



LloydsLink online

Focusing on security



Introduction

Banking is not so different today to the way that business leaders were accustomed to twenty years ago. Managing your cash flow, optimising the return on your investments, paying suppliers and initiating trade transactions are still the principal activities of the modern treasurer as you seek to achieve efficiencies in your organisation's financial supply chain.

But the Internet has changed the way these transactions are handled.

Viewing your statements and your cash balances can now be done at any time of the day and anywhere you choose. The flexibility that this entails can be liberating, freeing up your time to concentrate on what matters most – running your business.

The downside has been the growth of security related threats, such as identity theft, phishing attacks, hacking and online fraud – which is why we all need to **focus on security**.

This paper provides an overview of our Internet banking service – LloydsLink online – it explores the security measures we already have in place as well as some potential future developments. It also provides some handy hints and tips about protecting your organisation and your computer while you are online.

Identity and Access Management

We recognise the importance of security to our customers and while the Internet has enabled us to deliver innovative services, it has also focussed our attention on ensuring that access to those services is highly secure.

Secure servers

Our LloydsLink online services are run on secure computer servers which are continuously monitored. By using a range of technologies, e.g. firewalls and intrusion detection, we protect the security of both our customers and our systems. We use the latest security and virus detection applications and our systems are regularly tested by independent experts to ensure that we continue to protect our customers.

Secure connections

Our LloydsLink online services use Secure Sockets Layer (SSL) protocol, 128-bit encryption technology and Public Key Infrastructure (PKI) certificates, which are recognised industry standards, to protect the security of your online session.

You can check that you have a secure connection in two simple ways:

- Check that the web address starts with https – the 's' stands for secure.
- Check that the padlock symbol, in the locked position, appears in the bottom right-hand corner of your screen.

If you still have suspicions about a website that has all the appearances of being secure, even down to the 'https' in the browser address and the locked padlock icon, you can check the site certificate.

Sites that are serious about security always show a valid site certificate. Sometimes fraudsters try to duplicate these certificates but there are simple ways to check their validity. The Internet authorities issue site certificates to verify who operates a particular website, and whether it is secure or not.

For information on how to check the validity of a certificate, visit:

www.lloydstsb.com/security/site_certificates.asp

When accessing our services and making transactions all data is transmitted securely using encryption technology, enabling you to bank with confidence. Additionally, we have internal security controls in place to ensure privacy, integrity and authentication of your data as it is transmitted through our systems.

Secure access

While we have put in place the checks and firewalls to secure our systems, it is down to you to decide who has access. You can offer access to everyone who needs it and user permissions can be configured to suit your requirements.

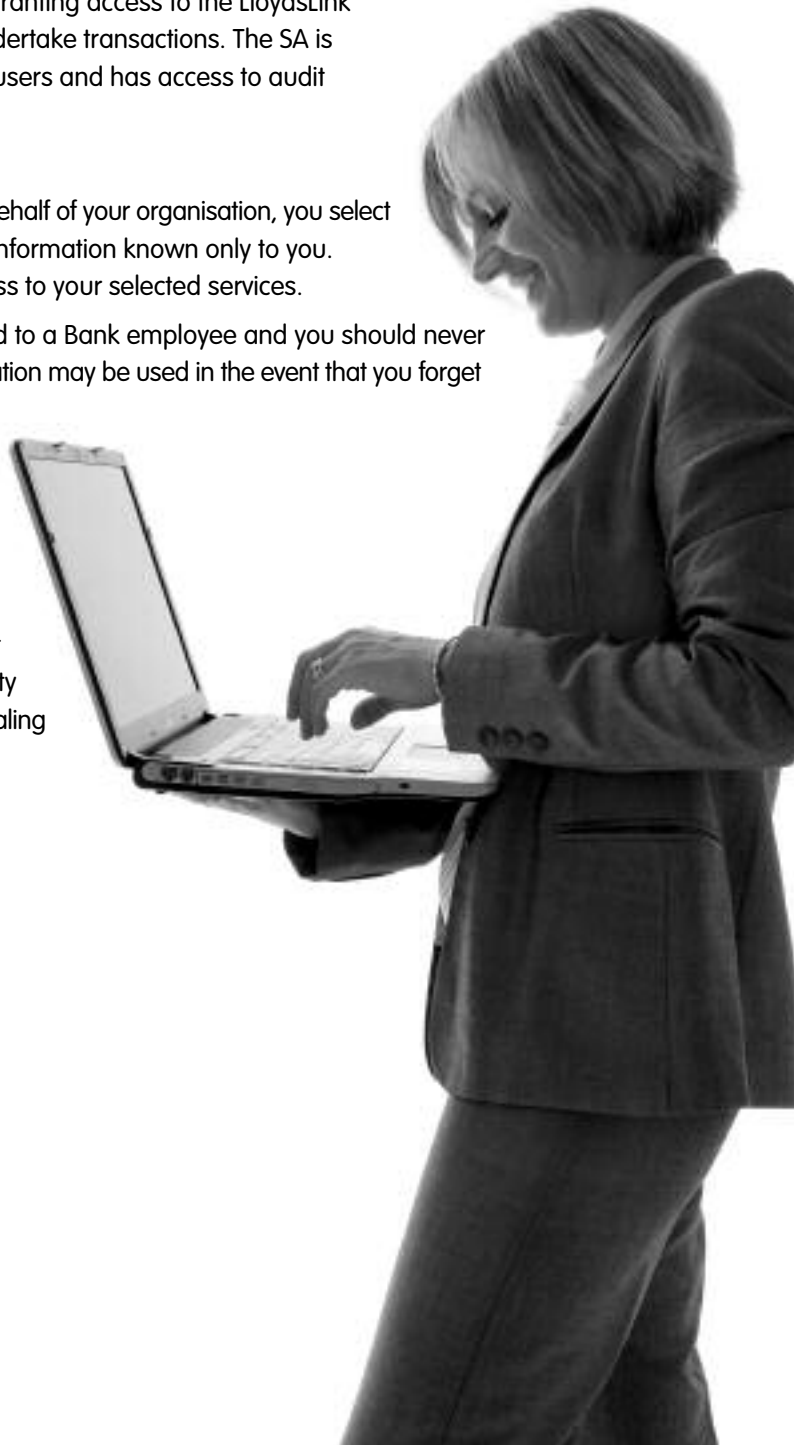
Subscription to a service begins with the appointment of a Service Administrator (SA) who, by authority of company signatories, has control in granting access to the LloydsLink online services and giving permission to users to undertake transactions. The SA is given a number of tools to help them manage their users and has access to audit logs that support this role.

Unique username and passwords

When you subscribe to one of our online services on behalf of your organisation, you select a username and password and record memorable information known only to you. The username and password are used to gain access to your selected services.

We will never ask you to reveal your whole password to a Bank employee and you should never disclose it to any third party. The memorable information may be used in the event that you forget a password or as part of a means to identify you.

Your user name and password are securely maintained within our Identity and Access Management system which is the entrance to our LloydsLink online services. This forms part of our security infrastructure which means that only authorised users can gain access. The Payment service within LloydsLink online has additional security controls and this is covered in the following section dealing with transaction authorisation.



Transaction authorisation

It is recognised that for certain transactions, additional security is required. In addition to the controls previously mentioned, we have developed an additional layer of security to certify that a transaction originated from you is authentic and has been 'signed' by an authorised member of your staff.

Smart Card and reader

Our online Payments service requires that any user who will be responsible for 'signing' transactions is issued with an Authenticator Smart Card and reader, as per the illustration below.

Features

- Pocket-sized for ease of use and maximum flexibility.
- Not physically connected to your PC – wherever you are, so long as you have secure access to the Internet, you can approve payments.
- Uses state-of-the-art encryption technology.
- Is PIN protected for additional security.
- Simple and easy to use with support documentation available.
- An accessible version of the card and reader for customers with disabilities is available (see below for more information).

The Smart Card and reader is used to produce a code which is input into our Payments service as a response to a 'challenge' code that has been generated by our systems. Successful validation of the code by our authentication system will mean that the payment has been electronically 'signed' by you and can be submitted for processing.



Accessible Authentication Device

We are committed to implementing services that meet the needs of all of our customers, regardless of their physical abilities. That's why we take accessibility seriously and work closely with professional organisations to ensure that our products and services meet or exceed recognised web accessibility guidelines such as those set out by the World Wide Web Consortium (W3C) and the Web Accessibility Initiative (WAI).

To enable all of our customers to be able to make an online payment and retain the additional layers of security required, we have developed an alternative version of our Authenticator Smart Card and reader. The solution enables a user to generate authentication codes on screen and read them back with assistive software such as a screen reader or magnifier.

For more information on accessibility and how you can make best use of the related features within your internet browser, visit: www.lloydstsbcorporatemarkets.com/accessibility.asp

Protecting yourself

We've developed LloydsLink online services to deliver high levels of security, however there are additional steps that you and your colleagues can take to increase your protection.

Completing online application forms

When completing our online application forms, do not leave the screen idle for more than 20 minutes as the registration process will end automatically and any entered information will be lost. You should also make sure that no-one else can access your computer during the online registration process as this could lead to your personal information being known to other people.

Passwords

Choose robust passwords (e.g. alphanumeric and mixed content) and change them regularly; avoid obvious passwords (e.g. names of family members, pets and favourite musician) and do not tell anyone else your passwords. You should not write a password down and if you think someone knows your password, go online and change it immediately.

Online session

When you have finished your session, make sure you log off and disconnect from the Internet. This will prevent the viewing of previous pages of your online session via your computer.

Fraudulent emails

If you receive an email that appears to be from Lloyds TSB that you suspect is fraudulent, do not click on any link contained within the email or provide any Internet banking or telephone banking log on details.

While we may email you from time to time, we will never ask for your security details. If you suspect you have received a fraudulent email claiming to be from us, please forward it to us for investigation at emailscams@lloydstsb.co.uk and then delete it immediately.

This information will be used to help reduce online fraud.

If you think that a fraudster already has your Internet banking details, or that someone other than you has accessed your account online, call us on **0870 900 2070** (+44 **0870 900 2070** from overseas). Lines are available Monday-Friday 9am-5pm except bank holidays.

Outside these hours, please call us on **0845 3000 116** (+44 **20 7649 9437** from overseas). Lines are available Monday-Friday 7am-10pm and Saturday/Sunday 8am-6pm except bank holidays.

Protecting your computer

In addition to protecting yourself, there are a number of steps you can take to protect your computer, including the following:

Keep your software up-to-date

Occasionally publishers discover vulnerabilities in their products and issue 'patches' to protect against any security threats. It is important that you regularly visit the website of the company which produces your operating system (e.g. Windows XP) and browser (e.g. Internet Explorer) to check for any patches or updates they may have issued.

If you're using Microsoft software, you can do this by visiting their website:

www.microsoft.com/security

If you are a Mac user, you can visit their website:

www.apple.com/uk/support

Protect against viruses

Use anti-virus software and ensure that it's kept up-to-date – this should protect your computer against the latest viruses. Popular anti-virus products include: ZoneAlarm Internet Security Suite from Zone Labs, McAfee Virus Scan, Norton Anti-Virus, or Sophos Anti-Virus. You can type any of these names into a search engine and go to their websites for further information.

Never download software if you are unsure of the source – this includes websites which prompt you to click 'yes' or 'OK' to run a program or install a browser plug-in.

Be wary of unexpected or suspicious-looking e-mails from unknown sources. E-mails are a common way to spread harmful codes or to trick you into revealing your Internet banking information.

Use up-to-date anti-spyware software to protect against programs that fraudsters can use to collect information about your Internet usage. Popular anti-spyware software such as AdAware or Spybot's Search and Destroy can help to protect your computer. You can type any of these names into a search engine and go to their websites for further information.

Use a firewall

You can get further protection against harmful codes by using firewall software that prevents unauthorised access to your computer when you are on the Internet. Popular firewall software includes: ZoneAlarm Internet Security Suite from Zone Labs, McAfee Internet Security Suite, or Norton Internet Security. Type any of these names into a search engine and go to their websites for further information.

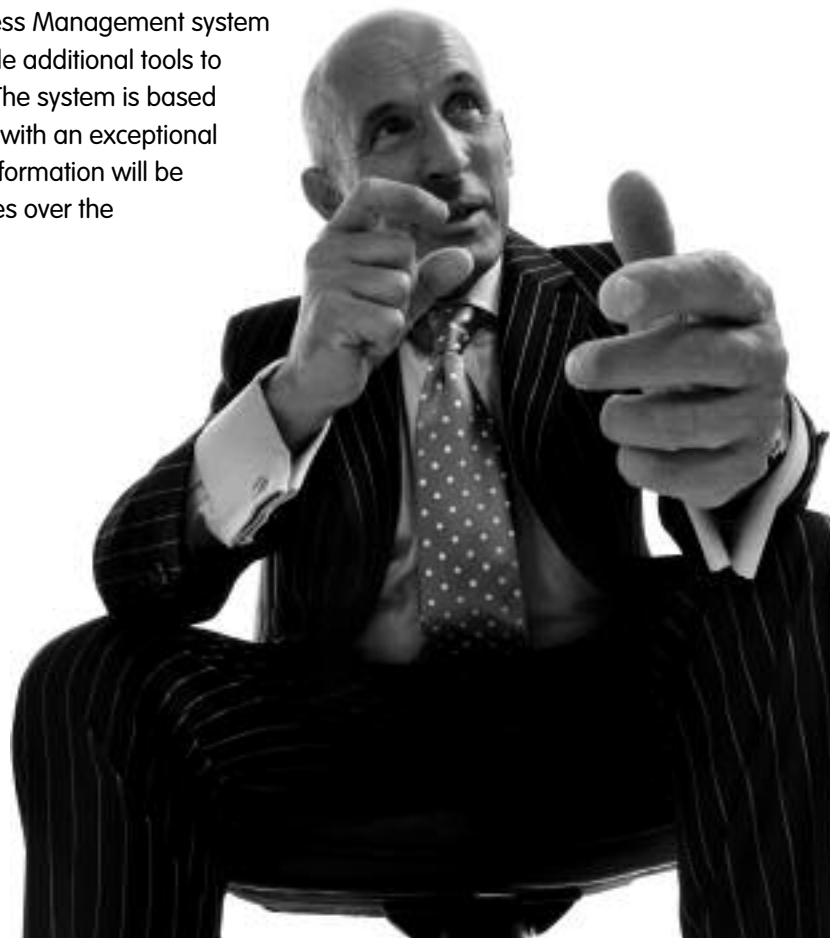
The Lloyds TSB BankSecure programme is aimed at providing you with information on how to protect yourself and your computer. This includes a free security scan and a discount on security software. For more information on this programme, please visit: www.lloydstsb.com/security

Future developments

As part of our commitment to providing you with a secure service, we are continually monitoring the evolving Identity and Access Management arena. We are not only looking to enhance our existing security services, but also to determine the most effective way to continue to meet your needs.

Identity and Access Management system upgrade

We are currently enhancing our Identity and Access Management system to improve the registration experience and provide additional tools to enable customers to better manage their users. The system is based on market leading technology which provides us with an exceptional platform to enhance our service offering. More information will be provided to customers who use our online services over the coming months.



APACS and Industry Groups

Lloyds TSB is a member of APACS and other key industry bodies and is actively engaged in developing new technologies and schemes to both protect our customers and improve the user experience.

Identity theft is a major concern and, as a member of the APACS Electronic Commerce Group and the eFraud sub-committee, we are working closely with the police and government bodies to find appropriate solutions. We also participate in the Home Office Identity Fraud Committee which includes representation from the following areas:

- APACS, British Bankers' Association and the Financial Services Authority
- Association of Chief Police Officers
- CIFAS, the UK's Fraud Prevention Service
- Department for Constitutional Affairs
- Department of Work and Pensions/Jobcentre Plus
- Driver and Vehicle Licensing Agency
- Finance and Leasing Association
- HM Revenue & Customs, Home Office and Identity & Passport Service
- Telecommunications UK Fraud Forum.

If you would like further information on anything covered in this paper, please contact me:

Ivan Hilton
Identity and Access Management
Lloyds TSB Corporate Markets
Tel: (+44) 207 463 1086
E-mail: Ivan.hilton@lloydstsb.co.uk

www.lloydstsb.com/corporatemarkets

Please contact your relationship manager if you'd like this in Braille, large print or on audio tape.

We accept calls made through RNID Typetalk.

Lloyds TSB Corporate Markets is a trading name of Lloyds TSB Bank plc and Lloyds TSB Scotland plc.

Lloyds TSB Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065.

Lloyds TSB Scotland plc. Registered Office: Henry Duncan House, 120 George Street, Edinburgh EH2 4LH. Registered in Scotland no. 95237.

Authorised and regulated by the Financial Services Authority and signatories to the Banking Codes.

Issue date: March 2007.

