Action Fraud sees sharp rise in TSB phishing attacks

CITY OF LONDON POLICE
National Policing Lead For Fraud

Protect Alert

Published on 24/05/2018
Reference 18050001

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.

What you need to do

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.