



JERSEY FRAUD PREVENTION FORUM

NEWSLETTER

APRIL 2020

Message from the Chair

The coronavirus outbreak has impacted so many aspects of our lives. It's changed how we live, work and socialise; pushing many of us to communicate with our colleagues and loved ones in new and interesting ways.

The situation has also become a playground for scammers. In March, we noticed a spike in Covid-19 related scams. Some Islanders even received text messages from scammers claiming that the UK Government was offering hundreds of pounds to all residents to help fight the virus. Since February, more than 640 victims have lost almost £2 million in scams reported to Action Fraud.

Fraudsters are cashing in on uncertainty and duping people to trust them with their health, so we all need to be calm and extra vigilant at this time. While we social distance from friends, family and colleagues, be sure to keep scammers even further away.

Stay safe. Stay home.

Detective Chief Inspector Chris Beechey
Chairman of Jersey Fraud Prevention Forum

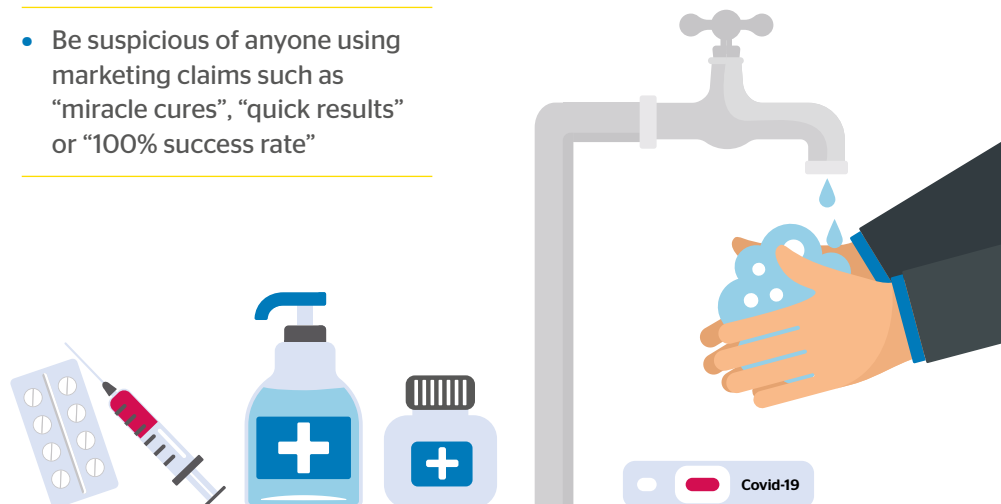


Don't put your health in their hands

While medical professionals work rapidly to develop treatments and produce more medical supplies to fight coronavirus, criminals have been selling fake testing kits, counterfeit hand sanitisers and even bogus vaccines to profit from the pandemic. Fraudsters are exploiting the current situation and conning members of the public online, over the phone and door-to-door.

You should:

- Get advice from a registered healthcare professional such as your GP or local pharmacist
- Only buy medicines and medical devices from authorised retailers or pharmacies
- Be suspicious of anyone using marketing claims such as "miracle cures", "quick results" or "100% success rate"
- If you have bought any imitation kits or unapproved medicines, you shouldn't use them and instead immediately contact Action Fraud actionfraud.co.uk



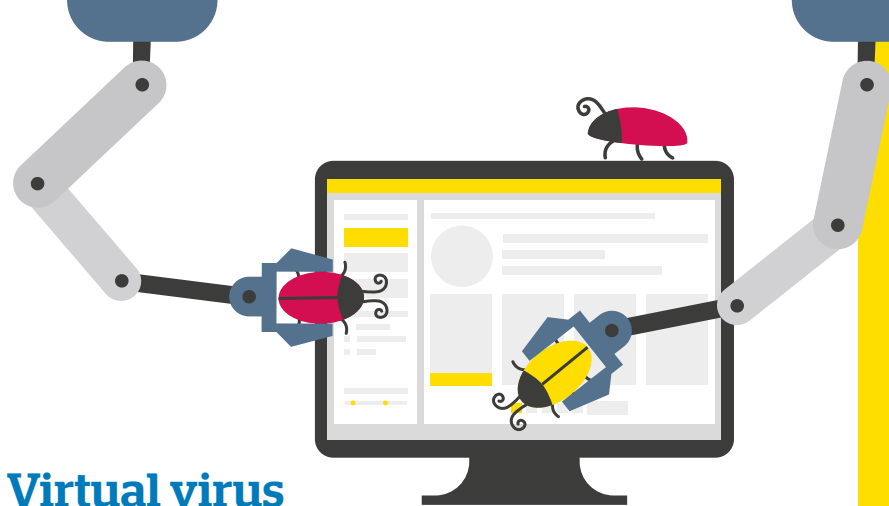
Hi, you're entitled to a refund...

Before you sigh with relief at the thought of being offered a refund on your cancelled holiday, be cautious, it could be a scam.

Fraudsters are operating as bogus insurance firms and tricking people into giving them their bank account details and personal information. Be suspicious of any cold calls.

To find out if you are entitled to a refund, you should contact the airline, booking website, travel agent, or your bank or credit card provider directly through official channels.





Virtual virus

Whether it's real or virtual, we all need to be vigilant about viruses and try to prevent them from spreading. With so many of us using smart devices, there's an increased risk of scammers infecting our computers and phones with viruses that could destroy hardware and steal our personal information, pictures and passwords.

Use these top tips to keep your devices healthy:

- Avoid saving passwords or credit card information to online accounts, especially if you are using a shared device
- Ensure your computer is up-to-date with the latest anti-virus software
- Make sure you complete any software updates so your device isn't vulnerable to malware
- Don't download any files or documents unless you're absolutely sure of the source. If your anti-virus software warns you about the security of files, delete them. Don't forget to empty your recycle bin too
- Don't click on any pop-ups offering free health checks, Covid-19 test kits, etc. These could be filled with viruses or inappropriate images.

Watch out for fraudsters:

- Pretending to be the tax office or Government, offering rebates
- Imitating insurance firms offering refunds on cancelled trips
- Requesting donations to help fight the virus
- Advertising quick, hassle-free loans.



Are you a scam-smart superhero?

Are you smart enough to fight off the fraudsters? Master the maze to find out. See back of the newsletter.



Working remotely, working wisely

With so many Islanders working remotely or home schooling, you need to be sure your working environment is safe and secure. We are currently a captive audience for fraudsters, who will prey on our vulnerabilities, whether online or over the phone.

Be cautious if you are contacted out of the blue. In particular, treat offers of Government aid, bank-related support and approaches for donations with extreme caution.

The Government of Jersey has shared the following advice to protect you and your family:

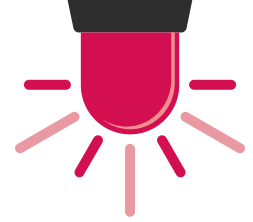
- Beware of anyone offering deals to make it easier for you to work from home
- Make sure your Wi-Fi network is private and password protected and your devices are up-to-date with anti-virus installed
- Consider using a Virtual Private Network (VPN) to make it harder to track your information as it travels the internet
- Add extra layers of security to logins such as multi-factor authentication
- Make sure other members of your household don't have access to sensitive information about customers, staff or your business
- If you're sharing a device, set up a separate user profile or account for work purposes.



Tips from telecoms

Forum partners, Airtel, JT and Sure have reported a significant increase in the number of Islanders reporting scam calls. They're reminding everyone to stay safe from scammers:

- Be sceptical of anyone claiming to be your bank, the police or even your service providers such as internet or telecoms. Being asked to share your personal information, transfer money into another account or settle a debt you're not aware of should all be warning signs
- Scammers will try to keep you on the phone for as long as possible. Don't be afraid to say no and put the phone down if you're unsure
- If you are experiencing scam calls or texts, write down the caller's number and time of the call and report it to your service provider. This could help them to identify patterns and potentially block nuisance calls in the future.



Safeguard your finances and your future

Forum partner, the Jersey Financial Services Commission, is warning Islanders to be extra vigilant about their investments and retirement arrangements. The regulator is concerned people may be more at risk of falling victim to investment scams or making hasty financial decisions by investing in high risk products or transferring out of their defined benefit pensions. By using regulated financial advisers and getting professional, credible advice, Islanders can better protect their finances. Visit jerseyfsc.org for more information.

Keep your information close, your data even closer

If you are worried about how your personal data may be used during the pandemic, keep these tips from the Jersey Office of the Information Commissioner in mind:

- Government of Jersey can share vital public health messages via phone, email or text. **You do not need to give them your consent**
- You might be asked to give details to your employer or organisations about sensitive health conditions and recent travel. **They shouldn't be asking for more information than is necessary**
- If you become ill with coronavirus, your employer might need to tell your colleagues. **They can do this without sharing your name**
- If a volunteer is helping you, **make sure you know how your personal information will be used, who has access to it and where it will be stored.**

For more advice and information, visit jerseyoic.org



Self-isolating shoppers

Just because we're at home, doesn't mean we can't enjoy doing what we love the most! Scammers are taking advantage of the increasing time we are spending browsing, chatting and shopping on social media sites and it is now much easier for them to scam unsuspecting users.

Watch out for fraudsters posting products using fake accounts, attractive images, videos and rave reviews. They could in fact be selling counterfeit, defective or even non-existent items. Only shop from reputable and official websites and use secure methods of payments.



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



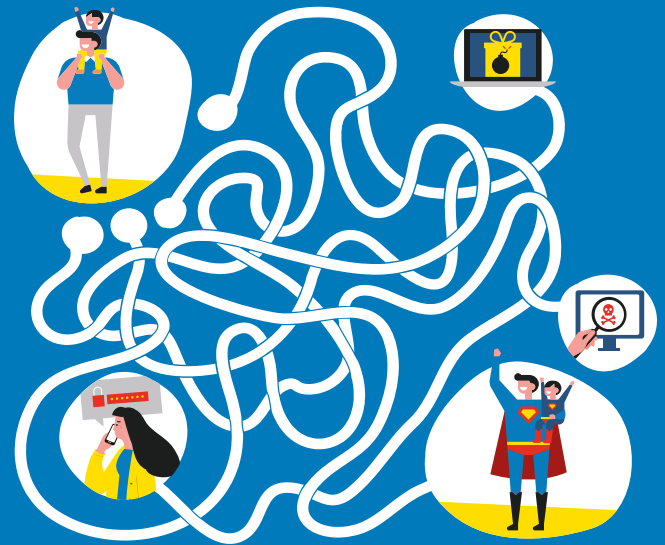
Word search

Scam	Download	Malware
Passphrase	Moneymule	WiFi
Antivirus	Security	Safe
Firewall	Cyber	Did you find the bonus word?

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

Maze

Fraudsters are on the hunt to find their next victim. As a scam-smart superhero your job is really important to keep yourself, your family and friends safe from people trying to steal money and personal information. Can you beat them?



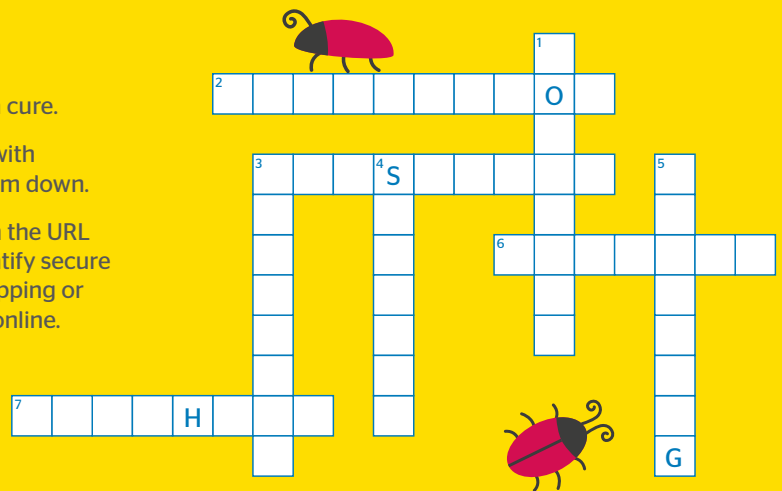
Crossword

Down:

1. Beware of fraudsters trying to sell you bogus products over the telephone.
3. Fraudsters disguise themselves as other people to trick you into giving them money. Don't get hooked!
4. Another word for fraudster.
5. Fraudsters mimic official telephone numbers to deceive you.

Across:

2. This is better than a cure.
3. Never share these with anyone or write them down.
6. Look for this icon in the URL toolbar to help identify secure websites when shopping or making payments online.
7. When fraudsters send you a text message to trick you into following a malicious weblink.



To find out if you answered the puzzles correctly, visit our website fraudprevention.je

Members of the Jersey Fraud Prevention Forum



To the best of our knowledge, the information contained in this newsletter is accurate and reliable as of the date of publication. However, we do not assume any liability for the accuracy and completeness of the above information.