安全性

Link Market Services Hong Kong（Pty）Limited（“Link”）非常重視網站及網站用戶的安全性。

為了保障網站的安全性並確保所有用戶都可以使用我們的網上服務，鏈接網站使用監控網絡流量的軟件程式來識別未經授權試圖作出上傳或更改信息，或以其他方式造成損害的情況。

任何使用本網站的人士都明確同意接受此類監控，亦清楚如果監控程式發現可能存在濫用或犯罪活動的證據，則可向有關執法人員提供此類證據。

嚴禁未經授權試圖上傳或更改 Link 服務器上的信息，一經定罪，可受到適用司法轄區的法律，包括管理電腦欺詐的法律處分。

以下提示可幫助您建立更安全穩固的網上環境。我們亦提供了概述，講解 Link 如何幫助保護您的網上安全。

個人安全

您可以如何在網上保護自己？

1. 留意網絡釣魚電郵

網絡釣魚是一種犯罪活動，一般使用電子郵件或即時通訊等電腦技術，並通過在電子通訊中偽裝成可信人士，試圖以欺詐手段獲取敏感信息，如用戶名稱、密碼及信用卡詳細信息。網絡銀行經常成為網絡釣魚者的目標，另外，具備交易功能且需要安全權限的公司網站亦然。網絡釣魚的一個例子，是通過虛假電子郵件要求用戶回復電子郵件或訪問網站來獲取個人詳細信息。

這些電子郵件可能看似來自 Link，但實際上並非如此，而當您點擊電子郵件中的鏈接後，您可能會被帶到虛假網站或在您的電腦中安裝了惡意軟件。

請注意聲稱來自 Link 的電子郵件。如果您想舉報含有可疑 Link 的電子郵件，請與我們聯繫。

大多數現代瀏覽器都有網絡釣魚過濾器及其他工具來幫助您管理這些風險，我們鼓勵您啟用這些過濾器以更安全地進行訪問。

- 訪問谷歌的網絡釣魚及惡意軟件偵查網頁。
- 訪問微軟的 SmartScreen 過濾網頁。
- 訪問 Mozilla 的網絡釣魚及惡意軟件保護網頁。

2. 避免點擊寄件人不明的電郵內的鏈接或附件

請遵循以下準則，以幫助您保護自己免受網絡釣魚及其他威脅影響：

- 如果您不知道電子郵件的寄件人是誰，請不要點擊電子郵件中的任何鏈接或附件。
- 您可以選擇“回覆”並查看“收件人”一欄中的地址來確認回覆電子郵件地址的真實性，以確定電子郵件地址與收件箱中的寄件人地址是否相同。
- 不要在電子郵件中向任何人提供任何登入詳情或個人信息。
- 請確保在新的瀏覽器視窗中輸入 www.linkmarketservices.hk（或使用您的收藏夾或書籤菜單）來訪問 Link。

Link 絕不會向您發送電子郵件來指示您按照鏈接來訪問我們的網站。我們亦絕不會通過電子郵件詢問您的登入詳情或任何個人信息。

3. 請確保您安裝了防毒軟件

安裝及保養防毒軟件十分重要，它們可以保護您的電腦免受惡意軟件攻擊。您應定期掃描電腦中的病毒，並確保防毒軟件使用最新的病毒定義。

市面上有許多商業及免費防毒軟件可供使用，雖然現在許多操作系統都包含一套內置的防毒軟件，但我們仍建議使用額外的防毒軟件一個好的防毒軟件應該包含至少以下功能。

- Rootkit 的檢測
- 實時保護
- 啟發式防毒
- 防火牆
- 特徵檢測

4. 安裝個人軟件或硬件防火牆

在您的電腦上運行個人防火牆可以在您的電腦及互聯網之間建立一道安全屏障。因此，您在使用互聯網時應考慮使用防火牆作另一種重要工具來保障您的個人安全。防火牆的基本功能是控制不同信任程度的電腦網絡之間的流量。如果您使用 Windows XP 或 Vista 的話，您的系統已內置 Windows 防火牆，除非您另外使用第三方的防火牆，否則應啟用該防火牆。

5. 保養您的電腦軟件

電腦操作系統需要定期更新才能保持安全。微軟等軟件製造商會定期就其操作系統進行安全升級，即“修補程式”，以解決新的安全漏洞。這些修補程式可在製造商的網站上找到，或通過 Windows 操作系統的“自動更新”功能自動下載。

另外，請確保使用最新版本的網頁瀏覽器來使用最新的修補程式。

6. 使用防間諜軟件

間諜軟件可以隱藏在您的電腦上，並在您不知情的情況下將信息（包括儲存在您的電腦上的任何個人詳細信息）傳輸給第三方。為避免下載間諜軟件，請不要打開未知的電郵附件、點擊電子郵件中的鏈接或訪問可疑網站。

除了防毒軟件外，您亦應該使用防間諜軟件定期掃描您的電腦。微軟、蘋果及 Linux 均為它們的操作系統提供了合適的防間諜軟件，坊間亦有許多商業或免費軟件可供使用。

包括；

- 微軟 Windows Defender
- Lavasoft 的 Ad-Aware
- Spybot 的 Search and Destroy

7. 避免使用公共或共享電腦

訪問 Link 網站時，請避免使用公共或共享電腦。網吧及圖書館極易受到惡意軟件的侵害。如果您曾在上述地方訪問我們的網站，請盡快更改您的密碼。

8. 保護您的密碼

您的用戶名稱及密碼是登入我們網站的認證工具，請妥善保管。

- 選擇難以猜測的密碼。
- 不要與其他人分享您的密碼。
- 不要為了任何目的將密碼提供給其他網站。
- 不要在所有網頁瀏覽器活動及/或社交媒體網站使用相同的密碼。
- 定期更改密碼。

9. 其他可以在網上保障您自己的方法

使用電腦時請注意使用常識。

- 登錄到 Link 時不要讓電腦無人看管–請謹記在完成後立即登出。
- 定期檢查您的網上詳細信息，以查看是否有未經授權的交易或更改。

10. Link 會向我致電嗎？

在某些情況下，我們需要向您致電。

- 某些情況，我們可能需要向你致電以討論您的賬戶詳情或回答您提出的問題。基於安全理由，我們可能需要向您詢問一些隨機的安全性問題，以驗證我們是否與正確的客戶交談。
- 如果您感到不安或對來電的合法性有任何疑慮，請致電我們。
- 請謹記，我們絕不會向您致電要求您提供密碼。

11. 研究網上的預防性安全措施

有許多網站會提供有關網上保護措施的信息。例如：

- “Protect Your Financial Identity”網站為公眾提供信息，教導如何在日常生活中保護自己的財務身份以及在出現問題時將損害降至最低。它由澳洲銀行家協會(ABA)、澳洲高科技犯罪中心(AHTCC)及澳大利亞證券及投資事務監察委員會（ASIC）開發，旨在幫助減少盜用身份的案件。
- 澳洲政府提供 Stay Smart Online，以幫助家庭電腦用戶及小型企業安全地使用網絡。

Link 如何保護您的網上安全性？

1. 保護您的信息

Link 非常重視您的信息安全性。我們使用經過驗證的科技及物理安全措施來確保高度保護您的信息。

我們不斷監控趨勢，並與行業專家及機構合作，確保我們提供最高級別的保護。

2. 傳輸層安全性協議(SSL)加密

我們的網站使用 256 位 SSL（傳輸層安全性協議）加密協議，為網頁訪問、電子郵件、即時通訊及其他數據傳輸提供安全的互聯網通訊，以確保他人無法攔截及使用您的電腦和我們的網站之間的通訊信息。

3. 閒置超時

當您通過保留驗證或使用您的用戶名稱及密碼登入 Link 時，網站將在閒置 15 分鐘後自動登出。這可防止您在訪問我們的網站時忘記登出，並在您的電腦閒置時，其他人企圖收集或更改您的個人詳細信息。

4. 封鎖帳戶

我們會記錄並監控所有企圖登入但失敗的次數，如果我們檢測到您的帳戶存在安全威脅，您的帳戶可能會被永久禁用或封鎖。您需要與我們聯繫以將您的帳戶解鎖。

5. 與用戶聯絡

當我們發現新的網上服務威脅時，會通過更新此安全頁面、主頁以及偶爾通過非電子郵件（如我們認為有此需要）與您聯絡。如果您對我們的網上服務的安全性有任何疑慮，請與我們聯繫。