



MailOnline

Most recent stories related to this article:

-  [HSBC makes £7bn profit in six months... but STILL won't help firms as lending remains low](#)
-  [HSBC announce soaring profits beating expectations amid lending furore](#)

How safe is your current account?

By [Lauren Thompson](#)

Last updated at 9:54 AM on 21st July 2010

Millions of customers of three of Britain's state-backed banks are at risk of having their accounts plundered by online fraudsters, an investigation has revealed.

Online banking customers with the three big names are vulnerable to a remote attack by criminals because of poor security on the banks' websites.

The claim comes in a report by Ben Smyth, a researcher from the University of Birmingham's School of Computer Science. He probed the security of the main High Street banks and discovered particular problems with state-aided RBS, NatWest and Halifax.

He says that questions asked if someone has forgotten their password are too easy to guess and leave customers particularly vulnerable to attacks from former partners, estranged family members or colleagues.

'Millions of people could be at risk from online banking sites that are poorly designed,' says Mr Smyth. 'Banks are too interested in making their sites user friendly, instead of secure.'

Banks lost a staggering £59.7 million to online banking fraudsters in 2009 — a 14 pc rise on the previous year.

But the real losses suffered by consumers could be much higher, as in many cases banks refuse to pay back consumers who fall victim to online scams and say customers must have been 'negligent' with their password if their account is hijacked.

Banks blame the increase in fraud on:

- Phishing attacks, where a victim opens a scam email and clicks on a link to a fake banking website.
- Computer viruses, known as malware, that capture everything a victim types, allowing fraudsters to learn passwords.

While both these types of attacks are increasing, banks rarely admit some fraud losses might be down to the poor design of their own websites.

The Royal Bank of Scotland Group, which includes NatWest, has 4.7 million customers who bank online. It requires users to state their name; date of birth; card number; three-digit security code; sort code and account number if they have forgotten their password.

If a fraudster has this information, they can access an account - although they can only make payments to people already set up as payees on the account.

Halifax, which has almost 3 million customers banking online, and its subsidiary Bank of Scotland, requires customers to answer two of the following four questions if they have forgotten their password: father's first name, mother's first

name, place of birth and first school.

They must also answer a question that the customer has set themselves - but many people choose an obvious question which is easy to guess, such as: 'What is my mother's maiden name?'

If a fraudster is also able to gain access to the victim's email account, they could completely take over their bank account and potentially drain the funds.

Mr Smyth says it is possible for fraudsters to gain access to email accounts in a number of ways because many email accounts have 'Remember me' technology, whereby a user remains logged in on a particular computer.

Personal and financial information could be easily accessible to cleaners, lodgers, retailers and bank staff committing 'inside jobs', as well as remote attackers.

Michael Lynch, of insurer CPP, says: 'It is very important to buy good anti-virus software from a reliable source - such as your bank or internet service provider - and keep it regularly updated.'

A spokeswoman for Lloyds Banking Group, which includes Halifax, says: 'Should any of our customers fall victim to fraud via their online bank, we will reimburse them for their loss so they do not suffer financially.'

An RBS spokeswoman says: 'Online transactions are restricted to registered users and controlled by several levels of security - some of which will not be visible to customers.'

Hijacked

Andrew Gates had his online bank account hijacked by fraudsters last month. The 29-year-old discovered someone had set up a monthly standing order for £900 after somehow obtaining access to his HSBC account.

The bank immediately refunded the money. 'I have no idea how the fraudster accessed my account,' he says. 'I only noticed the standing order because HSBC sends me a text message every morning with all my recent transactions.'

Mr Gates, pictured with girlfriend Helen Chapman, from Brockley, South-East London, has never clicked on a link in an unsolicited email or told his log-in details to anyone.

He is not aware of any viruses on his computer.

He says: 'I've used online banking for years with no problems, but it's worrying that someone has managed to obtain my log-in details.'

If an HSBC customer has forgotten their log-in details, they need their date of birth and then either sort code and account number or credit card number, as well as three random digits from their security number, to regain access to their account.