

# LLL@Home Security



Finance  
with a  
mission

## **By using these tips on security, you will enjoy safer and more secure LLL@Home services.**

This document should be read in addition to the terms and conditions of LLL@Home which are available on the LLL website each time you log in. The information below is to help protect your personal information and to make you aware of how you can meet your responsibilities and comply with the terms and conditions.

## **Login ID/ Access Code Security**

One of your most important responsibilities is to keep your Login ID and Access Code (password) secure. **These details are not to be shared.** They have as much value as your signature.

When you receive the initial Access Code from us, you should immediately login to LLL@Home and change it to one of your choice. Try to memorise this Access Code and do not record it. Changing your Access Code regularly is encouraged.

### **Elements of a good Access Code**

Generally, people choose and use poor Access Codes because they're easy to remember. A good Access Code should be obscure to all but the owner of the account.

The best Access Code has these characteristics:

- It can be remembered by the authorised user.
- It can be typed easily and quickly.
- It won't easily be spotted by a 'shoulder surfer'.
- It is complex enough to withstand multiple guessing attempts.
- It has upper and lowercase letters.
- It has numerals and/or other non-letter characters.

## **Access Code pitfalls**

Choosing a bad Access Code can be easily done and can therefore make the hacker's job easy. Here are some methods to avoid as these are NOT a reasonable attempt to disguise an Access Code.

- Using the initial Access Code in reverse order.
- Using the same Access Code for multiple areas used for gaining access (eg ATM, internet banking etc).
- Writing your Access Code down.
- Saving your Access Code on your computer or allowing your computer to remember your Access Codes/ passwords.
- Choosing an Access Code that has obvious reference to you e.g. date of birth, recognisable part of your name, address, phone number etc. Even using family member's details as the Access Code can be an obvious guess for a hacker.

If you suspect that someone may have become aware of your Login ID and/ or Access Code, you should change it immediately. If you are constantly being blocked out of LLL@Home, it may be that a hacker is attempting to gain access. Contact us if you require assistance in changing your details, if you are being blocked out, or if you have forgotten your details.

## **The Padlock**

Whenever you enter a 'secure' internet site such as LLL@Home, you should always check to see a locked padlock symbol at the top or bottom right hand corner of the browser. All data transferred between the computer and the LLL is encrypted with 128 bit encryption, to ensure that if this data is intercepted, it cannot be deciphered. All recent web browsers incorporate this level of encryption, and so it is important to ensure that the browser you are using is one that the LLL recommends.

175 Archer Street  
Reply Paid 45  
North Adelaide  
South Australia 5006

Tel 08 8360 7200  
Fax 08 8267 1722

lll@lll.org.au  
www.lll.org.au

ABN 25 044 678 441

## Emails

The LLL does not send any unsolicited emails in relation to LLL@Home. You should never provide any financial or login/Access Code details in response to an unsolicited email request. The intention of the hacker is to be able to obtain these details directly from you so that they can then login and perform transactions on your account. Hoax emails can lead you to a false website that can look genuine.

## Bookmarking

Bookmark the LLL@Home login page using the Favourites/Bookmark option in your browser, and use this bookmark when logging into LLL@Home. This will ensure that you are always going to the correct website.

## Browsers

Always ensure that you have the latest version of your browser installed, together with any patches that are available. New discoveries are always being made by hackers on how they can infiltrate browser security, and so patches are required to ensure that you are not vulnerable in any web browsing. The LLL recommends using the latest version of either Microsoft Internet Explorer or Mozilla Firefox.

## Security Software

### Virus Protection

Ensure that you have virus checking software from a reputable company. Before logging into LLL@Home, check to make sure that the virus checker is up to date. This will reduce the risk of you obtaining a virus on your computer that may allow a hacker to do damage and put your funds at risk.

### Spyware Protection

Spyware monitors user activity on the internet and transmits that information to someone else without you knowing it. Spyware can also gather information about email addresses and even passwords and credit card numbers.

To avoid such spyware, choose a reputable internet security package that can secure your computer from spyware.

### Firewall

Firewall software and/or hardware can be used to prevent hackers from gaining access to your computer via the internet. You authorise the internet traffic that is allowed to pass to and from your computer. This can add further security to your computer, and is often already present within a business network or as part of an internet security software package.

### Not using a known secure computer?

Avoid using computers in public places such as internet cafes, to login to LLL@Home. Not only can someone look over your shoulder, but you do not know how secure the computer is on the internet. Many of these computers contain viruses and spyware, and should not be used for internet banking purposes.

## Logging out

When logged in to LLL@Home you should never leave your computer unattended. The 'Logout' button in the top right-hand corner of the page should always be used when you have completed your LLL@Home session. This will ensure that you are disconnected from LLL@Home and prevent others from accessing your private information. If you do forget to logout, LLL@Home will automatically do so after 10 minutes for your protection.

## Checking your account

Always check your account balance and transactions regularly to ensure there are no unauthorised transactions on your account. Call the LLL immediately if you find an unrecognisable transaction on your account, whether that is a deposit or a withdrawal.

Every time you login, the welcome page displays your last login date and time. It is always important to be aware of this so that you can confirm it.

## What the LLL does to protect your funds

We take security and privacy seriously. We provide a unique Login ID and Access Code to you and you only. We use advanced internet security which includes firewall technology and encryption, to ensure that account and transaction information is secure.

LLL@Home is a 'secure' site which uses 128-bit encryption for all information transmitted between your computer and LLL@Home. This ensures that if this data is intercepted, it cannot be deciphered by an unauthorised user. The padlock symbol appearing in your browser shows that you are logged into a 'secure' site, and that all data being transmitted is being encrypted.

The LLL will always ensure that your funds are secure, and will continue to introduce further initiatives to secure your funds as they become available. We trust that this document will help you to understand how you can ensure that your funds are protected when you use LLL@Home.

## LLL@Home Security Options

LLL@Home provides an additional security option which is used in conjunction with your Login ID and Access Code when logging in. You have the option of having a 'One Time Password' sent to your mobile phone in an SMS message, or having your own Security Token which self-generates a 'One Time Password'.

These security options are market leading protection tools, and together with your up-to-date internet security software, are an effective way to combat increasing fraud and identity theft. The LLL is pleased to offer these security options free of charge to our LLL@Home customers.

You can self register for one or both of these options in LLL@Home under the 'Other' menu and by selecting the 'Security Options' tab. Registering for both enables you to choose which method you would like to use each time you login to LLL@Home.