Tesco Bank hack: why you're more at risk of being targeted at the weekend

It was no coincidence that hackers targeted Tesco Bank on a Saturday night CREDIT: JEFF J MITCHELL/GETTY IMAGES

- Amelia Murray

- Richard Dyson

7 NOVEMBER 2016 • 1:16PM

The successful hacking of Tesco Bank - where the accounts of one in three customers were compromised over the weekend - is believed to be the biggest cyber attack on a British bank to date.

The success of the crime, which saw 40,000 accounts compromised and money stolen from 20,000 customers, has surprised and alarmed the banking industry and consumers alike.

Tesco Bank customers were notified after the weekend hacks took place

What did not surprise anyone is that the attack came on the weekend when, as *Telegraph Money* has consistently highlighted, banks are notoriously slow to respond to warning signs or customer reports of fraud.

Criminals are so expert at exploiting banks' low staffing levels over weekends that some forms of fraud are even known as "Friday afternoon fraud".

While banks' electronic fraud detection systems can raise alarms at any time, for the bank to take drastic action - such as halting payments from or to specific accounts - requires managerial intervention, according to fraud experts. And on the weekend these human managers are not at their desks.

You can report fraud anytime, but at the weekend the decision-makers will not be availableCliff Moyce, DataArt

“Tesco's systems are likely to have picked up the irregular activity early on but that would not be enough to stop certain transactions," said Cliff Moyce of DataArt, the technology firm, said.

"Alerts are likely to have been sent to certain key staff who in turn would need to contact senior managers who were unlikely to be working.

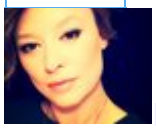
“You can report fraud anytime, but at the weekend the decision-makers will not be available.”

Tesco has said the fraudulent transactions appear to have taken place late on Saturday night and then on into "the early hours of Sunday morning."

Initial texts were sent to customers warning of possible fraud late on Saturday, with some being asked to contact the bank. By Sunday more detailed messages were being sent, acknowledging the widespread nature of the problem.

Countless customers complained they were kept on hold for hours and received no communication from Tesco Bank despite losing hundreds of pounds.

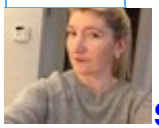
Follow



Kirsty Brown @kirstyktweet

@tescobankhelp we have been hacked, all money gone, no email or text!! Appalling response from Tesco so far #nobodyanswering

Follow



SamAllenAVFC @samallen72

@kirstyktweet @tescobankhelp oh no I hope you get it sorted asap. I understand trying to prevent fraud but the customer service is awful

Mr Moyce said this was typical of cyber attacks where the hope is to cause maximum disruption for the bank and thus win more time for the stolen funds to be successfully moved overseas or into accounts at other banks.

He said that based on Tesco customers' descriptions of their experiences, "automated fraud detection systems appear to have worked well, but a lack of people at desks will not have helped.”

How was the crime committed?

Exactly how criminals committed fraud on such a mass scale has resulted in a spate of speculation.

Mr Moyce said it is not difficult for criminals to get hold of individual customers' login details but the sheer volume of accounts suggests a "serious vulnerability" in Tesco Bank’s own systems.

Joe Hancock, a cyber security lead at Mischon De Reya, the law firm, suggested that as a comparatively small bank Tesco may not have invested as much in online security as larger rivals, making it vulnerable.

Mr Hancock said that rapidly-evolving technologies means customer information in the financial services sector can "sprawl" across a number of the bank's databases, including those of third parties.

Benny Higgins, Tesco Bank's chief executive, confirmed the attack and said the bank would be looking to refund those affected as soon as possible CREDIT: TESCO BANK

Many staff need access to customers data, another factor that makes it vulnerable. However Mr Hancock said the minute you "lock it down" so that only a few people can access it, issues may start to arise especially in terms of customer service.

Both experts suggested the hack could have been the result of a technical weakness or it may have been an insider job.

Mr Moyce said: "The fact it was 40,000 accounts compromised gives you a clue that the details were probably all got in one go.

"This may have been down to the exploitation of a weak system. Or it could be that a member of staff was involved."

Tesco has said nothing other than that the police and the watchdog, the Financial Conduct Authority, aer involved.

Telegraph Money has featured numerous cases where huge frauds have been perpetrated against individuals on, or just before, the weekend.

In most cases the victims did not have their accounts hacked. Instead they were traicked into transferring money to a criminal posing as a solicitor or other trusted party. These scams have become so formulaic they are now referred to as "Friday afternoon fraud."

In January 2015 Ellen Wright was duped into paying £137,000 to a fraudster for a south London flat she had bought at an auction. She called her bank First Direct at 6.40pm on a Friday night to report the crime but was told the fraud team had finished for the night. She was told to call back in the morning.

The fraud team of the fraudster's bank, RBS ,had also clocked off. RBS managed to recover £7,000 but the remaining £130,000 could not be traced.

John Beuvink was contacted on a Friday afternoon in September by a man purporting to be from TalkTalk. They gained access to his online banking and managed to steal almost £7,000. Mr Beuvink hung up immediatley and called his bank TSB. The bank's fraud department was unavailable that evening. It got back to Mr Beuvink the following Tuesday. The bank is still working on retrieving the funds.

Vivian Gabb was also targeted on the first Friday in June 2015. She transferred £47,000 for a buy-to-let flat in Colchester to a criminal she believed to be her solicitor. By the time she became aware of the ruse and contacted her bank Halifax there were no funds left in the criminal's account.

Andrew Doyle and Susan Paul were asked to transfer the last £204,390for their first property together just before the Easter bank holiday this year. The couple enjoyed

their break and did not realise they had been tricked until Wednesday. By this point the money had been drained from the account.

Which banks are the best and worst for online security?

Several banks have been improving their security in recent years with new features such as separate card-readers or biometric log-ins becoming more common.

In general, the "safer" banks have two-step authentication, experts say. So instead of just entering your user-name and password, you are required to prove your identity through an additional step.

This could involve, for instance, generating a unique number on a separate device sent to you by your bank; or generating a number via an app on your phone; or receiving one sent by text to your usual mobile phone number.

Your bank then "knows" that the user is in possession of both your password information and the phone or device regularly used by you - providing a level of confidence that it really *is* dealing with you.

Andrew Doyle and Susan Paul were targeted by fraudsters just before the Easter bank holiday weekend. They lost over £200,000 CREDIT: CHRISTOPHER JONES

But according to Which?, the consumer lobby group, of 11 major current account providers less than half insist on this two-step process for logging-in.

The banks that use two-stage authentication include Barclays, M&S, Nationwide, First Direct and its parent company HSBC.

With the latter two, which performed best in the assessment to log in and transact you need a one-use code generated either by a card-reading device or via an app on your smartphone.

First Direct was also among the first banks to use biometric log-ins. These are generally regarded as more secure than password or information-based-ins - and for consumers they are also often more convenient. Voice ID, where callers' voice patterns are recorded and then checked, is being introduced.

Users of iPhones can also log-in to First Direct's "fd" app by having their fingerprint read on their phone's scanner. This gives access to limited functionality, however. They can look at balances and make payments to existing contacts, but not new ones.

Which? said that banks battled to provide both security and convenience, and that sometimes these two objectives were in conflict.

It cited as worst the banks which either didn;t have two-step authentication or which had it, but did not require customers to use it for many transactions.

These included the banks within the Lloyds group (Lloyds Bank, Bank of Scotland and Halifax) and TSB, an independent bank which was formerly part of Lloyds.

In order to undertake the research Which? asked customers of all the major banks to volunteer so that a range of account features could be tested. These covered log-in processes and logging-off processes, as well as other potential vulnerabilities such as the ability to make payments to people whose details have not been entered before.

From best to worst: how online banks fare for security, according to Which?

Original article — http://www.telegraph.co.uk/personal-banking/current-accounts/tesco-bank-hack-why-youre-more-at-risk-of-being-targeted-at-the/