



遙距工作的保安貼士



妥善保護你的電腦裝置

- 安裝抗惡意程式碼軟件及個人防火牆
- 確保所有軟件 / 固件已安裝最新的修補程式並已更新
- 啓用保安功能，以防止有人未獲授權接達你的裝置



保護你的網絡

- 避免使用公共 Wi-Fi 網絡
- 使用安全連線（例如虛擬私有網絡（VPN））
- 使用 Wi-Fi 時，應確保使用 WPA2 或 WPA3 加密技術



保護你的帳戶

- 設定嚴謹的密碼及 / 或多重認證
- 切勿與他人分享你的個人帳戶
- 無需使用時，謹記登出遠程接達帳戶



保護你的數據

- 把重要資料備份，並把備份的資料保存在安全的場外地點
- 把敏感資料儲存在儲存裝置或雲端儲存服務時，採用數據加密
- 切勿在社交網站過度分享你的個人資料



提防欺詐訊息

- 切勿點擊可疑電郵 / 網站所載的連結
- 切勿開啓 / 下載來源可疑的電郵附件
- 通過電郵 / 網站提交任何個人 / 敏感資料前應提高警覺



為遙距工作提供足夠支援

- 提醒員工遵守機構的資訊保安指引及政策
- 確保遙距工作的員工充分了解資訊科技支援設施
- 確保事故應變計劃及業務持續運作計劃切合最新情況

