互聯網及網上銀行保安

2021 年 1 月

互聯網及網上銀行服務很容易成為騙徒的目標。我們建議閣下採取下列保安措施，以保障您的帳戶及個人資料：

網上銀行

- 避免使用公共電腦或公眾無線區域網絡連結進行網上理財，因為此舉可能會被截取資料。
- 只透過 LGT 網站登入網上銀行賬戶。若閣下使用 LGT 流動網上銀行應用程式，須確保該應用程式是由官方應用程式商店下載。
- 切勿向任何人士，包括 LGT 職員，披露您的用戶 ID、密碼或啟動信函。
- 確保您的登入憑證及裝置安全，防止未經授權人士錯誤使用。

裝置保安

- 在所有裝置（電腦、手提電腦、流動電話、平板電腦等）應使用最新版本的操作系統及瀏覽器。
- 安裝最新的防毒軟件、有效的防火牆和流動硬碟加密等，以減低網絡安全風險。
- 經常鎖定，或在使用完畢後登出您的裝置。

密碼保安

- LGT 網上銀行用戶應該立即更改 LGT 提供的密碼，並銷毀密碼通知書。
- 選擇一個獨特的密碼供網上銀行使用，切勿把該密碼用於其他服務或網站。
- 應設定複雜的密碼（例如由大寫和小寫字母、數字和符號組成），不應包含容易獲取的個人資料，例如：電話號碼、出生日期、姓名的一部份等。
- 應定期更改密碼。

識別網絡釣魚

- 仔細分析電郵，以識破網絡釣魚行為。即使電郵看來由熟悉的寄件人發出，也可能是假冒電郵。釣魚電郵常見的特徵：
- 非個性化的通用問候語，不是以用戶的真實姓名問候；
- 拼寫錯誤或文句不通；
- 要求提供個人資料，例如：信用卡號碼和密碼等；
- 使用緊急字句，意圖使你採取即時行動；
- 不尋常的要求，例如轉賬至不知名的收款人；
- 載有可疑的附件或連結等。
- 保持審慎，若電郵看來可疑，切勿點擊連結, 開啟附件或回覆電郵。

保持警惕

- 只使用安全可靠的無線網絡。
- 為您的家居 Wi-Fi 網絡增設密碼。
- 提防網絡釣魚詐騙電郵：
- 對主動聯絡或突如其來，並聲稱來自 LGT 的聯絡人保持警惕。
- LGT 絕對不會要求閣下透過電話、電郵或短訊披露保密資料，例如您的網上銀行密碼和賬戶資料等。
- LGT 絕對不會透過電話或電郵授權遙距登入閣下的網上銀行賬戶。