



Anti-Phishing Bot

Privacy by Default 

適用於  Microsoft 365 store  Google workplace

在不同詐騙電郵的情況下，APBot都能以人工智能及網絡追蹤解決8成電郵保安問題。

中小型企業能省下高達3成的技術支援成本。

中小型企業電郵保護方案



共享網釣智能



人工智能網釣偵測



知名品牌保護



一鍵點擊驗證



使用雲端技術，
無需額外安裝軟件

不同情境都能輕鬆處理

情境 1：財務總監 Paul

收到一封來自夏威夷商務活動的電郵邀請，需要進入網站連結查閱，他可以：

哪一個是
正確的決定？



現在我該
怎麼做？

情境 2：會計師 Mary

收到一封來自美國合作伙伴的電郵，其發票要求電匯20萬美元，她可以：



選項 1： 要求PDF檔案減低風險
(可能要15小時後才得到回覆)

選項 2： 請技術支援經理檢查連結是否安全
(金錢及時間成本較高)

選項 1： 聯絡美國合作伙伴確認
(可能要15小時後才得到回覆)

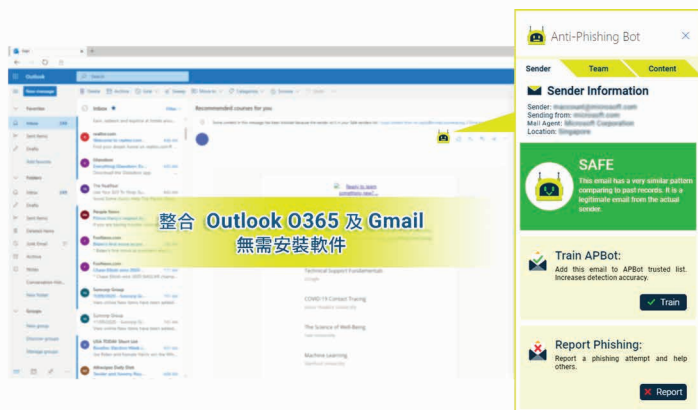
選項 2： 請技術支援經理檢查電郵是否安全
(金錢及時間成本較高)



選項3： 使用Anti-Phishing Bot 即時檢查電郵
(只需一分鐘及0.1美元)

已驗證寄件人資料

- 打開電郵時不用再為發件人的身份而煩惱
- 我們建立了一個擁有超過 1,000 間銀行和香港知名品牌的電郵格式數據庫。若電郵來自已驗證品牌，將會顯示「已驗證」徽標。



- 無需專業培訓
- 用戶能夠自我保護
- 用戶能夠更信賴銀行及金融科技的電郵
- 透過檢舉虛假電郵減少詐騙

社群互助

- 只需一鍵檢舉任何網釣訊息，令他人也能從中受益。

分享

與您的朋友和家人組成一個小組。APBot將使用來自該組的集體情報來處理報告的電子郵件和受信任的發件人信息，以檢測假電子郵件。

保護

當您訓練APBot去分辨和紀錄來自自己知品牌（例如銀行）的寄件人資料時，在您小組內的其他成員也可以從中受益。

抵禦

透過人工智能和數據分析，同一來源的電郵會被檢舉，從而提升網釣偵測率。

內容預覽

- 用戶可以在不公開您的IP地址或電腦資料的情況下查看連結。電郵防網釣BOT可以預先到訪該網站，並提供截圖，令您安心獲取所需的信息。



- 輕鬆查閱電郵內的連結
- 截屏會被收集和顯示