COMMERCIAL BANKING

STRONGER ONLINE SECURITY

Enhanced online banking without compromise

Manage your business banking efficiently and securely

Internet banking has given business leaders and treasurers greater control of financial transactions, at the same time liberating you to do your banking where and when it suits you. But it has also seen a corresponding rise in security threats such as identity theft, phishing, hacking and online fraud. Criminals continue developing new ways to breach the security of organisations and individuals.

At Lloyds Bank, we're committed to protecting you and your business. Our internet banking service, LloydsLink online, offers you enhanced accessibility, flexibility and control, without compromising your security. This brochure explains;

1. The measures we have in place to ensure your Internet banking is secure;
2. Additional security measures for crucial transactions;
3. What you can do to help us keep your online banking protected;
4. How you can keep your terminal safe; and
5. Ways we work to protect you from new threats in the future.

Confidence that your Internet banking is secure

Secure connections

Our LloydsLink online services use Secure Sockets Layer (SSL) protocol and 128-bit encryption technology, 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.

Site certificates are issued by the internet authorities to verify who operates a particular website, and whether it is secure or not. 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.

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.

LLOYDS BANK

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 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 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 password

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 username 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.

Additional security for crucial transactions

Transaction authorisation

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.

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.
- 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.

We never request a Challenge and Response code from you either at login or over the phone or by email.

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 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 the best use of the related features within your internet browser, visit **lloydsbankcommercial.com/accessibility** or speak to your relationship team.

Protecting yourself

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 Bank 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@lloydsbanking.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 **0345 900 2070** (**+44 1264 369835** from overseas). Lines are open Monday to Friday 7.30am–6pm except Bank Holidays.

Outside these hours, please call us on **0345 3000 116** (**+44 20 7649 9437** from overseas).

Security

We'll never email you asking for your security details. If you suspect you have received a fraudulent email claiming to be from us, notify us immediately.

Keeping your terminal secure

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**

Protection

Use the latest anti-virus software to protect your computer against viruses

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 and 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 emails from unknown sources. Emails 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.

Keeping you protected from new threats

As criminals seek to develop new ways to compromise security, we're continually working to make sure you stay protected. Here are some of the plans we have in place to protect you into the future.

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 Bank is a member of 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 so 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:

- Association of Chief Police Officers
- British Bankers' Association and the Financial Conduct Authority
- 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

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures for businesses with an annual turnover of up to £25m are published at **lloydsbank.com/business/contactus** and for businesses with an annual turnover of £25m or more they can be found at **lloydsbankcommercial.com/contactus**

Call 0345 900 2070

Lines are open Monday to Friday
7.30am–6pm except Bank Holidays.

Visit lloydsbank.com/business

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use Text Relay (previously Typetalk).

Important information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service. Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065. Telephone: 020 7626 1500.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 119278.

Lloyds Bank International Limited trading as Lloyds Bank and Lloyds Bank Commercial Banking. Registered Office and principal place of business: PO Box 160, 25 New Street, St. Helier, Jersey JE4 8RG. Registered in Jersey, number 4029. Regulated by the Jersey Financial Services Commission. We abide by the Jersey Code of Practice for Consumer Lending.

The Isle of Man branch of Lloyds Bank International Limited of PO Box 111, Peveril Buildings, Peveril Square, Douglas, Isle of Man IM99 1JJ is licensed by the Isle of Man Financial Services Authority to conduct deposit-taking and investment business and is also registered as an insurance intermediary in respect of general business.

The Guernsey branch of Lloyds Bank International Limited is licensed to conduct banking, investment and insurance intermediary business by the Guernsey Financial Services Commission under the Banking Supervision (Bailiwick of Guernsey) Law 1994, the Protection of Investors (Bailiwick of Guernsey) Law 1987 and the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law 2002.

Eligible deposits with us are protected by the Financial Services Compensation Scheme (FSCS). We are covered by the Financial Ombudsman Service (FOS). Please note that due to FSCS and FOS eligibility criteria not all business customers will be covered.