

臺灣區塊鏈新創推出 Email 上鏈工具 ChkSender 防堵商業電郵詐騙

- 臺灣新創團隊利用區塊鏈 釋出相容 Gmail 電子郵件真偽驗證服務 ChkSender

展望 2020 年，AI、Cloud 技術熱度持續發燒，加上 5G 在臺灣即將開通，金融資料大開放和新式數位身分驗證將上路，資安專家也預估今年會是資安威脅大躍進的一年。隨著創新應用爆發，資訊安全作為技術應用發展的前提，除了將重點放在防毒及對抗惡意軟體，國內有業者運用區塊鏈技術確保 email 資料真實性，並開發出可以辨別可疑寄件人的 webmail 擴充功能。

電郵詐騙手段升級 數個字母變化造成上百萬損失

BEC (Business Email Compromise) 是近年最受注目的資安威脅之一，詐騙集團甚至不用接觸到真人，透過一般電子郵件就能讓對方上當，造成鉅額損失。有心人士藉由窺探企業郵件往來，並在產生帳單交易時以相似的 email 帳號寄信，提供假帳戶，一般員工只要稍有不查，就會將帳款匯入假帳戶中，直到真正客戶催款才驚覺受騙。

美國聯邦調查局 (FBI) 統計自 2016 年 6 月至 2019 年 7 月，共有 16 萬多件 BEC 詐騙回報，預估損失總金額高達 260 億美元。2019 年 8 月日本汽車大廠豐田的子公司亦遭到商業郵件變臉詐騙攻擊，估計財務損失可達近 40 億日圓。而台灣至 2019 年九月底止，就接獲 37 起電郵詐騙案件，損失金額達到台幣 4 千多萬元。海內外 BEC 案件層出

不窮，而有了新的 email 驗證工具之後，使用者收信時僅需花費不到 10 秒的時間，就有機會避免平均每案件 15 萬美元的詐騙損失。

臺灣區塊鏈新創團隊瞄準國際市場 自主研發 Email 驗證比對工具

成立不到兩年的臺灣區塊鏈資安應用新創「區塊科技 BlockChain Security」，創辦人黃敬博先前在資安鑑識與數位證據領域耕耘多年，許多企業客戶都遇到過 BEC 案件。他看見 BEC 猖獗的問題，因此引進瑞典區塊鏈底層架構 Postchain，並整合科技法律專家的見解，利用區塊鏈資料不可否認、不可篡改、永久保存等特性，帶領團隊自主研發適用個人、企業機敏往來資料的資安解決方案，並在 2020 年 1 月初搶先釋出 ChkSender 區塊鏈電子郵件真偽驗證工具，鎖定全球 Webmail 使用者提供服務。

專利加持 Email 驗證工具揪出可疑寄件來源 一鍵上區塊鏈存證自保

ChkSender 是瀏覽器擴充功能套件，訴求為不改變使用者習慣的同時，確認寄件者來源與郵件內容未遭竄改，寄件者可存證郵件數位指紋至區塊鏈或是用密碼加密傳送郵件，收件者可驗證郵件來源真實性，並標示出真偽郵件的差異處，來確認該封郵件是否可信，降低 email 詐騙案件發生的機率，而這項技術也正在申請各國國際專利中。

目前 ChkSender 已經在 Google Chrome Web Store 上架開放前 1000 名公開測試者免費使用，Gmail 用戶可以在官網或到 Chrome 線上應用程式商店下載安裝，技術團隊也同步公開徵求使用者蒐集反饋，並祭出抽獎活動鼓勵使用者回報漏洞和使用建議，期許提供更準確有效的工具守護郵件與資訊安全。

官網：<https://chksender.com/>

下載連結：<https://chksender.pse.is/addon>

The top half of the image shows the ChkSender extension page on the Chrome Web Store. The page title is "ChkSender郵件存證與真偽驗證". It features a logo with a checkmark and the text "提供者: Blockchain Security Corp.". Below the logo, it says "★★★★★ 2 | 實用工具 | 25 位使用者". There are tabs for "總覽" (Overview), "評論" (Reviews), "支援" (Support), and "相關項目" (Related Items). A large graphic in the center illustrates a person at a desk with multiple envelopes, with text overlaying it: "一鍵辨別郵件詐騙" (One-click to identify email fraud) and "揪出駭客痕跡，比對原信差異" (Identify the traces of the hacker, compare the original message differences). To the right, there is a login form with fields for "帳號" (Account), "密碼" (Password), and "圖形驗證碼" (CAPTCHA). The CAPTCHA shows the text "SNPHOK". Below the form are links for "忘記密碼?" (Forgot password?) and "註冊帳號" (Register account). The bottom half of the image shows a Gmail inbox. An open email from "service@chksender.com (chksender.com)" contains the text: "Hello!", "Hello!", "Hello!", and "This is ChkSender!". Below the email is a toolbar with various icons for text styling and attachments. At the bottom of the screen, a status bar displays "Google Search Conso." and a link to "您的資源「https://app.chainsecurity.asia/」12月份在 Go...".

Gmail 搜尋郵件 ChkSender BETA 請訪

示範 - emma lu 寄給 我 Hi 黃執...

敬請在這 銀行帳號 汇款金額 謝謝 XXOO合

驗證結果差異
郵件已被篡改

#	原信件	寄件人資訊
主旨	✓	✓
寄件人	emma@chainsecurity.asia	emma@chainsecurity.asia
收件者	✓	✓
郵件內容	✗	✗
附件檔名	✓	✓

將此驗證信件之寄件者加入 黑名單 白名單

ChkSender powered by 區塊科技股份有限公司 © 2019 版權所有

回覆 轉寄

The screenshot shows a Gmail inbox with several unread messages. A ChkSender BETA verification overlay is displayed over an email from 'emma lu'. The overlay title is '驗證結果差異' (Verification Result Difference) with the subtitle '郵件已被篡改' (Email has been tampered with). A table compares the '原信件' (Original Email) and '寄件人資訊' (Sender Information) across five fields: Subject, Sender, Recipient, Body Content, and Attachment Name. Most fields show a green checkmark, except for 'Body Content' which has a red '✗'. At the bottom, there are buttons to 'Blacklist' or 'Whitelist' the sender, and a note that ChkSender is powered by ChainSecurity.