JERSEY FRAUD PREVENTION FORUM NEWSLETTER

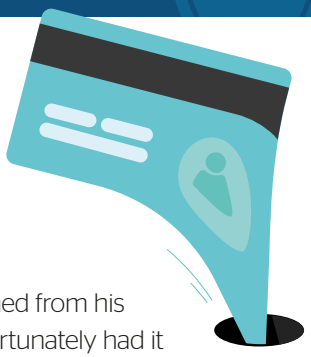
JANUARY 2018

Living in Jersey we can all too easily be overly trusting of our surroundings, in the misguided comfort that the Island is a safe place and that we are protected from falling victim to fraud and scams. But this may not be the case.

The Jersey Fraud Prevention Forum has been formed to raise awareness about the dangers, helping to educate and protect residents as well as offering them advice and support.

Chief Inspector Chris Beechey, Chairman of Jersey Fraud Prevention Forum

MORE THAN £217,000 STOLEN IN BANKING SCAM



In the run up to Christmas, a number of Channel Islanders were caught out by a banking scam after responding to fraudulent emails and texts purporting to be from NatWest and Lloyds.

In less than 24 hours fraudsters stole tens of thousands of pounds by sending messages claiming that there had been fraudulent activity on people's accounts and directing them to urgently call their bank's fraud prevention team on the number provided. Islanders who made the call were then tricked into disclosing their personal banking details.

One local professional had more than £8,000 siphoned from his account but fortunately had it returned by his bank. Recounting his own experience Ed Prow warns:

"The levels of sophistication of bank fraud is at an all time high, I would simply warn people to be extra vigilant."

The Jersey Fraud Prevention Forum is urging Islanders to never disclose passwords and other information regardless of how genuine the correspondence may seem. Anyone who receives a text or email of this nature should not respond but instead contact their bank and the States of Jersey Police.

TIGHTEN YOUR SAFETY NET

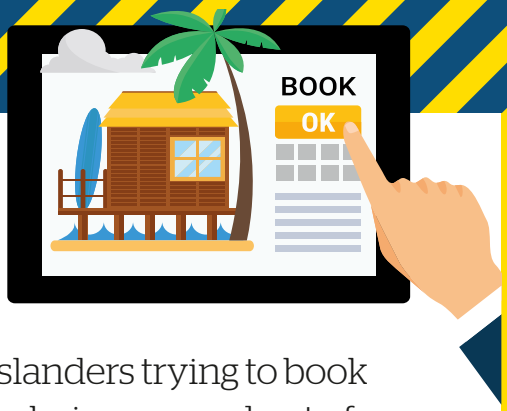
Being safe online is vital – and you expect to feel safe at home. But using Jersey-based websites and social media pages does not guarantee protection from cyber-crime.

Many Islanders get caught out on locally administered 'buy and sell' and auction pages, such as Jersey Insight, Jersey Stuff for Sale and Jersey eBay, because they assume the person they are dealing with is a legitimate buyer/seller here in the Island. But fraudsters, based both locally and remotely, operate on these pages by setting up fake profiles and products to target unsuspecting Islanders.

Some simple steps to avoid being scammed:

- **Don't take payment by cheque**
- **Use a secure payment method such as PayPal**
- **Only exchange money/goods if you're sure it's genuine**
- **Do your research and make sure you have all the details before you commit. Read reviews but be mindful that they may not be legitimate.**

HOLIDAY HOAX!



A growing number of Islanders trying to book their perfect holiday are being conned out of thousands of pounds in elaborate villa frauds. In one recent case an Islander lost more than £15,000 after being duped by a scam website and in the UK last year alone there were nearly 6,000 reported cases of this type of holiday fraud.

It's easy for fraudsters to post fake properties on reputable websites or set up scam sites of their own, tricking customers into paying big deposits or even the full amount for a bogus booking.

While on the whole it is far safer to use well-known websites such as Booking.com, unfortunately it does not always guarantee that a property is the real deal. But by being cautious and always following simple procedures, it does minimise fraudulent transactions. For example, you should only ever correspond with the property owner through secure websites rather than their personal email.

Some other simple tips for protecting yourself from holiday villa fraud include using secure payment methods such as PayPal, checking the property exists on Google maps, and reading all customer reviews to ensure they are legitimate.

If you use a reputable website and still lose money, contact the company directly and they may cover any losses. Using a credit card will give you protection as your credit card company is jointly and severally liable for any breach of contract or misrepresentation by the retailer/trader.

TAKE FIVE

If you receive a request to provide personal or financial information, you need to take a moment to reflect and step back from the situation. Even if they say they're the bank or another trusted organisation, you need to take the time to stop and think.

- **Don't give out personal or financial details**
- **Never automatically click on a link in an unexpected email or text**
- **Always question uninvited approaches – don't assume they are authentic**
- **If prompted, do not move money from your account. Verify with your bank**
- **Don't be rushed or pressured into making a decision – stay in control**

For more information from the UK's Take Five campaign visit www.takefive-stopfraud.org.uk

DON'T FALL FOR THE BAIT!

In just one day in the UK, 22,000 people replied to a scam email and sent their money to scammers.

Not to be confused with the sporting activity, this is phishing - an attempt to obtain your money and/or sensitive personal information such as **credit card details**, **PIN**, **usernames** and **passwords**. The fraudsters pose as trustworthy individuals or companies known to their victims and try to catch them out by sending emails and texts with fraudulent financial instructions as bait.

Several companies in Jersey have recently been caught out – one lost more than £700,000. But anyone can be targeted and it is becoming an increasingly common cyber-crime, although it can often be spotted by irregularities in the sender's email address and fake web links.

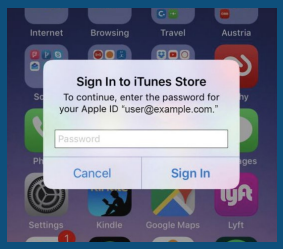
Always be mindful that there is certain personal information that legitimate contacts would never ask you for and if you are ever unsure you should contact the company or individual directly.

AN APPLE SCAM A DAY...

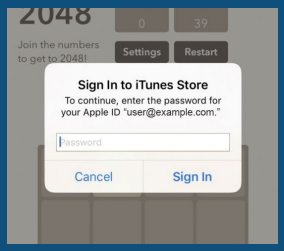
One scam currently in circulation involves fake pop-up password prompts on Apple devices. These look exactly the same as the official Apple password pop-up but the fake forwards you to a bogus login designed to steal your details and gain access to your account.

As Apple regularly asks users to supply ID and password, it is easy to become desensitised and fall for the fake. Luckily, it's relatively easy to check whether the prompt is real or not. Before entering any details, simply access your home button and, if the prompt is real, it will stay on your screen until you "Sign in" or "Cancel". If it is fake, it will close.

You can also enable two-factor authentication for your Apple ID device, which adds a layer of security to your account, making it harder for fraudsters to gain access if they do get your password.



Random system pop-up - real



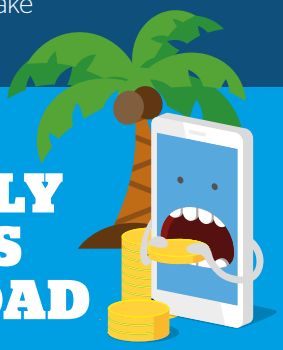
Phishing pop-up in app - fake

DON'T RETURN TO SENDER!

Every day we get unsolicited mail through our letterboxes and often it can be difficult to determine which is bona fide and which is scam. Forum partner Jersey Post is asking Islanders to be more vigilant following a rise in some of the more common postal scams.

Romance frauds are a big problem with victims falling for fake stories and being groomed into sending sums of money to fictitious overseas lovers. Equally Islanders are frequently corresponding with phoney 'relatives in need' to pay their urgent bills, purchasing property that they believe to be genuine, and sending money to bogus charities.

If you know someone who is regularly responding to this type of scam mail, please contact the States of Jersey Police and redirect the correspondence to PO Box 500 for investigation. **PO Box 500 is a free postal service.**



COSTLY CALLS ABROAD

If your phone is stolen while you're away on holiday, you need to contact your local telecommunications provider immediately.

Many people think disabling the device is sufficient but this does not stop fraudsters from using your SIM card in another phone and racking up huge bills at your expense. Forum partners Airtel Vodafone, JT and Sure are reminding Islanders to inform them about phone theft abroad so they can disable the service as well as the device, preventing any extra unwelcome roaming charges.

Helpful numbers:

Airtel Vodafone - 07829 700121

JT - 01534 882 882

Sure - 0808 1015 247

WI-FI ACCESS TO EVERYTHING...

Most people use public Wi-Fi without even thinking; logging on in hotels, shops, airports, shopping centres and other public areas which generally offer it free of charge. But cybercriminals do monitor Wi-Fi networks and can intercept your personal data, stealing banking details, account passwords and other valuable information. They even set up bogus wireless connections to trick users into thinking they are using a legitimate link.

To avoid problems, never connect to an unknown or unrecognised network, always verify the connection is secure by asking a member of staff at the venue and, if you are working, ensure you access your corporate network with a secure, encrypted Virtual Private Network (VPN).

When using public WiFi, avoid browsing websites which require your personal details and passwords such as online banking, social networking pages and sites that store your credit card information.

Smartphones, tablets and laptops are all equally vulnerable so make sure you protect yourself by installing up-to-date anti-malware software and security solutions.

For more information and more general advice about being safe online visit: www.getsafeonline.org

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 · citizens advice · DIGITAL JERSEY · Jersey Bankers Association · JERSEY CONSUMER COUNCIL · Jersey Financial Services Commission · Jersey Post · JT · States of Jersey · States of Jersey Police · sure.