

Online Security

Savings



*For the
road ahead*

What is online security?

This booklet is designed to make you aware of some of the latest threats that exist when managing your money online so you can protect your money in the same way you would protect your house, your car, or other things that are valuable to you.

We are committed to looking after your money. We use a variety of security measures to keep all your details totally safe when you manage your money online.

Top Tips for protecting yourself online

- Ensure you have Anti-virus protection
- Make sure you're protected by a Firewall
- Keep your computer software up to date
- Look after your security details
- Protect yourself from Trojans and spyware
- Take care not to respond to fraudulent Phishing e-mails
- Check the security of e-commerce sites
- Log out properly when you've finished with a secure site
- Exercise caution when using computers in public places
- Keep passwords and log in details safe
- Read this 'Online Security' booklet to understand how to protect your computer and who to contact if you're a victim of fraud.

How to protect yourself online

Protect your computer

Ensure you have Anti-virus protection

An Anti-virus protection system helps you to find and remove any viruses or suspicious programs. We strongly recommend that you have up to date Anti-virus software installed on your home computer and that you ensure that the software is kept up to date with the latest virus definitions.

If you access the internet from your workplace please check that your employer has installed an Anti-virus solution. It's recommended that you use an Anti-virus program which has an Auto Update feature. A scan of all files should be scheduled at least once a week; Norton, McAfee and Kaspersky are examples of credible suppliers that provide Anti-virus software. You can get free anti-virus software from Grisoft, Anti Vir, and ALWIL/Avast.

Be aware that some Anti-virus software is better than others - for further information please visit www.virusbtn.com

Make sure you're protected by a Firewall

A Firewall protects your computer from unauthorised access and blocks unwanted internet activity. If you're using your home computer to access the internet you should use a software Firewall. If you use a computer at work check that your employer is maintaining a Firewall.

It is recommended that your Firewall is set up to work on both incoming and outgoing traffic. Not only would you have control over what comes into your computer but you'd also have control on what leaves your computer. Like Anti-virus software, a range of Firewalls are available as free downloads from companies such as ZoneAlarm, Kerio and Sygate to commercial products from Norton, McAfee and Trend Micro. Firewall software is also built into Windows XP, Windows 7 and Mac OS X although you may need to activate these as they may not be setup to work as a default.

To ensure your firewall is working properly, visit: www.symantec.com/Norton/internet-security or www.grc.com Advice on Firewalls is available at www.firewallguide.com

Keep your computer software up to date

It's quite common for security problems to be discovered in existing software. When this happens the Software Company will usually issue an update known as a patch. If you've an Apple computer running OS X, you should run

the Software Update tool at least once a week. If you've a Windows computer, you should regularly use Windows Update or Microsoft Update to check for new patches from Microsoft. In some versions of Windows, this will be an option in the Start Menu, in others you may have to select Windows Update from the Tools menu of Internet Explorer.

You should regularly check for updates to the main software on your computer by visiting the suppliers website or using the update features in their software where these are available. To check for updates and patches you should visit your software publisher's website.

These websites can provide more information to help you keep your computer up to date: www.microsoft.com www.apple.com

Stay Safe Online

Exercise caution when using computers in public places

As you cannot be certain about the security of a computer in a public place such as a library or Internet café, you should be careful if you have to use such a machine. If you've any reason to be suspicious about a public computer you should not use it to access services such as Internet banking.

You should never change your security details such as your password on a publicly accessible computer (e.g. in an Internet café). If you do use a public computer to access Internet banking you should look out for anyone who could be watching you.

For more advice and a step by step guide to staying safe online visit www.banksafeonline.org.uk a website launched by APACS, the UK payment association working on behalf of the banking industry.

Log out properly when you've finished with a secure site

Never leave your computer unattended when logged in to a secure session such as when you're using Internet banking. Ensure you log out properly when you've finished banking online or using another secure site.

Keep hold of your cash

Don't be conned by convincing e-mails offering you the chance to make some easy money. If it looks too good to be true, it probably is. Be especially wary of unsolicited e-mails from outside the UK - it will be much harder to prove they are who they say they are.

Protecting your savings

Keep your identity secure

Look after your security details

Your UserID and Password, along with the answers to your security questions, are the key to your online accounts and information. You should keep these secure and never share them with anybody. Ensure you change your password within the online system on a regular basis. Additional information is available at www.antiphishing.org

Phishing

Watch out for fraudulent e-mails

A common type of e-mail fraud is **Phishing**. Phishing is the process where fraudsters (impersonating a well established financial organisation) send false e-mails in an attempt to trick the people who receive them into revealing their personal details. We will never ask you to send your personal details via e-mail. If ever you receive an e-mail that asks you to provide your personal information by clicking on a link please do not access any links, disclose your sign-in details or reply - even if the e-mail suggests that you need to take immediate action.

Phishing is not the only way that criminals try to use e-mail for fraud. E-mail has been used to make job offers, recruit people for money laundering and trick people into visiting sites that exploit weaknesses in their computer to download Trojans. Don't be conned by convincing e-mails offering you the chance to make easy money or provide your personal details. Remember, we will never ask you to confirm your personal details via e-mail.

You can report a phishing e-mail at www.antiphishing.org as well as forwarding the e-mail to us at abuse@birminghammidshires.co.uk Be very careful if you receive an e-mail from an unknown or dubious source. Be especially cautious if these e-mails contain attachments.

HOW TO SPOT A PHISHING E-MAIL

- Remember that we will never send you an e-mail asking you to verify your secure and online details. Any e-mails asking you to do this are surely a scam.
- Beware of links in e-mails. Genuine e-mails from us do contain links, but never to our online banking pages. If you're in doubt about whether an e-mail is genuine or not, don't click on the link.

WHAT TO DO IF YOU RECEIVE A PHISHING E-MAIL

- If you still have the original e-mail, you can assist us by providing a copy of the e-mail by following the procedure below.
- If you are using Microsoft Outlook or some other mail handling software, open the e-mail, click on 'file' and then 'save as'. This should allow you to save the e-mail as a separate file.
- Don't reply to the e-mail.
- Send the file you have just saved to abuse@birminghammidshires.co.uk (This allows us to preserve the source data from within the e-mail and makes it easier for us to track down the originator of the e-mail).
- Delete the e-mail immediately after sending it to the above, without clicking on any links or replying.
- Additional information is available at www.antiphishing.org

WHAT TO DO IF YOU BELIEVE YOU HAVE BECOME A VICTIM OF FRAUD

- Check your accounts regularly and report any suspicious activity by contacting us on **0845 603 6302**
- Contact other banks and financial institutions with whom you hold accounts to ensure they've not been affected.
- Check your computer is protected with adequate security.
- If you believe you have become a victim of fraud contact us immediately on **0845 603 6302**

HOW TO RESET YOUR PASSWORD

- If you'd like to reset your password, log into www.theAA.com/savings
- Enter your username, password and answers to memorable questions.
- Click option on left hand side to change password.
- Once you've changed your password, an e-mail will be sent confirming your password has been changed.

For more information, please call

0845 603 6302

Know about Trojans and Spyware

Trojans

A Trojan is a hidden program that contains malicious code designed to either give control of your computer to a hacker or record activity. They can also be used to delete files or even view the contents of your screen.

They can be used to record keystrokes with the aim of capturing User ID's and passwords which are then passed on to the person controlling the Trojan. Many Trojans can be detected and removed using up to date anti-virus software and there are also a number of specialist software programs that claim to detect and remove Trojans. Advice on Trojans and the software tools is available at www.anti-trojan.net

Spyware

A type of Trojan that is placed on your computer to secretly gather information about the user, and their browsing habits which is then passed on to advertisers or other interested parties. These programs are often installed without the user's consent as a result of visiting a website or through clicking on an option in a deceptive pop-up window.

Spyware can also be carried in viruses or installed alongside other free software downloaded from the internet.

You should read the licence agreements for such software very carefully before you agree to install it. Spyware can slow down your computer, alter your homepage, produce lots of adverts or links to websites and even include keystroke loggers to record details such as passwords and user names.

There are a number of free software tools and commercial products that claim to be able to remove Spyware from your computer.

These should be regularly updated with the latest definition files from the vendor. Two such free products are Ad-aware and Spybot, which are available at www.lavasoft.com & www.safer-networking.org

Stay Safe Online

Check the security of e-Commerce sites

Be aware that **spoof** (fake or fraudulent) sites do exist. Never go to our website via a link in an e-mail, only ever visit the website by typing the address **theAA.com** into your browser.

Secure website addresses usually start with the letters **https:** and display a padlock icon in the bottom section of your Internet browser. While these are good indicators that you are visiting a genuine site there have been cases where criminals have been able to recreate these features on their spoof sites.

As a result, it can be risky to rely entirely on the padlock icon. If you double click the icon a box will appear which contains details of the site owners and helps you to establish whether it is genuine.

Useful Websites

www.antiphishing.org

www.anti-trojan.net

www.apple.com

www.banksafeonline.org.uk

www.firewallguide.com

www.grc.com

www.lavasoft.com

www.microsoft.com

www.safer-networking.org

www.symantec.com/Norton/internet-security

www.virusbtn.com

Useful Contact

abuse@birminghammidshires.co.uk



Bank Safe Online

For more advice and a step by step guide to staying safe online visit www.banksafeonline.org.uk a website launched by APACS the UK payment association working on behalf of the banking industry.

Where we provide links to another website not under our control, we accept no liability for the content of, or your use of, that other site. Where we provide links to another website, we neither guarantee the accuracy of the content of that website, nor do we necessarily endorse or approve of that content. We cannot guarantee that you will be able to access the other websites at any time.

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 Safari (for Macs).

Cookies

Small pieces of information which are placed onto your computers 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 e-mail 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 e-mail scam which tries to get you to provide your personal sign-in details, so that fraudsters can gain access to your accounts. Remember, AA Savings will never ask you to confirm your secure information in an e-mail.

Spam

Unwanted e-mails, usually offering dubious products and services. Various types of anti-spam software are available, but the first line of defence may be your own Internet Service Provider - many offer spam-filtering 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're on a genuine online banking site, and not a 'spoof' website.

Spyware

Spyware is software, usually installed without your consent, that 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.

This information is also available on request in large print, Braille or audio. Customers can also contact us by using Text Relay.

PO Box 81, Pendeford Business Park, Wobaston Road, Wolverhampton WV9 5HZ.

Calls may be monitored and recorded for security and training purposes. Lines are open Monday to Saturday 8am-8pm.

The deposit taker for AA Savings Accounts is Birmingham Midshires, a division of Bank of Scotland plc, which is authorised for accepting deposits by the Financial Services Authority. It is entered in the FSA's Register and its Register Number is 169628. Registered office: The Mound, Edinburgh EH1 1YZ. (Registered in Scotland No. SC327000).