Information sent on behalf of Action Fraud (NFIB)

TSB Phishing Attacks

There has been a sharp rise in fraudsters sending out fake text messages (smishing) and phishing emails claiming to be from TSB. 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 people with this type of fraud.

Since the start of May there have been 321 phishing reports of TSB phishing made to Action Fraud. This is an increase of 970% on the previous month. In the same reporting period, there have been 51 reports of cybercrime to Action Fraud which mention TSB – an increase of 112% on the previous month.

Fraudsters are commonly using text messages as a way to defraud unsuspecting victims out of money. Known as smishing, this involves the victim receiving a text message purporting to be from TSB. The message requests that the recipient clicks onto a website link that leads to a phishing website designed to steal online banking details.

Although text messages are currently the most common delivery method, similar communications have been reported with fraudsters using email and telephone to defraud individuals.

In several cases, people have lost vast sums of money, with one victim losing £3,890 after initially receiving a text message claiming to be from TSB. Fraudsters used specialist software which changed the sender ID on the message so that it looked like it was from TSB. This added the spoofed text to an existing TSB message thread on the victim's phone.

The victim clicked on the link within the text message and entered their personal information. Armed with this information, the fraudsters then called the victim back and persuaded them to hand over their banking authentication code from their mobile phone. The fraudsters then moved all of the victim's savings to a current account and paid a suspicious company.

Protect Yourself:

Don't assume an email or text is authentic:

Always question uninvited approaches in case it's a scam. Phone numbers and email addresses can be spoofed, so always contact the company directly via a known email or phone number (such as the one on the back of your bank card).

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 text or email. Remember, a genuine bank will never contact you out of the blue to ask for your full PIN or password.

If you have received a suspicious TSB email, please do not respond to it, report it to us https://www.actionfraud.police.uk/report_phishing and also forward it to emailscams@tsb.co.uk

Every Report Matters. If you have been a victim of fraud or cyber crime, report it to us online or by calling 0300 123 2040.

Visit Take Five and Cyber Aware for more information about how to protect yourself online.

Message sent by

Action Fraud (Action Fraud, Administrator, National)

This message was sent to Nik Carter, please direct any feedback through Nik or register your own account on https://www.actionfraudalert.co.uk.

Message number : 221614

Information sent on behalf of Action Fraud (NFIB)

TSB Port Out Alert

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.

Protect Yourself:

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.

Message sent by

Action Fraud (Action Fraud, Administrator, National)

This message was sent to Nik Carter, please direct any feedback through Nik or register your own account on https://www.actionfraudalert.co.uk.

Message number : 221616