Office of Cyber-Security
& Information Assurance
Oik son Shickyrys Lectraneagh as Saoçhys Fysseree

Advisory Notice

Issue Date 13th January, 2020

TLP: WHITE

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE

WHITE **Public** - May be distributed freely, without restriction.

Scam Alert - Emails, phone calls and text messages

Criminals are using emails, phone calls and text messages to target the Isle of Man during lockdown.

Criminals want to convince you to do something which they can use to their advantage.

In a scam email or text message, their goal is often to convince you to click a link. Once clicked, you may be sent to a dodgy website which could download viruses onto your computer, or steal your passwords and personal information.

Over the phone, the approach may be more direct, asking you for sensitive information, such as banking details.

They do this by pretending to be someone you trust, or from some organisation you trust. This could appear to be from a company you use like Amazon, a bank, or even a friend in need. And they may contact you by phone call, email or text message. The term 'phishing' is often used when talking about emails.

Scams during the COVID-19 pandemic

While everyone is worried about the coronavirus, cyber criminals have seen this as an opportunity. In emails and on the phone, they may claim to have a 'cure' for the virus, offer financial rewards, or encourage you to donate to worthy causes. Like many scams, these criminals are preying on real-world concerns to try and trick you into interacting.

We have had Manx numbers being replicated and scammers pretending to be Manx workers working from their homes.

These scam communications can be very hard to spot. They are designed to get you to react without thinking.

If you think you've already responded to a scam, don't panic. Whether you were contacted by phone, email, or text message, there are things you can do to limit any harm.

Reporting suspicious messages

The message might be from a company you don't normally receive communications from, or someone you do not know. You may just have a hunch. If you are suspicious, you should report it. By doing so you'll be helping to protect many more people from being affected.

Email -
If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at sers@ocsia.im

SMS text message -
Suspicious text messages can reported to the online reporting point at https://www.gov.im/about-the-government/office-of-cyber-security-and-information-assurance-forms/cyber-concerns-online-reporting-form/ and, if able, then send a screen shot by email to warp@gov.im quoting the reference number provided when initially reported.

What to do if you've already responded

If you've already responded to a suspicious message, take the following steps:

- If you've been tricked into providing your banking details, contact your bank and let them know.

- If you think your account has already been hacked (you may have received messages sent from your account that you don't recognise, or you may have been locked out of your account), there is information here:- https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

- If you received the message on a work laptop or phone, contact your IT department and let them know.

- If you opened a link on your computer, or followed instructions to install software, open your antivirus (AV) software and run a full scan. Allow your antivirus software to clean up any problems it finds. Uninstall any applications you may have installed on your device, and if in doubt about how to do any of this, contact an IT specialist to assist with securing the device.

- If you've given out your password, you should change the passwords on any of your accounts which use the same password.

- If you've lost money, tell your bank and report it as a crime via the OCSIA reporting link:- Isle of Man Government - Cyber Concerns Online Reporting Form. By doing this, you'll be helping the battle against criminal activity, and in the process prevent others becoming victims of cyber crime.

Spotting suspicious messages

Spotting scam messages and phone calls is becoming increasingly difficult. Many scams will even fool the experts. However, there are some tricks that criminals will use to try and get you to respond without thinking. Things to look out for are:

- **Authority** - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.

- **Urgency** - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.

- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

- **Scarcity** - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

- **Current events** - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

If you think it could be genuine

If you think a message or call might really be from an organisation you have an existing relationship with, like your bank, and you want to be sure:

- Go back to something you can trust. Visit the official website, log in to your account, or phone their advertised phone number. Don't use the links or contact details in the message you have been sent or given over the phone.

- Check to see if the official source has already told you what they will never ask you. For example, your bank may have told you that they will never ask for your password.

Make yourself a harder target

Criminals can use publicly available information about you to make their phishing messages more convincing. This could be gleaned from your social media accounts.

To make life harder for the criminals, you can do the following**:**

- For your social media applications and other online accounts, review your privacy settings.

- Think about what you post (and who can see it).

- Change your phone number to be unlisted, or 'ex-directory'.

We have detailed advice on protecting your privacy on social media. More information can be found on our OCSIA Knowledge Base, here: www.gov.im/ocsia

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security & Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.