Divert/Deter SOC Alert - 18th October 2018

Through liaison with the Police Scotland Economic Crime Unit it is reported that there has been a noticeable increase in vishing frauds against the elderly. Below is a list of recent vishing fraud MO's in Scotland.

> **Vishing:** The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details or credit card numbers.
>
> *Oxford Dictionaries*

1. The victim is contacted by landline or mobile knowing basic details about who they are and who they bank with. The fraudster uses spoofing so the caller phone number matches numbers used by the banks. The fraudster introduces themselves as an employee of the bank and claim there has been suspicious expenditure on their accounts. They convince the victim that they must move their money to 'safe accounts' set up for them. The victim thereafter logs into their online banking and transfers all their money into their own current account. From there they are provided with a list of mule accounts and instructed to send the funds to these accounts. Fraudster states the victim will receive new bank cards in the post.

2. Contact with victim as above. Fraudster then states that bank staff in the victim's local branch are responsible for intercepting people's money and stealing it. To catch them the fraudster requires the victim to attend the local branch and make transfers to 'safe accounts'. By doing so they claim they will see the flow of the funds and be able to identify which staff member is responsible. The victim is schooled in how to answer any questions if challenged by bank staff. The following have been used recently:

- They are sorting out their financial affairs
- The money is for their Grandchildren
- The money is for building contractors

It is reinforced that they must not trust anyone in the branch. Fraudsters also warn victims that it is a criminal offence to tell anyone about the contents of the phone calls.

The victim is also told to describe what they are wearing as the fraudster will be monitoring live CCTV footage of within the branch. On occasions they have been told to keep an open line on their mobile phone so the fraudster can monitor what is being said.

Victims have also been told they will receive a four figure sum for assisting with this investigation. On several occasions they have then followed up with calls pretending to be

Police Officers. They have used the genuine name of a financial investigator within the police (who has previously made various media releases available on open source).

The successful levels of social engineering can be demonstrated in the following two very recent examples:

- A recent vishing fraud resulted in an elderly female attending at a local Bank of Scotland branch on three occasions in one afternoon. On each occasion the fraudster even insisted she took taxis and not the bus. In total £36,000 was transferred (4 lots of £9000) over the three visits. The victim was only challenged once but provided the answer that the money was for her Grandchildren. The victim thereafter believed a fictitious Police Officer would be attending to take a statement causing a delay in any reporting.

- An elderly male was victim of social engineering over a three week period from fraudsters purporting to be from RBS and the FCA. This resulted in him cashing out his investments into his RBS accounts. Thereafter he was instructed to attend another RBS branch which wasn't his local branch. The male was specifically told to go to this other branch with the reason being that RBS staff in his local branch rotate the branches they work in. The male made an international transfer to Dubai of £600,500. He was schooled to lie to RBS staff if he had been challenged.

3. The victim receives a text message on their smart phone claiming to be from PayPal stating their account has been compromised and they have 36 hours to login and fix this. There is a fraudulent internet link on the text message. Victim clicks this link and is taken to a fake PayPal page where they ultimately unwittingly provide the fraudsters with their PayPal details.

The victim is later called using spoofing technology. The fraudster claims to be from a Fraud Team of their bank and question fictitious spending at Argos (or similar). The fraudster thereafter states the victim's account has been compromised via PayPal and they must move their money to a safe account. The victim thereafter is talked through how to do this via online banking. At this stage, the fraudster may have gained remote viewing access to the victim's computer via spyware. The fraudster may go through direct debits and recent expenditure on the victim's account. The victims bank account names on their online banking app had also been changed to 'locked' or 'closed', further suggesting remote access.

Further advice to protect yourself from cyber scams can be found at "The Little Book of Cyber Scams" http://www.scotland.police.uk/assets/pdf/174967/the-little-book-of-cyber-scams?view=Standard