

## Security

### Anti-virus software

To combat the increasing threat from viruses and hackers, it's important that you run antivirus software on your computer to detect viruses and other threats to your computer. Anti-virus software checks the contents of files on your computer against the information it holds about known viruses. The software will alert you when it finds a problem, and either remove it for you, or recommend further action.

Anti-virus software can only check for viruses it knows about, and new viruses come out on a daily basis. So, to stay safe from the latest viruses, it's essential to keep your anti-virus software up to date. There's a wide range of anti-virus software products available. In addition, there are a number of companies that provide 'Internet Security' products, which combine anti-virus software, firewall and anti-spyware software into a more complete package. The following are leading providers:

- [Zone Alarm Internet Security](#) (opens a new window)
- [Trend Micro PC-Cillin Internet Security](#) (opens a new window)
- [Norton Internet Security](#) (opens a new window)
- [McAfee Internet Security Suite](#) (opens a new window)

These links are provided as part of our commitment to making online banking safe and secure. However, we cannot accept responsibility or liability for the content or availability of external sites. We cannot guarantee that any software downloaded from these sites will work, or be free from viruses or malicious code.

### Cookies

#### How we use cookies

Cookies are small pieces of information which are placed onto your computer's hard disk by a website you have visited. They can be accessed at a later date by the same website, to retrieve details you may have supplied to that site.

For example, a weather site may ask you to specify where you live. It would then store this information in a cookie, so that when you return to the site it knows which forecast to show you. Cookies from the Halifax International website (apart from those which store your sign in details) remain in your browser for 90 days before they expire.

\*If you have any anti-spyware software installed on your computer, e.g. 'cookie washing', you may be unable to have your username remembered.

### Identity theft

Identity theft occurs when someone's personal information is used by someone else without their permission or knowledge.

A person's identity is a valuable commodity and criminals have become ever more ingenious in their quest to get hold of a convincing false identity. A criminal does not need to obtain a person's whole identity to commit fraud; they may only need the key elements such as name, address and date of birth. This may then be used to support criminal activity, involving fraud, deception, or obtaining benefits and services in the person's name. It is estimated that more than 100,000 people are affected by identity theft in the UK each year, costing the economy over £1.3 billion annually.

## Keeping your Browser updated

We recommend you keep your browser up to date, because the newer versions provide higher levels of security. You can download the latest browser versions from the web for free, subject to your usual telephone or internet usage charges. The main sites to obtain upgrades are:

- [Microsoft Internet Explorer Home](#) (opens a new window)
- [Firefox home page](#) (opens a new window)
- [Safari Support page](#) (opens a new window)

These links are provided as part of our commitment to making online banking safe and secure. However, we cannot accept responsibility or liability for the content or availability of external sites. We cannot guarantee that any software downloaded from these sites will work, or be free from viruses or malicious code.

## Operating systems

Your computer's operating system performs basic tasks such as handling input from the keyboard, sending output to the monitor, keeping track of files and folders, and talking to external devices, such as printers. It also provides an environment for other programs, such as word processing programs and web browsers, to run in. Common operating systems include Windows XP (for PCs) and Tiger (for Macs).

It's important to keep your operating system up to date, as updates are released from time to time to address security issues. If you're running Windows, you can download updates from the [Microsoft security site](#) (opens a new window). This site will also allow you to set up your PC to receive updates automatically from Microsoft, so you don't have to remember to do this when updates become available.

Further information on identity theft and how to protect yourself is available at the [Home Office website](#). (opens a new window).

These links are provided as part of our commitment to making online banking safe and secure. However, we cannot accept responsibility or liability for the content or availability of external sites. We cannot guarantee that any software downloaded from these sites will work, or be free from viruses or malicious code.

## Passwords

The online banking service features very high levels of security, but none of it will help if someone gets hold of your personal sign-in details, particularly your password. For this reason it's extremely important to choose a secure password and keep it safe. Here are some tips for doing just that.

- Always use a mixture of letters and numbers in both upper and lower case for your password. Don't use names in their usual form (**m4X13** is better than **Max13**), or words that you find in a dictionary (**F15hing28** is better than **fishing28**)
- Don't use the same passwords for a number of different online services
- Never write your password down or save it on your computer
- Never give your password and/or security details to anyone else
- Change your password frequently-every couple of months at least

If you think that someone else knows your password, sign in and change it straight away.

**Please note we will NEVER ask you to confirm your password by email.**

## Phishing

Phishing emails look like they're from your bank, and usually ask you to log into your online service to confirm your personal details and security information.

When you click the link in the email, you are taken to a 'spoof' site which looks like your bank's online service, but in fact has been set up by the person who sent the email. They hope that you will be fooled into giving away your confidential details.

Halifax International would never ask you to confirm your sign-in details in this way.

The sender of the phishing email does not know you are a Halifax International online banking customer – they send emails to a huge number of addresses, knowing that some of the recipients will be Halifax International customers. So how did they get hold of your email address? It will probably have been intercepted, or sold on, when you provided it over the internet for legitimate reasons. Halifax International would never pass on your details to anyone else.

### How to spot a phishing email

Phishing emails usually include official-looking logos and information taken from legitimate websites in an effort to appear convincing. But there are things you can look out for, which should make you suspicious.

First and foremost, Halifax International would never send you an email asking you to verify your secure online banking details. Any email asking you to 'verify your account', 'confirm your sign in details', or using a similar form of words, is certainly a scam. Secondly, beware of links in emails. Web addresses in phishing emails can be masked (disguised) so that they appear to be taking you to a trusted address, but in fact they point to somewhere different usually a spoof site that has been set up by the fraudsters, to try and get you to hand over your details. Genuine emails from Halifax International do contain links, but never to the online banking sign in page. If you are in any doubt about whether an email is genuine, don't click the link.

### What to do if you receive a phishing email

- Don't follow any links in the email, or reply to it
- Forward the email to **onlineemailinvestigations@hbosplc.com** replacing the subject line with 'Report'
- Delete the suspicious email

If you are concerned that you may have disclosed any personal or security details, please call our helpdesk immediately on: **08458 50 06 29**.

If you receive phishing emails from organisations other than Halifax International (such as other banks, eBay or PayPal), please contact those organisations directly to report the problem.

You may also wish to:

- Check that your anti-virus software is up to date – the email may also contain a virus
- Check that you have all the necessary browser and operating system updates installed (if you are running Windows, start by visiting [Microsoft Security Home](#) (opens a new window))

## **Spam and scams**

If you have an email address, you'll be used to receiving spam - unwanted junk email, sent automatically to thousands of people. There are a number of ways you can end up on a spammer's mailing list, including:

- Signing up for a newsletter from a unscrupulous website, which sells on the email addresses of its subscribers
- Providing your email address on a newsgroup, message board, or your personal web page
- Choosing an email address which is then guessed (automatically generated) by software used by the spammers

## **Sinister spam**

Some spam emails contain attempts to defraud you or damage your computer:

- They may infect your computer with a virus - a program that does something malicious, such as sending random files (or copies of itself) from your computer to everyone in your address book.
- They may contain a Trojan - a malicious program that may appear to be innocent (or be invisible altogether), but does something you don't expect, like sending your confidential information to a remote computer.

## **What you can do about spam**

To cut down on the amount of spam you receive, you can ask your ISP (Internet Service Provider) about spam-filtering software. This will allow you to flag e-mails as spam, so that you do not receive as many in future. But some spam will always get through, so you'll still need to delete it.

If you are unsure about whether an email is genuine, assume it isn't and delete it. If you receive an attachment you weren't expecting, or from someone you don't know, don't attempt to open it. If the email looks like it's from Halifax International, report it to us.

To get more information about online security issues, try the following links:

- [Bank Safe Online](#) (opens a new window).

An advice website set up by APACS, the UK payments association, to keep banking customers up to date on online security issues.

- [IT Safe](#) (opens a new window).

A government site launched to provide individuals and small businesses with advice on protecting computers and other devices against internet fraud.

- [UK Government](#) - Home Office (opens a new window)

A site provided by the Home Office Identity Fraud Steering Committee to combat the threat of identity theft.

- [British Bankers Association](#) (opens a new window)

- [Metropolitan Police](#) (opens a new window)

## **Spyware**

Spyware is a term used for software that is installed on your computer, often without your proper consent, to display advertising, collect personal information, or change the configuration of your computer.

You might have spyware or other unwanted software on your computer if:

- You see pop-up adverts even when you're not browsing the web
- Your browser's start page or search settings change without warning
- A new toolbar appears in your browser that you didn't want
- Your computer starts to run slower or crash more often

Spyware is often installed along with other software that you have downloaded. 'Free' software like browser toolbars, weather programs and screen savers sometimes install spyware onto your computer. In the 'small print' of the license agreement that you see during installation, it will tell you that the extra software is going to be installed, but many people don't realise the implications.

Usually this software is fairly harmless - it collects information about your browsing habits and displays advertising targeted to your interests - but it may slow down your computer and you may think it invades your privacy. If you have read the terms and conditions of installing the software and are happy to accept them, there's no problem. Some spyware is more malicious - it may scan your hard disk to try and capture your personal information, such as banking details and passwords, and transmit them to criminals. It may also try to shut down your anti-virus or anti-spyware programs. To help keep your system free of these threats, follow our tips on avoiding spyware.

## **Avoiding spyware**

Spyware can invade your privacy, bombard you with pop-up windows, slow down your computer, and even make it crash.

There are three main steps you can take to protect your computer against spyware and other unwanted software.

### **1. Download and install anti-spyware protection**

Microsoft offers a free anti-spyware program, [Windows Defender](#) (opens a new window), to Windows users.

### **2. Keep your software up to date**

Make sure the software on your computer - particularly the operating system - is up to date. If you're running Windows, you can download updates from the [Microsoft security site](#) (opens a new window). You can use the Microsoft security site to allow your PC to receive updates from Microsoft automatically, so you won't have to remember to download them. Alternatively, you can manually set your computer to receive updates automatically.

### **3. Surf and download safely**

Most spyware is installed when people surfing the net don't realise what they're agreeing to. Follow these tips to make it less likely you'll be caught out.

- Only download programs from websites you trust. If you're not sure whether a particular program is safe, ask a knowledgeable friend, or enter the name of the program into your favourite search engine, to see if anyone has reported that it contains spyware
- Read all security warnings, license agreements, and privacy statements associated with any software you download
- Never click 'OK' or 'I agree' in a pop-up window on the internet unless you are sure what you are agreeing to
- Be wary of 'free' music and movie file-sharing programs, and make sure you understand what the software comes packaged with those programs

Links to external sites are provided as part of our commitment to making online banking safe and secure. However, we cannot accept responsibility or liability for the content or availability of these sites. We cannot guarantee that any software downloaded from these sites will work, or be free from viruses or malicious code.

### **Personal firewall**

A personal firewall looks after the security of your internet connection. It blocks any malicious attempts by hackers to connect to your PC.

A firewall also lets you decide which programs are allowed to connect to the web. If a program tries to connect to the internet when you haven't previously given permission, your computer will display a warning. You can then decide whether to allow or block the connection. This helps guard against viruses, adware and spyware.

Windows XP comes with a firewall built in, and a number of free and reasonably priced personal firewall programs are available.

### **Trojans**

A Trojan is a computer program that may seem innocent, but has been designed to damage your computer in some way, or send confidential information to another computer over the internet.

Fraudsters can use Trojans to record your activities on the internet (sometimes known as keylogging), without you knowing. They can then find out sign-in details for online banking, and access your account.

Some Trojans are designed to display a dialog box when you visit certain websites, such as online banking sites. The dialog box pops up in front of the website, asking you to enter your sign-in details. It looks like you are logging in, when in fact you are sending your confidential information to the fraudsters.

We would never ask for your sign-in details in a pop-up window or dialogue box. If you are asked to complete your sign-in details in a format which appears to be different to our standard sign-in page, it's probably because of a Trojan (or an attempt at phishing).

### **Viruses**

A virus is a computer program that is installed onto your computer without your knowledge, with the intention of doing something malicious. This can range from making your computer behave strangely (playing music or displaying messages) to changing or deleting files, or even wiping the contents of your hard disk.

Viruses are designed to replicate themselves when they are run, so that every part of your computer becomes infected. If your system is infected, you can easily spread the virus to others through sharing disks or sending email attachments.

To keep your system free of viruses, use anti-virus software and keep it updated.

## **Glossary**

### **Adware**

Short for 'advertising-supported software', adware is software that displays advertisements. 'Free' software sometimes conceals the fact that it carries advertising - it may even install a separate adware program on your computer without telling you. For this reason, it's a good idea to be wary of free software, unless you are confident that the software provider is genuine.

### **Anti-virus software**

Software which detects viruses and other threats to your computer. The program alerts you when it finds a problem, and either removes the problem from your computer or recommends further action.

### **Browser**

A software program used to find and display web pages on the internet. Examples of browser programs include Internet Explorer, Firefox and (for Macs) Safari.

### **Cookies**

Small pieces of information which are placed onto your computer's hard disk by a website you have visited.

### **Dialog box**

A small window which appears on screen, usually prompting you to respond.

### **Encryption**

Scrambling data so that personal information, for example, can't be seen by anyone else as it travels between your computer and a secure website.

### **Firewall**

A program which protects your computer from unauthorised access by third parties over the internet.

### **Internet Service Provider (ISP)**

The company who supplies you with your internet connection, for example BT Openworld, Tiscali, Blueyonder.

### **Malware**

Shortened from 'malicious software', malware is a generic term used to describe software intended to cause damage or disruption to a computer, or to do something not in the interest of the person using it. Examples of malware include viruses and Trojans.

### **Operating system**

The underlying program, such as Microsoft Windows XP, that enables your computer to run software applications, such as email and browser programs.

### **Patch**

An update to a program or operating system, which is needed to correct a problem (often a security issue) overlooked at the time the program was released. Sometimes called a 'fix'.

**Phishing**

'Phishing' is an email scam which tries to get you to provide your personal sign-in details, so that fraudsters can gain access to your accounts. Remember, Halifax International would never ask you to confirm your secure information in an email.

**Spam**

Unwanted emails, usually offering dubious products and services. Various types of anti-spam software are available, but the first line of defence may be your own ISP - many offer spamfiltering services.

**Security certificate**

Security certificates are issued to secure websites to allow them to prove they are genuine. To view a security certificate, double-click on the yellow padlock icon at the bottom right of your browser window. This allows you to check that you are on a genuine online banking site, and not a 'spoof' website.

**Spyware**

Spyware is software, usually installed without your consent, which communicates personal or confidential information about you to a third party. The information may contain reports on your web-surfing habits, collected for market research purposes, or more sensitive information, such as credit card numbers.

**SSL**

SSL (Secure Sockets Layer) is a way of encrypting (scrambling) information, such as bank account details, as it is passed from a web browser to a web server. A web address beginning with https: shows that SSL is being used, so the website is secure. A security certificate allows you to check the credentials of the secure site.

**Trojan**

A malicious program that may pretend to be innocent (or be invisible altogether), but does something you don't expect, like sending confidential information to somebody else's computer.

**Virus**

A malicious program which is intended to damage your computer.