The Oasis Centre - Cornwall

Registered Charity Number 1139355, founded to serve the communities in the parishes of St Columb Major, St Mawgan-in-Pydar, St Eval and St Ervan

Looking Out for …… Telephone Numbers

Number 34 in a series of notes on important issues.

If asked, many people would probably say that their most useful piece of modern technology is their mobile phone. Calls, texts, Internet searches, music and photos are all available at the click of a button. They can be used for networking, entertainment, shopping and of course banking. That is where criminals start to become very interested. If they can take over somebody's mobile, it might provide a wealth of opportunities.

Welcome to the world of "port-out" fraud and SIM swapping! Let's start with the latter. The SIM card is the magic bit inside a mobile. SIM stands for 'Subscriber Identity Module'. The card is small, it can be removed and replaced relatively easily. It contains its own unique serial number and identity and it holds all the really useful things needed on a mobile such as passwords, messages and phone book contacts. The telephone number for that mobile is among them.

If a fraudster is able to impersonate the owner of a mobile, they may be able to persuade that person's network provider to supply a new SIM card. If they do, that gives them access to the telephone number and they can intercept text messages and use services linked to that number. Those services can include the ability to request a banking password reset or provide access to two-factor authentication services.

The variant on this fraud involves the use of "number porting". This is a genuine service provided by telecommunication companies. It allows a customer to keep their existing phone number and transfer it to a new SIM card, perhaps one in a new, modern mobile linked to another network. The existing network provider will send its customer what is known as a "Port Authorisation Code" or "PAC". When that code is presented to the new provider, the phone number can be transferred to the new SIM card.

Action Fraud say that victims have reported large losses as a result of this fraud. One of them initially ignored text messages received from their network provider containing a PAC number. Two days later £6,000 was removed from their bank account. The network provider reported that someone had contacted them purporting to be the victim, cancelled their contract and transferred their number to a new SIM.

Any unsolicited notification about a PAC Code request means that you should contact your network provider immediately to terminate the request. You should also notify your bank about your phone number being compromised if you are using it for your banking. Do this quickly! It is also worth remembering that criminals can mimic the phone numbers and e-mail addresses of companies you know and trust, such as your bank.

Jeremy Simmonds, Chair, The Oasis Centre - Cornwall