This is MONEY.co.uk
FINANCIAL WEBSITE OF THE YEAR

How safe is your online banking? Three things you must know to check that your money is protected

- **Banks take security very seriously and invest millions each year into it**
- **But some banks are considered to have safer systems than others**
- **We explain what you must know about bank security and how to check yours**

By AMELIA MURRAY FOR THE DAILY MAIL
PUBLISHED: 11:22 BST, 10 September 2018 | **UPDATED:** 17:30 BST, 10 September 2018

The rise of online banking means it's never been quicker to check your balance or pay bills. But all this convenience comes with some big risks.

For example, what if an IT meltdown freezes you out of your account?

Or what if a cyber-criminal hacks into your account and raids your savings?

Banking online has become a way of life for many Britons, but how safe is it?

Those of a younger generation tend to take a gung-ho attitude to these risks.

But many of those who did not grow up with computers remain reluctant to join the online banking revolution.

Perhaps that's no surprise when you consider that online, telephone and card banking fraud cost victims nearly £1billion last year, according to figures from trade body UK Finance.

Over the past few years, we have detailed numerous cases of customers being duped out of hundreds of thousands of pounds. If they hadn't used internet banking, this wouldn't have been possible.

So how safe is it to use your home computer or smartphone to manage your money?

Passwords alone won't keep you safe

Banks take security extremely seriously and invest millions in trying to keep you safe.

Normally, they will ask you to key in several different passwords containing both letters and numbers when you log into your account online.

They may also ask you to recall memorable information that you've previously supplied.

But security experts warn that passwords alone are not enough to protect your cash because they can be stolen or guessed.

It's particularly risky if you use the same log-in details for several websites; if one gets hacked, fraudsters might be able to obtain enough security details to raid your account.

Earlier this year, the Daily Mail revealed that personal financial information is being bought and sold daily on hacking websites.

The answers to common security questions, such as your mother's maiden name, can also be gleaned from social media or even ancestry websites.

Banks have brought in two factor security to protect customers, because simple password systems are easier to hack

Why two-factor security matters

Some banks, such as First Direct and HSBC, have added a second layer of security to help.

This second layer usually takes the form of a code which is generated either on your mobile phone or a small digital device or a card-reader that is given to you by your bank.

HSBC's device looks a bit like a small calculator. Every time you log into your account online, you need to generate a code on this device and type it into the website. In theory, this should make it very difficult for a cyber crook to hack in and steal your savings.

Barclays and Nationwide offer a small, pocket-sized card-reader. To make a payment, you insert your debit card into the gadget to generate a code. This can then be entered online to approve the transaction.

This extra layer of security is known in the jargon as 'two-factor authentication' — and it's extremely important. Experts say this type of two-step process is the bare minimum level of security banks should be using to verify who is really logging in.

Two-step authentication cuts the risk of fraud by around 80 per cent, according to Cliff Moyce, global head of finance practice at technology consultancy DataArt.

The first step is normally defined as something you know, such as your password or other key facts about yourself. The second step is something you have in your possession, such as a gadget that generates a code.

Many banks are using, or developing, so-called biometrics technology to take this second step of security to an even higher level. Biometrics mean something unique to your own body that can be scanned, such as your fingerprint, face or your iris.

Some banks send text messages to confirm payments, but fraudsters can manipulate these systems too and steal thousands of pounds

The dangers of using texts to confirm payments

But, incredibly, not all banks have this crucial second stage of identity checking when you log in.

Last year, consumer group Which? named and shamed five High Street banks that do not require two-factor authentication when customers sign in — despite having the technology to do so.

Lloyds Banking Group, which includes Halifax, Lloyds and Bank of Scotland; Santander; TSB; NatWest and the Co-Operative Bank, have still not brought in two-factor authentication when customers log in.

In fact, they use the extra security checks only if customers try to pay someone they have never sent money to before.

Yet, as Which? has warned, if fraudsters managed to get hold of a customer's passwords and make it past the first stage of security, they could find details of recent transactions and a goldmine of personal information they can use to carry out scams.

Money Mail has heard from scores of people who have lost their savings to sophisticated ploys like this. Criminals, typically posing as bank staff, cold-call their victims claiming they have spotted suspicious activity on the person's account.

The crooks explain that to verify the customer's identity or freeze outgoing payments a code will be sent to their mobile. The bank customer is then encouraged to read this out over the phone.

Once in possession of the code, the fraudster is able to log in and make payments to siphon money out of their account.

When thousands of TSB customers were locked out of their accounts in the bank's IT meltdown earlier this year, opportunistic thieves used this type of ruse to scam victims.

Posing as bank staff, they claimed customers needed to hand over codes as part of the security procedure or to get money back for trouble caused.

Mr Moyce warns there are even weaknesses in mobile phone networks that allow hackers to intercept messages sent to your phone.

He says: 'Criminals can get into your online account using information gained from another type of data breach, and then intercept messages to your phone and carry out transactions as though they were you.'
Banks including First Direct, Metro and NatWest have introduced thumbprint or face scans when customers log in via their smartphone apps. But Mr Moyce says even this technology is not completely failsafe.

Lloyds Banking Group, NatWest, Santander, TSB and Co-Operative Bank all say their security is in line with industry standards, but they are always looking at new ways to protect customers.

All say they require two-factor authentication for payments to new payees and other higher risk transactions.

A spokesman from UK Finance says the industry is constantly investing in security systems to keep customers safe, as well as providing free security software.

A spokeswoman for the Financial Conduct Authority says that from September 2019, all banks will have to comply with stricter measures for verifying a customer's identity.

Original article can be found here:
https://www.thisismoney.co.uk/money/beatthescammers/article-6150709/How-safe-online-banking-Three-things-know.html