

**Don't be fooled, don't be phished**  
A guide to personal online banking security





## Don't be fooled, don't be phished

### A guide to personal online banking security

#### Introduction

Welcome to this simple, plain English guide to banking safely online. It is a shocking fact that online banking fraud cost the **UK £52m in 2008** – and this does not take into account the disruption, worry and sometimes hardship this crime causes its victims.

Thankfully, avoiding falling victim to online banking fraudsters is mostly a matter of common sense – if you know how they operate. This guide will give you the facts you need to keep the fraudsters out of your bank account.

#### **First of all, don't be put off**

Remember that online banking is safe and secure, as long as you take the necessary steps to protect yourself. This is really no different from putting locks on the doors and windows of your home – you just have to know what the risks are and how to protect yourself.



## How do fraudsters access my online bank account?

In essence, they seek to get hold of your log-in and security details (passwords, customer numbers and the like – all the details you would use to access the service securely).

Once they have these details, they can access your accounts in the same way you do, and siphon off your money



## How do they get hold of my details?

There are broadly two ways in which fraudsters try to get your passwords:

### Phishing:

- The fraudsters send emails which seem to have come from your bank. These emails will use all kinds of ruses to get your attention – for instance claiming to be alerting you to a security issue that needs your attention.
- The email will ask you to log into your internet banking site, for instance to reset or confirm your security details – and, crucially, provide a link to the site.
- However, the link will either direct you to a fake site, or to the genuine site with an unusual ‘pop-up’ box over the top, asking for your log in details. The sites are designed purely to record your passwords on behalf of the fraudsters.

### The Trojan virus:

- These scams work in very much the same way as the Trojan horse they are named after.
- Again, they originate from unsolicited emails – sometimes they may even appear to have been sent by people you will know. The email will include a link to a website, often offering discounts on things like electrical goods.
- When you visit the site, your computer will be infected by a virus – a Trojan virus capable of installing software on your computer.
- This software is called a ‘keystroke logger’ – in essence, this software will record everything you type and send the details back to the fraudster.
- With that information, it is a relatively simple matter for the criminals to work out all your passwords.



## How do I avoid these scams?

Once you know how these scams work, avoiding them is mainly about applying common sense and keeping your computer's security software up to date.

### Phishing:

- It is important to realise that, whilst banks may email their customers from time to time, they will **NEVER** ask you to give your security details.
- Once you realise this, avoiding phishing emails is pretty straightforward.
- First of all, there are some tricks to spotting phishing emails:
  - You can sometimes identify phishing emails by looking at the address they come from (an unusual address such as service12@bank.com), or because they use strange spelling or grammar to avoid getting caught up in your email spam filter. However, the 'From' address in an email is easily faked, so this alone should not be relied on.
  - Remember also that the scammers send out huge quantities of these emails and may not know your name. The email may be vaguely addressed – for instance 'Dear valued customer' - or will use the first part of your email address
- **REMEMBER** – whilst the above are useful pointers, it is always better to err on the side of caution. If in doubt, contact your bank by telephone or in person.
- In general, the following guidelines will help to ensure that you do not fall victim to phishing scams:
  - **NEVER** click on internet links in unsolicited emails from financial companies, even if you think they may be genuine.
  - Always type your bank internet address into your web browser (for instance Internet Explorer or Mozilla Firefox) – most internet banking log in page addresses will begin with the letters 'https' and will display a small padlock symbol in the bottom right hand corner. These are good indications that you are visiting a genuine online banking website
  - Remember, if in doubt, contact your bank by telephone or in person to ask if an email is genuine. Never act on the instructions in any email apparently from your bank without doing this first.
  - Finally, you can report suspicious emails by forwarding them to reports@banksafeonline.org.uk. It's OK to open the email in order to forward it, but **DON'T CLICK ON ANY INTERNET LINKS**



## Trojans:

- First and foremost, since Trojans are viruses, make sure that your computer is properly protected:
  - Use a secure web browser. For instance, if you use Internet Explorer, make sure you keep up to date with security updates from Microsoft – in particular any Internet Explorer Critical Updates. These are available for free from <http://windowsupdate.microsoft.com/>. Alternatively, you could consider using a different web browser, such as Mozilla Firefox (but you will still need to update it as new versions become available).
  - Make sure your computer has a firewall installed and switched on. Basically, a firewall is a bit of software that prevents any unauthorised access to your computer via the internet. To check your firewall is switched on, open your computer's Control Panel (Start Menu) and select 'Security' or 'Security Centre'.
  - Make sure your computer has anti-virus software installed, and that the software is set to update itself automatically. This will ensure that your computer is always protected by the latest software updated.
- The steps above will help to ensure that your computer is not vulnerable to viruses, but there are also some common sense steps you can take to avoid being scammed in this way:
  - Treat unsolicited emails with suspicion, and **NEVER** open any internet links they may contain
  - If an email appears to come from someone you know, but contains unusual spellings and a link to a website you do not recognise, treat it with suspicion and **DO NOT** open the link. If you are intrigued, check with the person who seems to have sent you the email. It may be that their email account has been compromised by fraudsters and the email is a fake

We hope you find this guide useful, and that it helps you to enjoy the convenience of online banking safely and with confidence. If you need more information, we suggest visiting <http://www.banksafeonline.org.uk/index.html>. The site is provided by the UK banking industry and contains a wealth of information and resources on banking online securely.