

Victims say they never gave away personal details, so... have crooks got hold of TSB account passwords?

- Fraudsters appear to have obtained reams of personal details for TSB customers
- They are now using these passwords and account numbers to drain accounts
- Con artists call customers pretending to work for the bank's fraud department

By [AMELIA MURRAY FOR THE DAILY MAIL](#)

PUBLISHED: 21:48 BST, 29 May 2018 | UPDATED: 10:39 BST, 1 June 2018

Today, Money Mail raises the alarm over the safety of the personal information that TSB Bank customers use to log into internet banking.

Fraudsters appear to have obtained reams of personal details, passwords and account numbers belonging to TSB customers - and are using them to drain their accounts.

Last week, we revealed that in the wake of the bank's IT meltdown last month - which followed a bungled transfer of accounts to a new IT system - scores of TSB customers were being robbed of their life savings.



Fraudsters: They appear to have obtained reams of personal details on TSB customers

For the fraudsters to steal money, they either have to hack into someone's account or get hold of the information that a customer uses to log in.

To log in with TSB Bank, customers need their online banking ID number, their password and memorable information.

But dozens of fraud victims who have contacted Money Mail insist that they have never handed this information to crooks.

One customer says he has never shared his password with his wife, let alone a stranger.

In some cases, customers say they have had their accounts emptied without even being contacted by a fraudster.

All this raises the prospect that the private details of TSB customers may have fallen into the hands of criminals.

Many customers are being called by sophisticated con artists pretending to work for the bank's fraud department.

Typically, they are told there has been suspicious activity on their account or they are asked to confirm whether a particular transaction is genuine.

The customer is then told to read out a six-digit code that is sent to their mobile phone as part of what the fraudster claims is the bank's 'routine security checks'.



Many customers are being called by sophisticated con artists pretending to work for the bank's fraud department

Money Mail can reveal that these are in fact the 'one-time passcodes' that TSB requires to authorise a payment out of a customer's account.

The bank says it introduced this text message verification system on April 22.

Crucially, to generate a code, someone must already be logged into a customer's online bank account - which suggests that the crooks could be in possession of customers' ID numbers, their secret passwords and memorable information.

TSB says no customer information was leaked in the bank's bungled computer systems upgrade in April - indicating that crooks are getting hold of the information another way.

One theory is that they are exploiting TSB's system and changing passwords and usernames.

To change these details online, customers are asked for their full name, date of birth, postcode, account number and sort code.

The bank then calls a phone number registered to their account to verify the changes.

Some victims claim their mobile phones stopped working just before their accounts were emptied by crooks. Experts say it is possible that their mobile phones were hijacked.



TSB says no customer information was leaked in the bank's bungled computer systems upgrade in April

Over the past two years, bank fraudsters have been known to use a sophisticated technique to divert text messages and calls to their own phones.

This enables them to intercept any codes needed to change passwords or make payments.

Another theory is victims may have been tricked into opening an email that appears to come from TSB and clicked onto a link.

Cliff Moyce, head of financial practice at DataArt, a consultancy, warns: 'Plenty of personal details can be gleaned from sources such as Facebook and other social media.'

And if fraudsters have enough information to pose as the customer, they might be able to trick staff into handing over other details on the phone.'

TSB customer Bernie Wright, a taxi driver from Essex, is adamant that he's never given any personal information to a stranger, or been a victim of computer hacking.

Yet on May 8, fraudsters stole £10,000 he'd set aside for his tax bill, leaving just 52p in his current account and £1.52 in savings.

Bernie, 65, says he only noticed the missing money the next time he logged into his account.

He says his daughter used to work at the fraud department for a big bank, so he follows all the rules to keep his information safe, including never opening or responding to unsolicited emails and hanging up on cold-callers.

He uses the same computer to access his Barclays bank accounts, and these have not been affected.

'There must be something going wrong at TSB,' he says. 'Even my wife doesn't know my password, but the fraudsters managed to get past all of TSB's checks.'

A number of victims have received letters from TSB explaining that the bank's fraud detection systems failed to spot suspicious transactions. The bank would not confirm how many letters had been sent.

Action Fraud, the UK's fraud and cybercrime reporting service, says it has received 51 reports of fraud from TSB customers since the bank's IT meltdown. Together, victims have lost £189,000 — or £3,708 each on average.

However, the true figure is likely to be far higher as many customers do not report scams to the fraud body, or they take months to do so, and many victims have struggled to get through to TSB.

One customer said she had spent a total of 16 hours on hold, while others have waited five hours before being cut off or told the fraud team had gone home.

Mr Moyce at DataArt says: 'The bank is in breach of its banking licence. 'You cannot take people's money and then not provide the service promised.'

A spokeswoman for TSB says: 'Protecting our customers' information is our number one priority.

'We are working with the police and anti-fraud agencies to ensure customers don't become a victim of fraud, whether they bank with us in branch, online or via the phone.

'We also have a specialist team dedicated to investigating the issues reported.

'Meanwhile our commitment is absolutely clear: no customer will be left out of pocket as a result of the recent IT issues.'

amelia.murray@dailymail.co.uk

Original article can be found here: <http://www.thisismoney.co.uk/money/news/article-5784371/Have-crooks-got-hold-TSB-account-passwords.html>