Office of Cyber-Security & Information Assurance

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

Advisory Notice

Issue Date 8th December, 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.

Common Vishing Scams

Overview

The Office of Cyber-Security & Information Assurance (OCSIA) receives a considerable number of reports each week from Island residents concerning cold calls claiming to be from organisations that know the receiver of the call.

In almost every case, these cold calls are scams run by fraudsters attempting to steal money and personal data from unsuspecting victims. We call this kind of scam 'vishing' which is a portmanteau of 'voice' and 'phishing'.

These vishing calls can often be quite distressing for those who do not know that they are being scammed and create a sense of urgency by threatening the call recipients with legal action, cutting off services or financial loss.

To find out more about phishing, vishing and other cyber security threats, visit our OCSIA Knowledge Base: https://www.gov.im/ocsia-knowledge-base.

Detail

Here are some of the most common vishing scams we have been made aware of:

- **Amazon (Prime)** - Amazon is a popular online marketplace and service provider. The company is being impersonated by fraudsters to persuade call recipients into providing payment for subscription services or request remote access to their computer to resolve the issue. This can result in large sums of money being transferred to the scammers.

- **(UK HM Revenue & Customs) Tax Division** - This scam can be very distressing for call recipients. As with many of the other scams in this document, the call is initiated with an automated voice but this one will threaten the call recipient with legal action unless a tax issue is resolved.

Office of Cyber-Security & Information Assurance (OCSIA)
OCSIA@gov.im (01624) 685 557

- **Bank Suspicious Activity** - This scam involves the operator on the other end of the line warning the call recipient that suspicious activity has been identified on their bank account and that funds must be moved to a "safe" account whilst an investigation is carried out. The scammer will tell the recipient to keep the transfer of funds a secret and to use a believable reason for the transfer if asked by any bank staff (such as paying medical bills to a friend) because the staff in the bank are being investigated – this is not the case and is just a ploy to try and convince the banking staff not to block the transfer.

- **BT (Open Reach)** - This scam usually begins with the fraudster advising the call recipient that there is an unpaid bill and that their telephone connection will be cut off unless a payment is made. This is an easier scam to detect on the Island because BT is not a service provider over here but it is still quite a common scam and people can still be caught out when put under pressure.

- **(Microsoft) Technical Support** - This scam typically involves the scammer warning the recipient that they have identified errors or malicious activity on their computer system or device. They may direct the recipient to programs and utilities that look like the system has multiple errors that need fixing. The next step usually involves asking the recipient to install a remote access tool which will give the scammer full access to the computer. The scammer will proceed to "fix" the issue and demand payment for resolving the problem. They may also install malicious software that maintains their presence on the system until a payment is made.

Organisations will never cold call and ask to install software or remotely access your computer. Be extremely wary of any unexpected calls claiming to be from organisations even if they know your name or other personal information and follow the recommendations below.

Recommended Action

- If ever in doubt about a call, hang up and contact the genuine business using known contact details from an official source. Don't be coerced by the person on the other side end into providing personal information or bank details.
- If you believe money has been transferred to a scammer, contact your bank as soon as possible.
- If the scammers have accessed your computer or device, turn it off and arrange for it to be restored by a competent IT specialist.
- Remain vigilant and share this advice with your friends, family and colleagues.

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.

TLP: WHITE