jersey Office of the Information Commissioner (JOIC) has seen a sharp rise in the number of cases being reported. The current email scam doing the rounds asks people for their email login details.

If you receive an email asking you to click a link or open an attachment to verify your login details stop and think. Check the email is legitimate by contacting the sender but only use the contact details you have and not those listed in the phishing email.

If you think your personal information has been lost, compromised or accessed, contact the JOIC on (01534) 716530 and report phishing attacks to scams500@police.je

A quiz you won't win...

Finding out which celebrity you look like or which food matches your personality in a quiz on social media may seem like harmless fun but it could cost you your identity.

Cyber criminals use these quizzes as 'clickbait' to trick us into giving up our personal data and then hack our online accounts. Seemingly random questions like "what was the name of your first pet?" usually prompt very similar responses to the ones we use to set up our online accounts. Once we give up this information we are exposed to attack.

Keep your data safe and avoid online quizzes that ask for personal information, no matter how innocent they seem.

Tackling bank transfer fraud

Banks are hoping to crack down on bank transfer fraud with a new alert system that's set to launch in March 2020. Essentially a bank account name-checking service, the Confirmation of Payee system will send an alert to anyone making a payment if the name of the payee does not match the bank account they are transferring the money to.

In 2018 alone, people lost more than £354 million to this type of fraud, by paying fraudsters for fake goods or services. If you think you've fallen victim you should contact your bank immediately and then the States of Jersey Police.

Wangiri - Don't answer back!

One ring and drop. That's the literal Japanese translation of Wangiri. This is when you get a missed call from an international or unusual number. If you ring back, you could end up on a premium rate call that could leave you seriously out of pocket.

Our three local providers, Airtel, JT and Sure, advise to only return calls from numbers you recognise or to look up the number online before you dial back.

Protect yourself from online scams

Don't make online payments while using Wi-Fi hotspots - they may be unsecure or fake. Use your data, a broadband dongle or a virtual private network instead.

Keep your virus protection software up-to-date on all your devices including your mobile. Don't ignore updates as they can protect against new types of scams, viruses and ransomware.

Keep your identity. Be wary when giving out personal info and never reveal your passwords. This info can be used to steal your identity and access your accounts.

Check your privacy settings on social media. Don't share information with people you don't know.

Be wary of unsolicited emails, calls and texts asking for information such as your password, login or other security details.

Make sure all your accounts have strong passwords. Don't use the same password for multiple accounts and change them regularly.

For more information visit Get Safe Online – the UK's leading awareness resource set up to help protect people, finances, devices and businesses getsafeonline.org

T'was the scam before Christmas

Black Friday, Cyber Monday, and Christmas shopping offers get bigger and better every year with retailers enticing customers with bargains, in store and online. But could you tell the difference between a genuine offer and a scam?

Keep these tips in mind before you buy:

- Avoid clicking on suspicious links on websites or emails that advertise discount codes and offers
- Shop only on trusted and secure websites and only use secure payment methods
- Don't be tempted by limited-time offers, high value freebies or offers that sounds too good to be true
- Set strong passwords for online accounts and avoid saving your card or bank account details when websites prompt you to

Report it!

If you think you have been targeted by fraudsters or fallen victim to a scam, report it to the States of Jersey Police on (01534) 612 612. You can re-direct scam postal mail to PO Box 500 and fraudulent emails to scams500@police.je.

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

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 Post · JT · Government of JERSEY · sure.