Jersey Financial Services Commission

18 August 2017

JFSC warning following £450k targeted cyber fraud attempt on regulated business

The Jersey Financial Services Commission (**JFSC**) has today issued a warning to local businesses following a series of targeted attempts to defraud Jersey companies and their clients.

We are aware of at least three cases where locally registered companies have been the subject of an attempted 'impersonation attack' whereby fraudsters have registered a domain name that is almost identical to the organisation's domain and then sent bogus emails to the firm's customers requesting large sums of money. The fraudulent emails also include legitimate signatures to make them appear more authentic.

In one of the cases reported to our Supervision division, fraudsters tried to extort more than £450,000 in an attempt to impersonate a local company, but fortunately this was detected.

JFSC Director General John Harris commented:

"We are asking local companies and Islanders to be extra vigilant. We are aware that this is not an isolated incident and that cybercriminals have purchased several domain names that are similar to local companies' domain names with the intention of conducting fraudulent activities. Verifying the authenticity of any unexpected emails requesting funds is key to avoid falling victim to this type of cyber-crime."

JFSC Cyber Security Senior Manager Davey Sandiford added:

"This type of attack relies on social-engineering to deceive its targets. In this case the domain name used by the criminals appeared to be the same as the local company's but had an extra letter which could easily have been overlooked by the recipient on first glance. If you receive an email from a domain that appears to be slightly different to the norm then check the request immediately with the organisation it's claiming to come from, making sure that you use official contact details rather than those in the email."

If you fall victim to cyber fraud or you identify an attempt on your organisation, you should immediately report this to the States of Jersey Police. Please email scams500@police.je with full details of the fraud. This should be in addition to contacting your JFSC supervisor.

If you are aware that there has been a breach in personal data you should also contact the Information Commissioner.

It is advisable to also:

- Consult a professional on Cyber-security to assess whether your systems have been compromised

T +44 (0)1534 822000
E info@jerseyfsc.org
PO Box 267 14-18 Castle Street
St Helier Jersey JE4 8TP
jerseyfsc.org

- Provide the JFSC with a clear chronology of facts and keep your supervisor updated regularly
- Reaffirm your internal plan to mitigate risks (e.g. additional checks before customer doing transfers)
- Consider notifying your insurance provider, if applicable

We recommend the use of good cyber-security practices to help protect yourself against such attacks including, but not restricted to:

- Using complex passwords/passphrases
- Do not re-use passwords for multiple services and applications
- Use multi-factor authentication where appropriate
- Make sure that systems are patched and up to date
- Ensure anti-virus is installed and up to date
- Deny by default principle used on Firewalls
- Carry out awareness training for employees
- Do not reply to emails that request personal or account information
- If you receive an email that looks suspicious or asks you for this type of information, never click links that supposedly take you to a company website
- If the email appears to come from a company, contact the company's customer service via phone or web browser to see if the email is legitimate – do not use the contact details in the email you have received
- Search the internet for email subject lines, followed by the word hoax to see if anyone had reported this scam.

Kind regards,
John Harris
Director General