Security

The security of our website and the security of our website users is taken very seriously at Link Market Services Hong Kong (Pty) Limited ("Link").

For site security purposes and to ensure that this web service remains available to all users, the Link website employs software programs that monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Anyone using this website expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, such evidence may be provided to appropriate law enforcement officials.

Unauthorized attempts to upload or change information on Link's servers are strictly prohibited and may be punishable by the laws of the applicable jurisdiction, including the legislation governing computer fraud.

Below are some tips for helping you to create a safer and more secure online environment and an outline of how Link helps to protect you online.

Personal Security

What can you do to protect yourself online?

1. Be conscious of phishing emails

Phishing is a criminal activity which uses computer technology such as email or instant messaging to attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Online banking is frequently targeted by phishers, along with companies with website that are transactional in nature and require secure access. Phishing, through a fake email for example, will typically request that users give out personal details either by return email or by accessing a website.

These emails may look like they came from Link, but in fact have not, and clicking on the link inside the email may take you to a fake website or install malicious software onto your computer.

Be careful of emails claiming to originate from Link. If you wish to report a suspicious Link email, please contact us.

Most modern browsers have phishing filters and other tools to help you manage such threats and we encourage enabling these filters for a more secure browsing experience.

- Visit Google's Phishing and Malware Detection page.
- Visit Microsoft's SmartScreen Filter page.
- Visit Mozilla's Phishing and Malware Protection page.

2. Avoid clicking on links or attachments in emails from unknown senders

To help protect yourself against phishing and other threats, follow these guidelines:

- If you don't know who sent you an email, don't click on any links or attachments in the email.
- You can check the authenticity of the return email address by selecting ‘Reply' and looking at the address in the ‘To' field to ascertain if the email address matches the senders address in your inbox.
- Don't provide any login details or personal information to anyone in an email.
- Always access Link by typing www.linkmarketservices.hk into a new browser window (or use your favourites or bookmarks menu).

Link will never send you an email instructing you to follow a link to access our website. We will also never ask for your login details or any personal information via email.

3. Ensure you have anti-virus software installed

Installing and maintaining anti-virus software to protect your computer against malicious software is essential. You should regularly scan your computer for viruses and ensure that the virus definitions the anti-virus software uses are keep up to date.

There are numerous commercial and free-ware anti-virus software packages available and although many operating systems now include a suite of anti-virus software built in, it is still recommended to use a third party solution. A good anti-virus software package should, at minimum, include the following features;

- Rootkit detection
- Real-time protection
- Heuristics
- Firewall
- Signature-based detection

4. Have a personal software or hardware firewall installed

Running a personal firewall on your computer to create a security barrier between your computer and the Internet is another essential tool you should consider for your personal security arsenal when using the internet. A firewall's basic task is to regulate the flow of traffic between computer networks of different trust levels. If you are using Windows XP or Vista, the "Windows Firewall" is built in and should be enabled unless you use a separate third-party firewall.

5. Maintain your computer software

Computer operating systems require regular updates to remain secure. Software manufacturers such as Microsoft release regular security upgrades to their operating systems called 'patches' to address new security vulnerabilities. These are found on the manufacturer's website or delivered automatically as with the Windows operating system, through the "Automatic Updates" feature.

Ensure that you are also running the latest version of your web browser to take advantage of new security 'patches'.

6. Use anti-spyware software

Spyware is installed on your computer by stealth and can transmit information (including any personal details stored on your computer) to third-parties without your knowledge. To avoid downloading spyware, don't open unknown email attachments, click on links in emails or visit dubious websites.

As with anti-virus software, you should also regularly scan your computer using anti-spyware software. Once again, Microsoft, Apple and Linux distributions all provide suitable anti-spyware software for their operating systems and there are many commercial or free software packages available.

These include;

- Microsoft Windows Defender
- Ad-Aware from Lavasoft
- Search and Destroy from Spybot

7. Avoid public or shared computers

When accessing the Link website, avoid using public or shared computers to do so. Internet Cafes and libraries are extremely susceptible to malware. If you do access our website at one of these places, you may like to change your password as soon as possible afterwards.

8. Keep your password protected

Your username and password are your keys to our website. Please keep them safe.

- Choose an password that is difficult to guess.
- Don't share your password with anyone else.
- Don't provide your password to another website for any purpose.
- Don't use the same password for all of your web browser activities and/or social media sites.
- Change your password regularly.

9. Other ways you can protect yourself online

Use commonsense when using computers.

- Don't leave your computer unattended while logged in to Link - Remember to logout as soon as you have finished.
- Check your online details regularly for unauthorised transactions or changes.

10. Will Link call me?

There are some occasions where we will need to call you.

- On occasion, we may be required to call you to discuss your account details or to answer a question you may have asked. For security reasons, we may need to verify that we are speaking to the correct customer by asking you some random security questions.
- If you do not feel comfortable or have any concerns about the legitimacy of the call, please call us back.
- Remember that we will never phone you to ask you for your password.

11. Research preventative security measures on the internet

There are many websites available for you to find out more about online protection. Some examples are:

- The Protect Your Financial Identity website provides information for the public about how you can protect your financial identity in everyday life and minimise the damage if a problem occurs. It has been developed by the Australian Banker's Association (ABA), the Australian High Tech Crime Centre (AHTCC) and the Australian Securities & Investments Commission (ASIC) to help reduce the incidence of identity theft.
- Stay Smart Online has been provided by the Australian Government to help home computer users and small businesses to be safe when online.

How Link helps to protect you online?

1. Protection of your information

Link takes the security of your information very seriously. We use proven technology and physical security measures to ensure a high level of protection for your information.

We continually monitor trends and work with industry experts and authorities to ensure that we provide the highest level of protection available.

2. Secure Socket Layer encryption

Our website uses 256-bit SSL (Secure Sockets Layer) cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, instant messaging and other data transfers to ensure that others cannot intercept and use information communicated between your computer and our website.

3. Session timeout

Once you have logged in to Link, through either a holding validation or by using your username and password, your session will automatically timeout after 15 minutes of inactivity and you will be logged out. This is to guard against the possibility of you forgetting to log out when accessing our website and leaving your computer unattended where others may attempt to gather or change personal details.

4. Account lockout

We log and monitor all failed login attempts, your account login may be permanently disabled or locked if we detect a security threat on your account. You will need to contact us to have your account unlocked.

5. Communication to users

We will communicate to you when we become aware of new threats to online services by updating this security page, the home page and occasionally through non-electronic mail should the threat warrant this action. If you have any concerns about the security of our online service, please contact us.