“Port-Out” Fraud Targeting TSB Customers

CITY OF LONDON POLICE
National Policing Lead For Fraud

Protect Alert

Published on 24/05/2018
Reference 18050002

There has been an increase in reports made in May by TSB customers relating to “port-out” fraud. Fraudsters are number porting a victim’s telephone number to a SIM card under their control and then using the number to access the victim’s bank accounts.

The increase in the number of reports corresponds with the timing of TSB’s computer system update, which resulted in 1.9 million users being locked out of their accounts. Opportunistic fraudsters are using TSB’s system issue to target individuals, which follows the increase in phishing and smishing communications also targeting TSB customers this month. Victims’ bank account and personal details including their phone number are collected by the fraudster, providing them with the information to execute the fraud.

Number porting is a genuine service provided by telecommunication companies. It allows customers to keep their existing phone number and transfer it to a new SIM card. The existing network provider sends the customer a Port Authorisation Code (PAC), that when presented to the new provider allows the number to be transferred across. This service can, however, be abused by fraudsters.

To gain control of the victim’s phone number, fraudsters convince the victim’s mobile phone network provider to swap their number on to a SIM card in the fraudster’s control. Once the fraudster has control of the number they are able to intercept the victims’ text messages, allowing them to use services linked to the victim’s phone number. This can include requesting an online banking password reset or access to any two factor authentication services.

Victims have reported large losses as a result of this fraud. One victim initially dismissed text messages received from their network provider containing a PAC number. Two days later £6,000 was removed from the victim’s TSB current account. The victim subsequently contacted their phone provider and was informed that someone contacted the provider purporting to be the victim and had cancelled their contract and transferred their number to a new SIM. This action allowed the banking fraud to take place.

What you need to do

PAC Code notifications

If you receive an unsolicited notification about a PAC Code request, contact your network provider immediately to terminate the request. Also notify your bank about your phone number being compromised.

Clicking on links/files:

Don’t be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text. Remember, criminals can spoof the phone numbers and email addresses of companies you know and trust, such as your bank.

Requests to move money:

A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account.

Port-out Fraud versus SIM Swapping

Port-out fraud is often incorrectly referred to as SIM swap fraud. SIM swap fraud works in a similar fashion, however, instead of porting the victim’s number to a new network provider, the fraudster impersonates the victim and requests a new SIM card for their account. Once they have access to the new sim, they have access to the number.

Every Report Matters

If you have been a victim of fraud or cyber crime, report it to us at Actionfraud.police.uk, or by calling 0300 123 2040.