JERSEY FRAUD PREVENTION FORUM NEWSLETTER

NOVEMBER 2018

Reports of online fraud received by the States of Jersey Police have increased by 100% in the last 12 months. From January to October this year, Islanders lost £763,000. In the UK, criminals stole £500m in the first half of 2018.

Social engineering has been identified as the main cause for the losses. This is when fraudsters cleverly manipulate our natural human tendency to trust, grooming us into giving up personal and financial information.

Impersonation and deception scams are a common form of social engineering whereby fraudsters contact victims pretending to be from a genuine organisation such as the police, a bank, utility company or government department.

Remember - People are not always who they say they are. If you get a call, text, email or social media message asking you to disclose your personal or financial details or to transfer money, it could be a scam. **Stop and think.** Check the request is genuine by doing some research. If you're in any doubt, contact the organisation via a trusted communication channel to verify the approach. If you think you've fallen victim, contact your bank immediately and then the Police.

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

CONTACTLESS or POCKETLESS?

Millions of contactless card transactions are carried out every day. Some of them by fraudsters, unbeknown to the victims until it's too late. By not needing to use our PIN code, these cards offer us a fast and convenient way to pay. But criminals have the technology to read our cards and make payment transfers just by standing close to us.

Called **skimming**, the thieves carry radio-frequency identification (RFID) card readers in their pockets, which trick contactless cards into transferring the maximum amount into fraudsters' accounts without the victim realising.

While most contactless spends are limited to a maximum value of £30 and you are sometimes prompted to enter your PIN as a security measure, some retailers and indeed some countries have greater payment limits, making it even more attractive for thieves.

Thankfully this type of crime is still relatively rare in Jersey but Islanders need to be mindful particularly when traveling abroad. You can protect your cards by investing in an **RFID protective wallet**, which RFID readers cannot penetrate. "Islanders can give themselves another layer of security by adding their cards to their Smart phone and using Apple or Google Pay. This way their thumbprint or facial recognition is needed to process the transaction" - *Jonathan Bugbird, Jersey Bankers Association*

TIP - Always check the amount before you tap. A decimal point in the wrong place could be a very costly transaction. If your card is lost or stolen, make sure you report it to your bank or card issuer as soon as possible so it can be cancelled.

DON'T BE BLUE THIS BLACK FRIDAY

The biggest shopping day of the year falls earlier than normal this year - 23 November will ignite the usual shopping frenzy both online and in store and scammers will be getting in on the act.

As a consumer, you're most exposed online where fake websites and emails will be pushing 'too good to be true' offers for unrealistically priced electronic and designer goods.

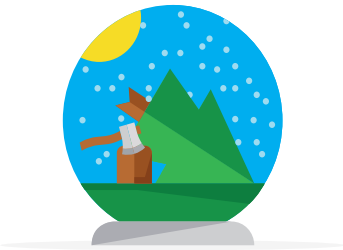
To avoid falling victim, stick to trusted, verified websites and avoid using public Wi-Fi to make your purchases. Keep an eye on your bank transactions and double-check any shopping apps before downloading them as they could be fake.

Remember – fraudsters will still be on the prowl on Cyber Monday on 26 November.

CONNED OUT OF CHRISTMAS

Christmas shopping gets most of us in a bit of spin – and fraudsters capitalise on it. It's prime time for them as we start making online (often panic) purchases. Here are a few tips to avoid getting conned this Christmas:

- **Never shop online from a device that isn't yours e.g. public computers**
- **Only shop using a safe and secure network - public Wi-Fi connections are notoriously unsecure and fraudsters may have hijacked the connection to track your activity**
- **Only use trusted, mainstream websites**
- **Avoid saving your card details to your online accounts**
- **Check your bank account on a regular basis to make sure you can account for all transactions**
- **Always use strong account passwords**
- **If you're making purchases over the phone, make sure you know who you're dealing with.**



HAVE YOU GOT ID?

According to figures from Cifas (a UK fraud prevention membership organisation), there has been a 24% rise in the number of under-21's falling victim to identity fraud. The majority of the fraud relates to plastic payment cards such as debit, credit or store cards.

There has also been a 26% increase in young people acting as 'money mules', basically allowing their bank accounts to be used for money laundering. The maximum prison sentence for this is 14 years. Report identity theft and money muling to the States of Jersey Police.

BE WEB SAFE

Not sure if a website is safe to visit? It's good to be cautious and it's absolutely vital to check that a website is secure before sharing any personal information (e.g. credit card numbers, passwords, addresses etc.) Here are some helpful tips:

- **Double-check links before you click on them – simply hover over the link to see where it will take you (the URL i.e. the address of the web page will appear in the bottom left corner of your browser)**
- **Make sure URLs are spelt correctly**
- **Check for HTTPS and not just HTTP at the beginning of the URL. The S stands for secure**
- **Use a website safety-check tool. These are available online**
- **If in doubt, call the company to verify its web address.**

FAKE TV NEWS

Watch out for fake emails claiming you're owed a refund on your TV licence. The emails link to convincing websites and try to get you to part with your bank account details. They state that you're due an overpayment refund but that crediting your account has not been possible due to invalid account details.

If you receive an email of this nature from any provider, check for suspicious and alarming subject lines and any spelling and grammar mistakes. Also make sure the sender's email address is correct for example *donotreply@tvlicensing.co.uk* - look closely as often the scam address can be very similar!

PUSHED INTO PURCHASING

In the first half of 2018, £145.4 million was lost in the UK in authorised push payment (APP) fraud.

This is when a criminal tricks their victim into transferring money directly from their account into the criminal's account. They do this by posing as genuine individuals or organisations and calling, emailing or texting victims.
If a customer authorises the payment themselves, under current legislation they have no legal protection to cover their losses. Two thirds of reported cases were 'purchase scams' – when a victim pays upfront for a product or service, such as a car or holiday rental, but they never receive it or it doesn't exist. Be wary of any offers or prices that look too good to be true and requests to pay by bank transfer.
Always use the secure payment method recommended by reputable online retailers and auction websites. Do your research and ask questions before you buy. Contact your bank immediately if you think you've fallen victim and then the States of Jersey Police.

BA WARE

The British Airways data breach in August/ September this year was yet another reminder that this type of cyber-attack is becoming commonplace with big global companies being the primary targets.

380,000 BA customers had their personal and financial details compromised. Following the attack fraudsters then targeted customers yet further by contacting them pretending to be BA staff to extract more information.

If you think your data may have been stolen in a cyber-attack, you can protect yourself by:

- **Being suspicious of unsolicited yet convincing requests for your personal or financial details**
- **Checking for suspicious activity on your bank accounts and notifying your bank / credit card company if you spot anything**
- **Resetting your passwords on other online accounts**
- **Reporting it - if you think you have been a victim of fraud or cybercrime, contact your bank and then the States of Jersey Police.**

GET SAFE ONLINE

Nearly all of the frauds and scams that we've covered in this issue are online.

With more of us going digital, we need to make sure we are cyber secure.

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

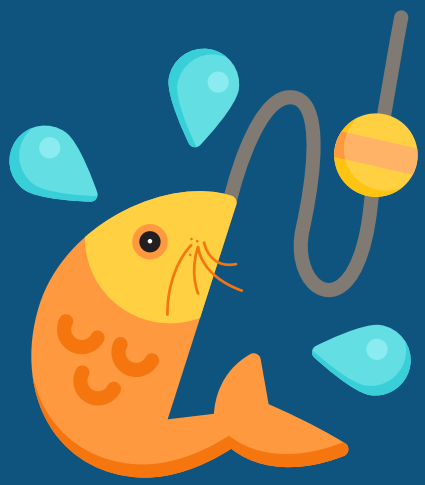
Access the Get Safe Online website for news and general advice: www.getsafeonline.org

CAUGHT BY A CATFISH

Catfishing is when scammers create false social media and online dating profiles to trick unsuspecting users into giving up their personal information and money. To avoid getting hooked, look for the following red flags:

- **Profiles with very few details / poor quality photos**
- **Early requests for personal information and mentions of financial difficulties**
- **A lack of other online profiles or discrepancies between profiles**
- **Avoiding meeting you in person**
- **Profile photos that aren't legitimate – you can check by reverse google searching the image.**

Just remember, always be sure you know who you are communicating with over social media and never give out your personal details until you are absolutely sure they are who they say they are.



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

Members of the Jersey Fraud Prevention Forum

airtel vodafone · citizens advice · Digital Jersey · Jersey Consumer Council · Jersey Bankers Association · Jersey CrimeStoppers. 0800 555 111 100% anonymous. Always. · Jersey Honorary Police · Jersey Financial Services Commission · Jersey Post · JT · States of Jersey · States of Jersey Police · sure.