(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201044836 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 16 日

(21)申請案號：099112950 (22)申請日： 中華民國 99 (2010) 年 04 月 23 日
(51)Int. Cl.： *H04L29/06 (2006.01)*
(30)優先權：2009/05/26 美國 12/472,094
(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)
美國
(72)發明人：法席林根岡德西 VAITHILINGAM, GANDHI (US) ；何晟 HO, CHENG (US) ；古瑞亞佩德歐亞倫 GRUIA, PITIGOI-ARON (US) ；文森班 VINCENT, BEN (US)
(74)代理人：蔡坤財；李世章
申請實體審查：無 申請專利範圍項數：20 項 圖式數：7 共 59 頁

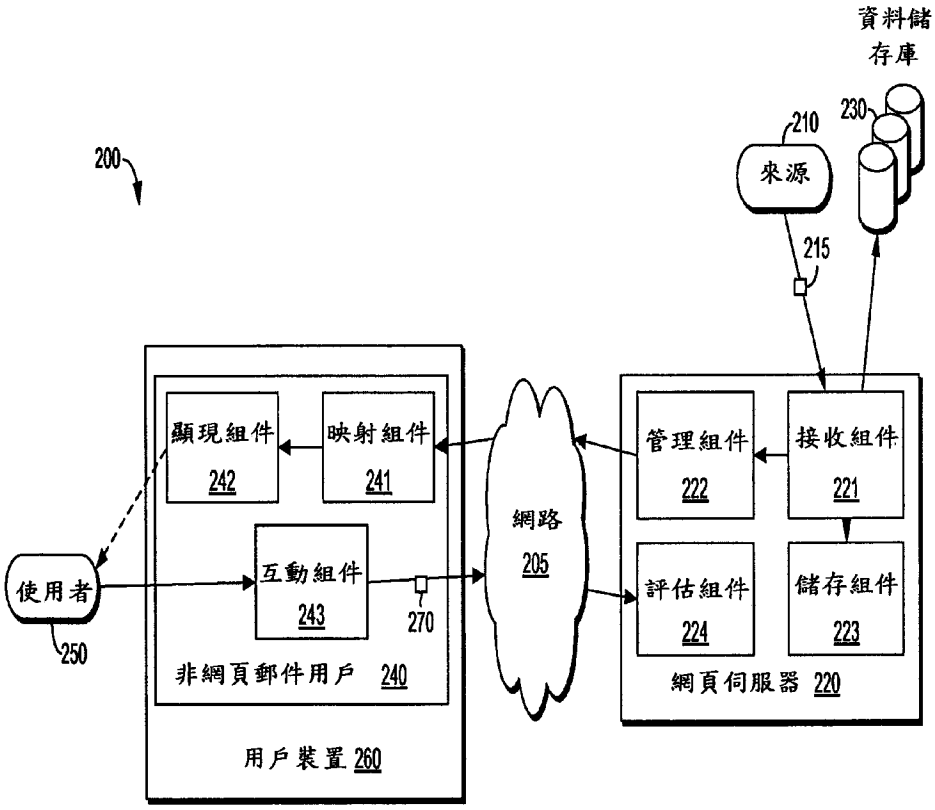
(54)名稱

在非網頁郵件用戶上下文中管理潛在的網路釣魚訊息

MANAGING POTENTIALLY PHISHING MESSAGES IN A NON-WEB MAIL CLIENT CONTEXT

(57)摘要

本發明揭示在識別通訊為潛在網路釣魚電子郵件後，提供用於管理該等數位通訊(例如電子郵件與即時訊息)的處理之電腦可讀取媒體與電腦化方法。服務提供者係用來控制帳戶行為，其被指定給該等通訊之預期的接受者。控制該帳戶行為係說明於顯現使用者介面(User interface， “UI”)顯示屏的非網頁郵件伺服器上下文中，其無法由該服務提供者動態配置。在一種技術方案中，控制行為藉由將這些通訊聚集於分開的文件夾中，警示使用者識別為潛在網路釣魚之通訊的存在。在另一種技術方案中，控制行為藉由以警告訊息取代該等潛在網路釣魚通訊之內容，以便保護該使用者。此警告訊息視需要包括統一資源定位符(Uniform-resource locator， “URL”)，其鏈結至該使用者可觀看該等潛在網路釣魚通訊的原始內容之網頁瀏覽器。



200：系統架構
205：網路
210：來源
215：數位通訊
220：網頁伺服器/裝置
221：接收組件
222：管理組件
223：儲存組件
224：評估組件
230：資料儲存庫
240：非網頁郵件用戶
241：映射組件
242：顯現組件
243：互動組件
250：使用者
260：用戶裝置
270：需求

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201044836 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 16 日

(21)申請案號：099112950 (22)申請日： 中華民國 99 (2010) 年 04 月 23 日
(51)Int. Cl.： *H04L29/06 (2006.01)*
(30)優先權：2009/05/26 美國 12/472,094
(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)
美國
(72)發明人：法席林根岡德西 VAITHILINGAM, GANDHI (US) ；何晟 HO, CHENG (US) ；古瑞亞佩德歐亞倫 GRUIA, PITIGOI-ARON (US) ；文森班 VINCENT, BEN (US)
(74)代理人：蔡坤財；李世章
申請實體審查：無 申請專利範圍項數：20 項 圖式數：7 共 59 頁

(54)名稱

在非網頁郵件用戶上下文中管理潛在的網路釣魚訊息

MANAGING POTENTIALLY PHISHING MESSAGES IN A NON-WEB MAIL CLIENT CONTEXT

(57)摘要

本發明揭示在識別通訊為潛在網路釣魚電子郵件後，提供用於管理該等數位通訊(例如電子郵件與即時訊息)的處理之電腦可讀取媒體與電腦化方法。服務提供者係用來控制帳戶行為，其被指定給該等通訊之預期的接受者。控制該帳戶行為係說明於顯現使用者介面(User interface， “UI”)顯示屏的非網頁郵件伺服器上下文中，其無法由該服務提供者動態配置。在一種技術方案中，控制行為藉由將這些通訊聚集於分開的文件夾中，警示使用者識別為潛在網路釣魚之通訊的存在。在另一種技術方案中，控制行為藉由以警告訊息取代該等潛在網路釣魚通訊之內容，以便保護該使用者。此警告訊息視需要包括統一資源定位符(Uniform-resource locator， “URL”)，其鏈結至該使用者可觀看該等潛在網路釣魚通訊的原始內容之網頁瀏覽器。

六、發明說明：

【發明所屬之技術領域】

本發明係關於在非網頁郵件用戶上下文中，管理潛在網路釣魚訊息。

【先前技術】

存在各種技術讓服務提供者能夠接收與處理來自各種來源的訊息(例如電子郵件、簡訊服務(Short Message Service，“SMS”)訊息等)，且允許使用者觀看並對那些訊息採取行動。有時候，該等來源可能係惡毒的實體，例如犯罪或非法的電腦程式，其傳送訊息給使用者來騙取該使用者對其個人資訊的揭示。透過詐騙訊息導致資訊揭示的此程序，普遍係指稱為網路釣魚。通常，「網路釣魚」(phishing)的特性為藉由在電子通訊中偽裝為可信的實體，試圖取得敏感資訊(例如使用者名稱、密碼、信用卡細節等)的犯罪詐騙程序；因而，引誘無戒備心的使用者提供除此之外受保護的資料。在例子中，網路釣魚的實現，係藉由發送外表與感覺類似於合法電子郵件或即時訊息的電子郵件或即時訊息給使用者，引導該使用者瀏覽假網站(亦即騙人的銀行網站)，且誘惑該使用者在該假網站處輸入私人資訊(例如銀行帳戶登入、使用者

識別、社會安全號碼等)。

服務提供者已採取步驟來識別這些網路釣魚訊息。另外，若該等服務提供者已識別訊息為網路釣魚訊息，則該等服務提供者可試圖減輕該網路釣魚訊息潛在造成之損害。然而，當使用與該服務提供者無關的用戶端應用程式來存取在該使用者帳戶中的訊息時，服務提供者無法提供該使用者適當保護，以免受該網路釣魚訊息的威脅。亦即，由於該用戶端應用程式的大多數要素並非由該服務提供者直接控制，故阻止該服務提供者採用通知該使用者該網路釣魚電子郵件的習知技術。

因此，這些現有技術並非配置來提供使用者適當的保護性措施，以防備網路釣魚訊息。據此，採用程序來限制當自用戶端應用程式或非網頁郵件用戶觀看時，網路釣魚訊息可造成的潛在損害，將增強當在他/她的帳戶中觀看並對訊息採取行動時，該使用者的經驗。

【發明內容】

此「發明內容」係以一簡化型式來做一選擇性觀念之介紹，其在以下的「實施方式」中會進一步加以說明。此「發明內容」並無意於識別出所主張申請標的之關鍵特徵或基本特徵，也並無意於用以限制所主張標的之範疇。

本發明具體實施例通常係關於電腦可讀取媒體與電腦化方法，其在識別數位訊息(例如電子郵件訊息、即時訊息等)為潛在網路釣魚電子郵件後，用於管理它們的處理。在一個示例性具體實施例中，服務提供者係用來控制帳戶行為，其被指定給該等數位訊息之預期的接受者。控制該帳戶行為可涵蓋多種操作。然而，這些操作之每一者皆實行於非網頁郵件伺服器上下文中。亦即，該預期的接受者透過該非網頁郵件伺服器所顯現之使用者介面(User Interface,“UI”)顯示屏存取他/她的帳戶。通常，該服務提供者不能夠施加控制於該UI顯示屏或修改其組態，因為該非網頁郵件用戶欠缺延伸協定來允許該服務提供者運用該UI顯示屏的態樣。據此，用於警告該預期的接受者，識別為潛在網路釣魚電子郵件的數位訊息之習知技術係無效的。

在一具體實施例中，用於控制該帳戶行為的操作，包括附加元資料標籤(metadata tag)於識別為潛在網路釣魚電子郵件的該等數位訊息，以及聚集它們於儲存位置中，其專用於存留(persist)該等標籤化的數位通訊，其與識別為合法電子郵件的數位訊息隔離。此專用的儲存位置映射至且可發佈為在該UI顯示屏上的文件夾。在選擇該文件夾後，配置於該專用的儲存位置之該等標籤化數位通訊的代表項(例如內容與數位通訊特性的元資料)係

發表(posted)給該接受者。據此，警示該接受者該等標籤化數位通訊的危險狀態，而不直接運用該 UI 顯示屏。

另外，使用者所啟動之動作可能係有限制的，其指向該等標籤化數位通訊的該等代表項。舉例來說，該接受者引動預先決定為受限制的動作(例如試圖移動標籤化數位通訊的指令、回應指令、對所有指令的回應及前向指令)之請求，被該服務提供者為了保護接受者的安全而使其失效。舉例來說，使該動作失效可包括攔截該請求、查明該動作係歸類為受限制的動作、查明該動作所指向之該數位通訊係標籤化為潛在網路釣魚電子郵件，以及無法實行該動作的該等步驟。在使該動作失效後，傳送操作失效指示(亦即已知的錯誤碼)至該非網頁郵件用戶，其轉而通知該接受者，該動作並未由該服務提供者實現。據此，提醒該接受者該標籤化數位通訊的危險狀態。再者，這些安全措施提供一層保護，防備可危害其他使用者的標籤化數位通訊之分布，即使該非網頁郵件用戶並不支援抗網路釣魚(antiphishing)特徵。

在另一具體實施例中，用於控制該帳戶行為的操作，包括取代識別為具警告訊息的潛在網路釣魚電子郵件之該等數位通訊。在一例子中，該警告訊息傳達該已識別的數位通訊可能係潛在網路釣魚電子郵件的一通知。在另一例子中，該警告訊息提供指示，透過網頁瀏覽器存

取該已識別的數位通訊之內容。在又另一例子中，該警告訊息包括鏈結至網頁瀏覽器的統一資源定位符(Uniform-Resource Locator, "URL")，其在由該接受者選擇後，允許該接受者在該服務提供者處，存取該已識別的數位通訊之內容。據此，藉由呈現該警告訊息給該接受者，以及避免揭露該已識別的數位通訊之內容，通知該接受者該數位通訊的危險狀態，並阻止該使用者不慎瀏覽至一遭侵入網站（compromised website）。

【實施方式】

於文中明確說明本發明標的以符合法定需求。然而，該說明本身係不欲限制此專利的範疇。而是，該等發明人已考慮所主張標的亦可以其他方式體現，配合其他現有或未來技術，包括類似於在此說明書中所說明之不同的步驟或步驟的組合。

據此，在一具體實施例中，本發明係關於體現於一個或多個電腦可讀取媒體上的電腦可執行指令，其在該使用者透過非網頁郵件用戶以存取帳戶後，執行用於警示使用者潛在網路釣魚電子郵件的方法。最初，該方法涉及在與該使用者相關的帳戶處接收數位通訊。附隨(incident to)識別該數位通訊為潛在網路釣魚電子郵件，附加元資料標籤於該數位通訊。接著，放置該標籤

化數位通訊於儲存位置內或與其相關，其專用於存留識別為潛在網路釣魚電子郵件的數位通訊。在該使用者透過該非網頁郵件用戶以存取該帳戶後，呈現該儲存位置的視覺代表項給該使用者。在具體實施例中，該視覺代表項提供指示給該使用者，潛在網路釣魚電子郵件已抵達該使用者帳戶處，且已被識別為具有危險狀態。

在另一具體實施例中，本發明的態樣涉及實行於伺服器的電腦化方法，當透過非網頁郵件用戶存取時，用於管理一個或多個數位通訊的處理。該方法包括在與該數位通訊之預期的接受者相關的帳戶處，檢測收到數位通訊，以及在接收該數位通訊後，施加過濾試探(filtering heuristics)來判定該數位通訊是否係未經要求的訊息或合法的訊息的該等步驟。當判定該數位通訊係未經要求的訊息時，標示該數位通訊為危險的。在接收使用者所啟動之請求來存取該危險數位通訊後，以警告訊息取代該危險數位通訊。在具體實施例中，該警告訊息可作用來執行以下服務中至少一者：傳達該危險數位通訊係識別為潛在網路釣魚電子郵件的一通知；提供透過網頁瀏覽器存取該危險數位通訊的內容之指示；或者提供鏈結至網頁瀏覽器的統一資源定位符(URL)，其在選擇後，允許該接受者存取該危險數位通訊的內容。

最後，指示該非網頁郵件用戶，顯露該危險數位通訊

的代表項於使用者介面(UI)顯示屏中所顯現之列表中。一般而言，該列表包括經判定為合法訊息的數位通訊之一個或多個代表項。在一例子中，該非網頁郵件用戶所顯現之該 UI 顯示屏，無法被管理該使用者帳戶的該服務提供者再配置。在接收該危險數位通訊的代表項的使用者所啟動之選擇後，傳遞指令至該非網頁郵件用戶，以呈現該警告訊息給該接受者，並阻擋揭露該危險數位通訊的內容。

在又另一具體實施例中，本發明涵蓋具有電腦可執行指令體現於其上的一個或多個電腦可讀取媒體，當執行時，其透過非網頁郵件用戶所顯現之使用者介面(UI)顯示屏，執行用於通知使用者潛在網路釣魚電子郵件已抵達該使用者帳戶處的方法。在一示例性具體實施例中，該方法包括產生儲存位置，其專用於存留識別為潛在網路釣魚電子郵件的一個或多個數位通訊。指示該非網頁郵件用戶來顯現文件夾於該 UI 顯示屏內。通常，該文件夾映射至該專用的儲存位置。

在一例子中，指示該非網頁郵件用戶顯現該文件夾於該 UI 顯示屏內包括指示該非網頁郵件用戶顯現該文件夾於列表中的程序，該列表包括映射至存留識別為合法電子郵件的數位通訊之儲存位置的其他文件夾。因此，該等潛在網路釣魚電子郵件係在視覺上與該等合法電子

郵件隔開。

在某時候，檢測到由該使用者實行以存取該文件夾的指示。在檢測後，指示該非網頁郵件用戶來顯現該等已識別的數位通訊的代表項。在一例子中，該等代表項包括元資料，其關於該等已識別的數位通訊之內容。

該方法可能更包括接收該使用者所啟動指向該等已識別的數位通訊之動作的該步驟。若認定該動作為預定義的受限動作，則該使用者所啟動之動作失效。在一例子中，使該使用者的動作失效包括阻止該動作的執行。此外，可傳送操作失效指示(例如標準的錯誤碼)至該非網頁郵件用戶，其中該操作失效指示傳達該動作失效的通知。

通常，本發明具體實施例係關於管理潛在網路釣魚電子郵件的處理。如於文中所使用，該片語「潛在網路釣魚電子郵件(potentially phishing emails)」不欲被理解為限制，且可涵蓋未經使用者要求的任何通訊。舉例來說，潛在網路釣魚電子郵件可包含濫發通訊、垃圾即時訊息及網路釣魚電子郵件。如以上所討論，網路釣魚電子郵件係自各種來源發送至預期的接受者帳戶，具有意圖騙取該接受者個人資訊(例如使用者名稱、密碼、信用卡細節等)的揭示。此誘因係有效的，因為該等網路釣魚電子郵件表示該來源為可信的實體。因此，引誘無戒備心的

接受者提供除此之外受保護的資訊。通常，該網路釣魚電子郵件具有類似於合法電子郵件或即時訊息的外表與感覺，且用於引導該使用者瀏覽假網站(亦即騙人的銀行網站)，其中詐騙引誘該使用者洩露敏感的資料(例如銀行帳戶登入、使用者識別、社會安全號碼等)。在其他的例子中，該網路釣魚電子郵件可以誘惑該使用者發送私人資訊至該網路釣魚電子郵件或其他惡毒實體的來源。

雖然該等潛在網路釣魚電子郵件於文中由該等片語「未經要求的訊息」、「標籤化訊息」、「危險數位通訊」及「網路釣魚電子郵件」指稱，但是這些片語之每一者皆應視為代表以上緊接著所說明之「潛在網路釣魚電子郵件」的共通概念。

在一個示例性具體實施例中，本發明係關於在非網頁郵件用戶上下文中，管理潛在網路釣魚電子郵件的處理。如於文中所使用，該片語「非網頁郵件用戶」不欲被理解為限制，且可廣泛指稱運行於終端使用者裝置(例如行動式裝置、電腦、個人數位助理(Personal digital assistant，“PDA”)或任何其他的用戶裝置)上的任何程式或應用程式，其無法像網頁瀏覽器一樣被管理。亦即，藉著運行於遠離該終端使用者裝置的伺服器上之服務提供者(例如 Hotmail)無法控制該非網頁郵件用戶所提供之使用者經驗。舉例來說，基於在該服務提供者處所接收

之訊息，無法修改該非網頁郵件用戶所顯現之 UI 顯示屏的該等要素。舉例來說，無法動態修改該 UI 顯示屏來通知該使用者潛在未經要求的訊息(例加潛在網路釣魚電子郵件)、警告該使用者電子郵件中的網路釣魚內容，或者限制使用者對特定通訊可採取的動作。

對該非網頁郵件用戶欠缺控制部分係由於以下因素中之一個或多個：用來存取該服務提供者的基本協定不具有標示數位通訊(亦即郵件訊息)為潛在網路釣魚電子郵件的語義；該非網頁郵件用戶所顯現之該 UI 顯示屏不能夠被該服務提供者運用(該 UI 顯示屏無法被管理該使用者帳戶的該服務提供者再配置)；以及該非網頁郵件用戶欠缺將允許該用戶支援新特徵的延伸協定，例如抗網路釣魚警告。據此，由於該非網頁郵件用戶(例如 Thunderbird)的該 UI 顯示屏係預定的，且無法被該服務提供者任意以動態方式管理，故用於警告與保護使用者防備潛在網路釣魚電子郵件(例如修改收件匣的 UI 顯示屏並提供專用的工具列)的習知技術係無效的。

簡要說明本發明具體實施例及其中某些特徵的概述後，以下說明適用於實行本發明的示例性操作環境。

一般而言參照該等圖式，且最初特別參照第 1 圖，顯示用於實行本發明具體實施例的示例性操作環境，且通常標示為運算裝置 100。運算裝置 100 係僅適合運算環

境的一示例，且不欲對於本發明使用範疇或功能作出任何限制。運算裝置 100 亦不應被理解為具有任何關於所例示之任何一組件或其組合之依賴項或需求。

本發明可說明於電腦碼或機器可使用指令之一般上下文中，包括電腦可執行指令，例如電腦或其他機器所執行之程式組件，例如個人數位助理或其他的手持裝置。通常，程式組件包括例式、程式、物件、組件、資料結構等，指稱執行特定作業或實行特定抽象資料型態的碼。本發明具體實施例可實作於多種系統組態中，包括手持裝置、消費者電子、通用電腦、專業運算裝置等。本發明具體實施例亦可實作於分布式運算環境中，其中作業係由藉由通訊網路所鏈結之遠端處理裝置執行。

持續參照第 1 圖，運算裝置 100 包括匯流排 110，其直接或間接耦合以下裝置：記憶體 112、一個或多個處理器 114、一個或多個展示組件 116、輸入/輸出(Input/Output，“I/O”)埠 118、I/O 組件 120，以及例示性電源供應器 122。匯流排 110 可代表一個或多個匯流排(例如位址匯流排、資料匯流排或其組合)。雖然第 1 圖的各種區塊為了清楚表示而以線顯示，但是實際上，描畫各種組件並非那麼清楚，且比喻來說，該等線若為灰色且模糊不清將更為精確。舉例來說，可考量展示組件(例如顯示屏裝置)係 I/O 組件。此外，處理器具有記憶

體。該等發明人於文中認定這係本技藝的本質，且重申第 1 圖的圖式僅為示例性運算裝置的例示，其可連同本發明一個或多個具體實施例使用。此類種類如「工作站」、「伺服器」、「膝上型電腦」、「手持裝置」等之間並沒有區分，因為所有都列入第 1 圖的範疇內考慮，且指稱「電腦」或「運算裝置」。

運算裝置 100 一般而言包括多種電腦可讀取媒體。舉例來說，而非限制，電腦可讀取媒體可包含隨機存取記憶體(Random Access Memory，“RAM”)；唯讀記憶體(Read Only Memory，“ROM”)；電子可抹除可程式化唯讀記憶體(Electronically Erasable Programmable Read Only Memory，“EEPROM”)；快閃記憶體或其他的記憶體技術；唯讀光碟(Compact Disc Read Only Memory，“CDROM”)、數位多功能碟片(Digital versatile disk，“DVD”)或其他的光學或全像媒體；卡式磁帶、磁帶、磁碟儲存或其他的磁性儲存裝置；或者可用來編碼所需資訊且可被運算裝置 100 存取的任何其他的媒體。

記憶體 112 包括具有揮發性及/或非揮發性記憶體形式的電腦儲存媒體。該記憶體可能係可移除的、不可移除的或其組合。示例性硬體裝置包括固態記憶體、硬碟、光碟機等。運算裝置 100 包括一個或多個處理器，其自各種實體(例如記憶體 112 或 I/O 組件 120)讀取資料。展

示組件 116 呈現資料指示給使用者或其他裝置。示例性展示組件包括顯示屏裝置、揚聲器、列印組件、振動組件等。I/O 埠 118 允許運算裝置 100 在邏輯上耦合於其他的裝置，包括 I/O 組件 120，該等裝置的某些可為內建。例示性組件包括擴音器、搖桿、遊戲墊、衛星碟形、掃描器、印表機、無線裝置等。

在某些具體實施例中，第 1 圖的運算裝置 100 係配置成實行本發明之各種態樣。在一例子中，這些態樣關於在檢測使用者所啟動之請求來觀看該潛在網路釣魚電子郵件後，或在接收該潛在網路釣魚電子郵件指向的動作後，管理潛在網路釣魚電子郵件的處理。在另一例子中，這些態樣關於將該等潛在網路釣魚電子郵件與識別為合法的電子郵件隔開，並且以通知非網頁郵件用戶的使用者它們的危險狀態之方式，呈現該等潛在網路釣魚電子郵件。

用於通知使用者數位通訊係危險的，以及用於保護該使用者防備由於潛在網路釣魚電子郵件而洩露個人資訊的這些技術，現在將參照第 2 圖進行討論。特定而言，第 2 圖描繪出例示適合用來實行本發明具體實施例的分佈式運算環境之示例性系統架構 200 的區塊圖。通常，實行本發明具體實施例關於通知預期的接受者：識別為潛在網路釣魚電子郵件的數位通訊，因此標示該數位通

訊為危險狀態，以及關於限制對該數位通訊可採取的動作(例如觀看內容、移動至另一文件夾、回應或前向等)。應瞭解與察知顯示於第 2 圖中的示例性系統架構 200 僅為一適合運算環境的一個示例，且不欲對本發明使用範疇或功能作出任何限制。示例性系統架構 200 亦不應被解譯為具有任何關於其中所例示之任何單一組件或組件的組合之依賴項或需求。

最初，示例性系統架構 200 包括來源 210、使用者 250、用戶裝置 260、資料儲存庫 230(亦即結構化可搜尋資料庫)、網頁伺服器 220，以及與這些項目之每一者互連的網路 205。顯示於第 2 圖中的用戶裝置 260、資料儲存庫 230 及網頁伺服器 220 之每一者皆可具有運算裝置多種種類的形式，例如上述參照第 1 圖之運算裝置 100。僅舉例來說而非限制，用戶裝置 260 及/或網頁伺服器 220 可能係個人電腦、桌上型電腦、膝上型電腦、消費者電子裝置、手持裝置(例如個人數位助理)、各種伺服器、處理設備等。然而應注意，本發明不被限制在實行於此類運算裝置上，但可實行於本發明具體實施例的範疇內在多種不同種類的運算裝置之任一者上。

一般而言，裝置 260 與 220 之每一者皆包括或係鏈結至某形式的運算單元(例如中央處理單元、微處理器等)，以支援運行於其上該(等)組件的操作(例如接收組件

221、管理組件 222、儲存組件 223 等)。如於文中所使用，該片語「運算單元」通常指稱具有處理能力與儲存記憶體之專用的運算裝置，其支援構成軟體、應用程式及電腦程式執行於其上之基礎的操作軟體。在一例子中，該運算單元係以有形的硬體元件或機器配置，其係整合於或可操作耦合於裝置 260 與 220，好讓每個裝置得以執行與通訊有關的處理及其他操作(例如在接收組件 221 處檢測數位通訊，以及在管理組件 222 處識別該數位通訊為潛在網路釣魚電子郵件)。在另一例子中，該運算單元可涵蓋處理器(未顯示)，其耦合於裝置 260 與 220 之每一者皆容納之電腦可讀取媒體。

通常，該電腦可讀取媒體包括實體記憶體，其至少暫時儲存可由該處理器執行的複數電腦軟體組件。如於文中所使用，該術語「處理器」並非意謂著限制，且可涵蓋該運算單元中具有運算能力的任何元件。在此類能力中，該處理器可配置成處理指令之有形的物件。在一示例性具體實施例中，處理可涉及提取、解碼/解譯、執行及回寫指令。

此外，除了處理指令之外，該處理器可轉移資訊至裝置 260 與 220 整合於或配置於其上的其他資源，以及自該等資源轉移資訊。通常，資源指稱讓裝置 260 與 220 能夠執行特定功能的軟體組件或硬體機制。僅舉例來

說，網頁伺服器 220 所容納之該等資源可包括以下一個或多個：接收組件 221、管理組件 222、儲存組件 223 及評估組件 224。一個或多個這些組件可結合，以提供服務提供者(未顯示)的特定功能態樣。通常，該服務提供者(例如 Hotmail)管理使用者線上帳戶(例如電子郵件帳戶)的態樣，例如接收、發送、組織及儲存郵件訊息。

在另一範例中，用戶裝置 260 所容納之該等資源可包括以下一個或多個：映射組件 241、顯現組件 242 及互動組件 243。一個或多個這些組件可結合，以提供非網頁郵件用戶 240 的特定功能態樣。通常，該非網頁郵件用戶(例如 Thunderbird)顯現 UI 顯示屏，其允許使用者存取與管理該服務提供者所支援之線上帳戶。

用戶裝置 260 可包括輸入裝置(未顯示)與展示裝置(未顯示)。通常，該輸入裝置係經提供來接收輸入，除了別的以外，該輸入影響包括數位通訊 215 及其代表項的文件夾展示，以及接收指向存留於該使用者帳戶處的一個或多個數位通訊 215 的動作。例示性裝置包括滑鼠、搖桿、小型鍵盤、擴音器、第 1 圖的 I/O 組件 120，或者能夠接收使用者輸入並傳遞該輸入的指示至用戶裝置 260 之任何其他組件。

在具體實施例中，該展示裝置係配置成顯現及/或呈現 UI 顯示屏於其上。可操作耦合於用戶裝置 260 的輸出之

該展示裝置，可配置成能夠呈現資料給使用者的任何展示組件，例如數位監視器、電子顯示面板、觸控螢幕、類比機上盒、電漿螢幕、音頻揚聲器、盲文鍵盤(Braille pad)等。在一種示例性具體實施例中，該展示裝置係配置成呈現豐富內容，例如存在著數位通訊與文件夾的代表項之顯示屏區域。在另一種示例性具體實施例中，該展示裝置能夠顯現與識別為合法的數位通訊相關之內容，或者顯現與識別為潛在網路釣魚電子郵件的數位通訊相關之警告訊息。在又另一種示例性具體實施例中，該展示裝置可呈現媒體的其他形式(例如音頻訊號)，或者主動的(例如該使用者可選擇瀏覽網站)或撤銷的統一資源定位符(URL)鏈結。

資料儲存庫 230 通常係配置成儲存與附加於識別為該(等)潛在網路釣魚電子郵件的數位通訊之存留標籤相關的資訊。在其他的例子中，資料儲存庫 230 係配置成儲存隔離列表於資料儲存庫 230 所容納之電腦可讀取媒體上。一般而言，該隔離列表充當索引，其列舉識別為已抵達該使用者帳戶處的潛在網路釣魚電子郵件的該等數位通訊之每一者。在另一具體實施例中，該隔離列表包括電子郵件識別(IDs)的清單，其已標示為具有危險狀態(例如間諜軟體、濫發、網路釣魚訊息、受感染的電子郵件等)。

在各種具體實施例中，儲存於資料儲存庫 230 處的資訊可包括，但不限於，顯現來代替潛在網路釣魚電子郵件內容的警告訊息、接收於該使用者帳戶處的數位通訊內容、用於判定數位通訊是否係危險的過濾試探、受限制動作的列表，以及支援該服務提供者的該操作之任何其他資料，如於文中所討論者。此外，資料儲存庫 230 可配置成可搜尋該已儲存資訊的適合存取。舉例來說，資料儲存庫 230 可搜尋與專用於存留潛在網路釣魚電子郵件的儲存位置相關之數位通訊。

熟習本技術者將可了解與察知，儲存於資料儲存庫 230 中的資訊係可配置的，且可包括有關產生與維護該專用儲存位置與該受限制動作的任何資訊。此類資訊的內容與量係不欲以任何方式限制本發明具體實施例的範疇。再者，雖然例示為單一、獨立組件，資料儲存庫 230 事實上可能係複數資料庫，例如資料庫叢集，其部分可常駐於用戶裝置 260、網頁伺服器 220、另一外部運算裝置(未顯示)及/或其任何組合上。

此示例性系統架構 200 係僅適合環境的一種示例，其可實行以實現本發明的態樣，且係不欲對本發明的使用範疇或功能作出任何限制。例示的示例性系統架構 200 亦不應被解譯為具有關於如所例示之裝置 260 與 220、資料儲存庫 230 及組件 221、222、223、224、241、242

與 243 的任一者或組合之任何依賴項或需求。在某些具體實施例中，一個或多個組件 221、222、223、224、241、242 與 243 可實行為獨立運行的裝置。在其他的具體實施例中，一個或多個組件 221、222、223、224、241、242 與 243 可直接整合於網頁伺服器 220 中，或者於互連以形成網頁伺服器 220 的分佈式節點上。熟習本技術者將可了解，組件 221、222、223、224、241、242 與 243(例示於第 2 圖中)在本質上與數量上係示例性，且不應被理解為限制。

據此，可採用任何數量的組件，以在本發明具體實施例的範疇內達成所需功能。雖然第 2 圖的各種組件為了清楚表示而以線顯示，但是實際上，描畫各種組件並非那麼清楚，且用比喻來說，該等線係灰色或模糊不清將更為精確。另外，雖然第 2 圖的某些組件係描繪為單一區塊，但是該等描繪在本質上與數量上係示例性，且不被理解為限制(例如雖然僅顯示一儲存組件 243，但是更多儲存組件 243 可容納於網頁伺服器 220 上、體現於資料儲存庫 230 上，或者可通訊耦合於用戶裝置 260)。

另外，該示例性系統架構的該等裝置，可藉由該相關領域中已知的任何方法互連。舉例來說，透過分佈式運算環境，其包括透過一個或多個網路 205 彼此耦合的多個運算裝置，網頁伺服器 220 與用戶裝置 260 可以操作

方式耦合。在具體實施例中，網路 205 可包括，而不限於，一個或多個區域網路(Local Area Network，“LAN”)及/或廣域網路(Wide Area Networks，“WAN”)。此類網路環境常見於辦公室、企業電腦網路、企業內部網路及網際網路中。據此，於文中並未另外說明該網路。

在操作時，組件 221、222、223、224、241、242 與 243 被設計以執行程序，該程序包括至少識別自來源 210 的數位通訊 215 為潛在網路釣魚電子郵件、附加指示數位通訊 215 具有危險狀態的標籤(例如元資料)於數位通訊 215，以及實行技術方案以保護與通知使用者 250 的該等步驟。這些技術方案包括警示使用者 250 潛在網路釣魚電子郵件的存在，以及限制使用者 250 對於該潛在網路釣魚電子郵件所請求之該等動作。在具體實施例中，來源 210 代表一個或多個惡毒的實體，例如犯罪或非法的電腦程式，其傳送訊息(例如數位通訊 215)給使用者 250，該等訊息騙取該使用者對其個人資訊的揭示。在具體實施例中，使用者 250 代表任何實體，其係來源 210 所分佈之數位通訊 215 之預期的接受者。舉例來說，使用者 250 可能係擁有/具備用戶裝置 260 的個人，其與該服務提供者處的帳戶相關，或者其能夠透過非網頁郵件用戶 240 存取該帳戶。

最初，接收組件 221 負責自從源 210 接受與檢測數位

通訊 215。為了達到存留與使用者 250 帳戶相關的數位通訊 215 之目的，接收組件 221 接著傳遞數位通訊 215 至網頁伺服器 220 上所容納之資料儲存庫 230 或儲存組件 223。連同促進數位通訊 215 的儲存，接收組件 221 可傳遞數位通訊 215 至管理組件 222。

在接收數位通訊 215 後，管理組件 222 係配置成執行多種操作。最初，該等操作包含自那些合法的數位通訊 215，過濾其中屬危險的及/或未經要求者。在一例子中，該過濾操作識別數位通訊 215 是否係潛在網路釣魚電子郵件，且如此標示數位通訊 215。識別數位通訊 215 為危險的或合法的該步驟，可基於採用過濾試探的分析。這些過濾試探在掃描進入的數位通訊 215 後，判定數位通訊 215 是否自可信的網站或已知的有害電子郵件的來源抵達，及/或該數位通訊的該等內容是否係惡意的或符合危害的臨界位準。

基於以上一個或多個這些條件，數位通訊 215 可識別為潛在網路釣魚電子郵件，且標示為具有危險狀態。由於該等過濾試探並不精確，且有時候係錯誤的(基於該電子郵件的屬性提供錯誤肯定)，故被認為危險的數位通訊 215 被視為「潛在」網路釣魚電子郵件來允許使用者 250 對數位通訊 215 是否係真正安全的做出最後判斷，藉此查驗該電子郵件的實際品質。此反抗識別為「網路釣魚

電子郵件」的訊息，其可自動從該使用者帳戶移除，而不提供使用者 250 機會以驗證該識別。

在具體實施例中，標示數位通訊 215 為潛在網路釣魚電子郵件或具有危險狀態，涉及附加標籤於數位通訊 215。此標籤可包含元資料，其儲存與數位通訊 215 相關，且用來控制數位通訊 215 儲存於何處，以及指向數位通訊 215 的什麼動作係受限制的。

雖然已說明用於標示數位通訊 215 為危險的或潛在網路釣魚的一種方法，但是熟習本技術者應可了解與察知，可使用提供潛在危害指示之其他種類的適合標旗(flagging)方案，且本發明具體實施例不限制於文中所說明之所附加的元資料標籤。舉例來說，藉由加上危險數位通訊 215 的識別於隔離列表，其列舉已抵達該使用者帳戶處的該等潛在網路釣魚電子郵件之每一者，可追蹤危險數位通訊 215。

在其他的具體實施例中，在查明數位通訊 215 係潛在網路釣魚電子郵件後，管理組件 222 所執行之該等操作包含產生儲存位置，其專用於存留識別為潛在網路釣魚電子郵件的數位通訊 215。若該專用的儲存位置係已存在，則放置標示為危險的數位通訊 215(例如附加元資料標籤的訊息)於該專用的儲存位置中，或者至少其儲存與該專用的儲存位置相關。在一例子中，該專用的儲存位

置係由儲存組件 243 管理，且占據在網頁伺服器 220 及/或資料儲存庫 230 上的記憶體。

通常，該專用的儲存位置用來提供實體記憶體位置，其與該記憶體位置隔開，其中存留與該使用者帳戶相關之其他數位通訊(例如識別為合法的訊息)。據此，當使用者 250 透過非網頁郵件用戶 240 存取該帳戶時，映射組件 241 將分別檢測該等分開的儲存位置，並個別產生映射至該等分開的儲存位置之文件夾。亦即，映射組件 241 係配置成設置該等文件夾於該 UI 顯示屏或用戶視面中，以反映該等儲存位置於網頁伺服器 220 上。舉例來說，可產生「收件匣」文件夾，其映射至持有合法訊息的該儲存位置，而可產生分離的「網路釣魚郵件」文件夾，其持有識別為潛在網路釣魚電子郵件的數位通訊 215。如此，使用者 250 的注意力被吸引至隔離來自已接收的數位通訊 215 之語料庫(corpus)的特定訊息，藉此警示使用者 250 危險的或潛在網路釣魚電子郵件的存在。

在產生該等文件夾且以適當的數位通訊 215(基於該等儲存位置與該等文件夾之間的映射)填入該等文件夾後，顯現組件 242 在 UI 顯示屏處，發佈該等文件夾給使用者。在一例子中，發佈可包括分別發表該等文件夾之每一者的標題。舉例來說，映射至持有合法訊息的儲存位置之文件夾的標題「收件匣」，可安置於該收件匣文件

夾的顯示屏旁邊，而映射至該專用的儲存位置之文件夾的標題「網路釣魚郵件」，可安置於該網路釣魚郵件文件夾的顯示屏旁邊。據此，該服務提供者能夠傳達特定訊息被認為是危險的給使用者 250，且能夠傳達為何指向存留於該網路釣魚郵件文件夾中的該等危險訊息的使用者所啟動之動作係受限的—缺乏運用網頁瀏覽器的UI顯示屏的能力。亦即，顯露該網路釣魚郵件文件夾減輕非網頁郵件用戶 240 所固有之無法通知使用者網路釣魚行為的問題，其中該減輕涉及允許使用者 250 在該收件匣文件夾上下文中，觀看該網路釣魚郵件文件夾。有利的是，當瀏覽文件夾時，該網路釣魚郵件文件夾提供使用者 250 一致的直覺性經驗，且可容許於非網頁郵件用戶 240 的範圍內。

如以上更完整的討論，可顯現該 UI 顯示屏於該展示裝置處，其可操作耦合於用戶裝置 260，非網頁郵件用戶 240 運行於其上。舉例來說，參照第 6 圖所顯現之示例性 UI 顯示屏 600，其包括在文件夾列表 640 內，接近於網路釣魚郵件文件夾 630 的代表項之收件匣文件夾 620 的代表項。在選擇文件夾 620 或 630 其中之一後，分別存留於文件夾 620 或 630 中之數位通訊 215 的代表項係顯示於 UI 顯示屏 600 上。如顯示於此例示中，收件匣文件夾 620 被選定。因此，儲存於收件匣文件夾 620 中之

某些數位通訊 215 的代表項係呈現於收件匣 680 中。據此，使用者 250 了解這些數位通訊 215 係識別為合法的，且可放心觀看、儲存、發送等。

一般而言，數位通訊 215 的該等代表項係提取自數位通訊 215 的特性及/或內容。舉例來說，數位通訊 215 的該等代表項可包括該等內容的快照、日期、該發送者的身份，及/或相當於數位通訊 215 的標題或主題列之標頭，如於第 6 圖的收件匣 680 中訊息 665 與 675 的代表項所描述。在選擇(例如滑鼠點擊)數位通訊 215 的代表項後，互動組件 243 傳送指令至該服務提供者，以擷取數位通訊 215 的該等內容。該服務提供者接著檢查附加於該數位代表項的該(等)標籤，以判定數位通訊 215 是否係標示為具有危險狀態，或者識別為潛在網路釣魚電子郵件。若識別為潛在網路釣魚電子郵件或是危險的，則該服務提供者可判定是否為了顯現該內容或以警告訊息(見第 7 圖的參考數字 700)將其取代，而傳達選定的數位通訊 215 的內容至非網頁郵件用戶 240。

在一種技術方案中，一般而言當查明該使用者所啟動之選擇係指向標示為潛在網路釣魚電子郵件(藉由檢查附加於數位通訊 215 的元資料標籤)之數位通訊 215 的代表項，且查明數位通訊 215 係存留於該專用的儲存位置中時，數位通訊 215 的部分內容而顯露出來供使用者 250

檢驗。在此技術方案中，一個或多個統一資源定位符(URL)鏈結係撤銷的，該鏈結納入存留於該專用的儲存位置中之該潛在網路釣魚電子郵件的內容內。據此，阻止使用者 250 透過該潛在網路釣魚電子郵件瀏覽詐騙網站，但在檢查其內容後，仍可評估該潛在網路釣魚電子郵件是否係真正危險的或未經要求的。有利的是，禁止該等 URL 鏈結減少該使用者暴露於潛在危險的網站(例如騙人的網站)，且有效減輕在試圖拜訪該網站後，可能造成的財務與個人的損害。

在第二技術方案中，一般而言當查明該使用者所啟動之選擇，係指向標示為潛在網路釣魚電子郵件之數位通訊 215 的代表項，且數位通訊 215 係存留於包括合法通訊(映射至該收件匣文件夾)的共用儲存位置中時，選定的數位通訊 215 的內容係以警告訊息取代，該訊息可能為了被使用者 250 檢驗而顯露出來。在此技術方案中，該警告訊息可以通知使用者 250：選定的數位通訊 215 被視為具有危險狀態，替代採用該專用的儲存位置(映射至該網路釣魚郵件文件夾)，以通知使用者 250 可能的危害。由於選定的數位通訊 215 的內容並未揭露，故該警告訊息可視需要包括在選擇後，導引使用者 250 至網頁瀏覽器之指令及/或 URL 鏈結。該網頁瀏覽器允許使用者 250 在受保護的環境中觀看選定的數位通訊 215 的內

容，其係由該服務提供者動態控制，且當使用者 250 與選定的數位通訊 215 互動時，該網頁瀏覽器可發出警示及其他的安全措施。據此，藉由隱藏該潛在網路釣魚電子郵件，基本上阻止使用者 250 瀏覽詐騙網站，但仍可在該網頁瀏覽器處存取該潛在網路釣魚電子郵件的該等內容，以查明其是否係真正危險的或未經要求的。

在一示例性具體實施例中，使用者 250 可能試圖執行關於識別為潛在網路釣魚電子郵件的一個或多個數位通訊 215 的動作。在一例子中，使用者 250 可能試圖強加「移動」動作於標示為危險的數位通訊上。舉例來說，該移動動作可包括，試圖自該專用的儲存位置移動該危險的數位通訊至儲存位置，其持有識別為合法的數位通訊。在具體實施例中，當使用者 250 即將引動該移動時，或者當非網頁郵件用戶 240 與該服務提供者係同步時，可傳送該移動動作為需求 270。

透過互動組件 243，可於請求 270 內傳送此移動動作至該服務提供者的評估組件 224。一般而言，評估組件 224 攔截該使用者所啟動之請求 270(例如施加於該 UI 顯示屏處)，且判定該移動動作是否係針對危險的數位通訊。若係如此，則評估組件 224 判定該移動動作是否出現於受限制動作的列表上。若係如此，則評估組件 224 不允許該危險的數位通訊在該專用的儲存位置外部移

動。據此，在同步後，回傳該危險的數位通訊的代表項至該網路釣魚郵件文件夾中，其映射至該專用的儲存位置，藉此通知該使用者：該數位通訊被認為持續具有危險的狀態。換言之，使用者 250 不能自該網路釣魚郵件文件夾，移動危險的數位訊息至任何其他文件夾，且讓該移動反映於網頁伺服器 220 上。即使在容許移動動作的例子中，自該專用的儲存位置退出該危險的數位通訊，並不影響與該危險的數位訊息相關的該元資料標籤及相關的功能。

在另一例子中，使用者 250 可能試圖引導另一受限制的動作朝向標示為危險的數位通訊。舉例來說，這些受限制的動作包含一個或多個回應指令、對所有指令的回應及前向指令。雖然已說明數個不同的指令為受限制的動作，但是熟習本技術者應可了解與察知，使用者所發出針對數位訊息之其他種類的適合指令，係考量為受限制的動作(例如儲存指令、編輯指令等)，且本發明之該具體實施例不限於文中所說明之那些指令。

於危險的數位通訊上提供該受限制的動作後，可透過互動組件 243，於請求 270 內傳送該受限制的動作至評估組件 224。再次，評估組件 224 攔截需求 270，且判定該受限制的動作是否係針對危險的數位通訊。舉例來說，判定危險的或潛在網路釣魚的數位通訊是否被針對

為目標涉及檢查該隔離列表，以查明該選定數位通訊的識別是否出現於其中。在另一示例中，判定危險的數位通訊是否被針對為目標涉及檢查該選定的數位通訊，以查明該數位通訊是否係附加著標示該數位通訊為網路釣魚訊息的標籤。

通常，附加於該選定的數位通訊的該元資料標籤控制如何處理該數位通訊，以及是否實踐發出於請求 270 中的動作。此外，可調整包含該標籤的該元資料，以允許特定動作而不允許其他動作。據此，在該等過濾試探判定與該等數位訊息個別相關的風險位準，且請願（memorialize）該風險位準為該標籤內的該元資料後，該等受限制的動作特定於每個數位訊息。

若使用者 250 針對危險的數位通訊，則評估組件 224 不允許該動作整體或部分的執行。在一例子中，使該動作的執行失效包括使對「回應」或「前向」該數位通訊 215 的指令失效。再者，發送操作失效指示或已知的錯誤碼至非網頁郵件用戶 240，以回應該失效的請求 270。在一例子中，該操作失效指示基本上係類似於當實現動作時，在該服務提供者遭遇實際錯誤後，那些所產生的與所傳送的指示，與此案例相反的例子中，使該受限制的動作之執行失效係故意的。在另一例子中，發送該操作失效指示，涉及回傳藉此已知的錯誤碼至非網頁郵件

用戶 240。在此例子中，非網頁郵件用戶 240 可自動傳達訊息、視覺指標(例如彈出式顯示屏)或該使用者所提供之動作失效的其他表達式給使用者 250。據此，該失效訊息或該指標強化使用者 250 所選擇之該數位通訊係識別為潛在網路釣魚電子郵件。

此外，藉由限制可提供至該等危險數位通訊之該等使用者動作，該服務提供者控制潛在網路釣魚電子郵件的分佈與影響。有利的是，根據以上的安全措施，其作用於不支援任何抗網路釣魚特徵之非網頁郵件用戶 240 的該等範圍內，由於禁止使用者 250 回應潛在網路釣魚郵件，故能確保使用者安全。

現在轉參考第 3 圖，其描述例示用於識別與組織本發明一具體實施例的潛在網路釣魚電子郵件技術的高階概述的操作流程圖 300。雖然於文中可使用該等術語「步驟」及/或「區塊」來暗示所採用方法的不同要素，但是該等術語不應被解譯為於文中所揭示各種步驟之間隱含任何特定的順序，除非與除了明確說明個別步驟的順序時。

最初，流程圖 300 顯示執行數個操作的服務提供者 310。服務提供者 310 可由第 2 圖的網頁伺服器 220 支援，或由遠離非網頁郵件用戶 240 之任何其他硬體支援。服務提供者 310 所執行之該等操作，包括自來源

210(見步驟 315)接收訊息(例如第 2 圖的數位通訊 215)，以及查明該訊息是否係潛在網路釣魚電子郵件(見步驟 320)。在查明該訊息係潛在網路釣魚電子郵件後，服務提供者 310 附加識別該訊息為潛在網路釣魚電子郵件的元資料標籤於該訊息，如步驟 325 所描述。

參照以上清楚說明的該第一技術方案，可儲存該標籤化訊息於儲存位置中，該位置專用於存留潛在網路釣魚電子郵件，且該標籤化訊息可在非網頁郵件用戶 240 所顯現之該 UI 顯示屏上的網路釣魚郵件文件夾中呈現給使用者 250。參照以上清楚說明的該第二技術方案，可儲存該標籤化訊息於連同合法訊息的共用儲存位置中，且該標籤化訊息可在非網頁郵件用戶 240 所顯現之該 UI 顯示屏上的收件匣文件夾中呈現給使用者 250。然而，該標籤化訊息的代表項的使用者所啟動之選擇，將自該服務提供者檢索取代該標籤化訊息的初始內容的警告訊息。

如步驟 330 所描述，於非網頁郵件用戶 240 處接收使用者所啟動之指令，以觀看與使用者 250 相關的帳戶，且該指令被傳達至服務提供者 310。舉例來說，在使用者 250 登入且促動該帳戶後，該觀看指令可自動發送。在接收該觀看指令後，服務提供者 310 組織文件夾，使得它們映射至該等已建立的儲存位置，且以基於標籤化

至其上的該元資料之適當訊息填入該等文件夾，如步驟340所描述。該等已組織的文件夾係由非網頁郵件用戶240所顯現，且發佈於UI顯示屏上，如步驟350所描述。這些已組織的文件夾用以通知使用者250：附加於該等訊息的該狀態(安全的或危險的)已填入每個文件夾中。

最後，可自使用者250接收請求(例如第2圖的請求270)，以提供動作於一個或多個該等訊息上。此係步驟360所描述。此請求發送至服務提供者310，其基於至少兩個以下條件判定是否實踐該需求：附加於該請求所針對訊息的該元資料，是否指示該(等)訊息係識別為潛在網路釣魚電子郵件；以及所提供之該動作是否係受限制的動作。若不符合該等條件之任一者，則實現該動作。或者，該受限制的動作並未實行於識別為潛在網路釣魚電子郵件的該(等)訊息上。此係步驟370所描述。當未實行或拒絕該動作時，發送操作失效指示至非網頁郵件用戶240，如步驟380所描述。

參照第4圖，根據本發明一具體實施例，顯示例示綜合方法400之流程圖，該方法用於在該使用者透過非網頁郵件用戶存取帳戶後，警示使用者潛在網路釣魚電子郵件。最初，方法400涉及在與該使用者相關的該帳戶處接收數位通訊，如區塊410所描述。附隨識別該數位通訊為潛在網路釣魚電子郵件，附加元資料標籤於該數

位通訊，如區塊 420 所指示。接著，放置該標籤化數位通訊於儲存位置內或與其相關，該儲存位置專用於存留識別為潛在網路釣魚電子郵件的數位通訊，如區塊 430 所指示。在該使用者透過該非網頁郵件用戶存取該帳戶後，呈現該儲存位置的視覺代表項給該使用者，如區塊 440 所指示。在具體實施例中，該視覺代表項提供指示給該使用者，潛在網路釣魚電子郵件已抵達該使用者的帳戶處，且已被識別為具有危險狀態。

參照第 5 圖，根據本發明一具體實施例，顯示例示綜合方法 500 之流程圖，該方法用於當透過非網頁郵件用戶存取時，管理一個或多個數位通訊的處理。最初，方法 500 包括在與該數位通訊預期的接受者相關之帳戶處，檢測數位通訊的接收。如區塊 510 所描述，在接收該數位通訊後，施加過濾試探以判定該數位通訊是否係未經要求的訊息或合法的訊息。當判定該數位通訊係未經要求的訊息時，標示該數位通訊為危險的，如區塊 520 所描述。在接收使用者所啟動之需求以存取該危險的數位通訊後，以警告訊息取代該危險的數位通訊，如區塊 530 所描述。在具體實施例中，該警告訊息可作用來執行以下服務至少一者：傳達該危險的數位通訊係識別為潛在網路釣魚電子郵件的通知；透過網頁瀏覽器提供指示以存取該危險數位通訊的內容；或者提供統一資源定

位符(URL)鏈結至在選擇後，允許該接受者存取該危險數位通訊的內容之網頁瀏覽器。

最後，如區塊 540 所描述，指示該非網頁郵件用戶，顯露該危險的數位通訊的代表項於使用者介面(UI)顯示屏中所顯現之列表中。一般而言，該列表包括判定係合法訊息的數位通訊之一個或多個代表項。在一例子中，該非網頁郵件用戶所顯現之該 UI 顯示屏，無法由管理該使用者帳戶的該服務提供者再配置。在接收該危險的數位通訊的該代表項的使用者所啟動之選擇後，傳遞指令至該非網頁郵件用戶，以呈現該警告訊息給該接受者，並阻擋揭露該危險的數位通訊的內容。此係區塊 550 所描述。

參照第 6 圖，顯示示例性使用者介面 600 之例示性螢幕顯示屏，其用於呈現映射至專用於存留潛在網路釣魚電子郵件的儲存位置之文件夾。如以上所討論，收件匣文件夾 620 與網路釣魚郵件文件夾 630 可顯示於文件夾列表 640 中。在具體實施例中，文件夾 620 與 630 的該組織在該服務提供者處，映射至該等儲存位置的該管理，而分別包括在文件夾 620 與 630 中的該等訊息，則映射至分別填入該等分開的儲存位置(例如專用的與共用的)之該等訊息。

另外，訊息 660 的代表項可顯示於使用者介面 600 上。

在一具體實施例中，僅在存取網路釣魚郵件文件夾 630 後，呈現訊息 660 的該等代表項，其附加著指示危險狀態的元資料標籤。另一方面，在第 6 圖所例示之該具體實施例中，在存取收件匣文件夾 620 後，於收件匣 680 中訊息 660 的列表中呈現訊息 665 與 675 的該等代表項，其附加著指示危險狀態的元資料標籤。亦即，存留該等標籤化訊息與該等合法訊息於共用儲存位置中，且將其填入共用文件夾，例如收件匣文件夾 620。據此，為了通知該使用者附加著元資料標籤之訊息 665 與 675 的這些代表項，係識別為潛在網路釣魚電子郵件，故在該使用者試圖打開與觀看訊息 665 與 675 後，顯露警告訊息。

現在轉參第 7 圖，顯示示例性使用者介面之例示性螢幕顯示屏，其用於呈現顯現來替代揭露潛在網路釣魚電子郵件的內容之警告訊息 700。如以上所討論，根據該第二技術方案，為了觀看而選定之標籤化訊息的內容係以警告訊息 700 取代，其由非網頁郵件用戶顯示給該使用者。因此，該警告訊息具體而言可以警示該使用者：與此訊息相關的潛在風險。具體實施例中的警告訊息 700 可包括明確的警告發表 710，以緊接著通知該使用者，選定訊息係與危險狀態相關。另外，警告訊息 700 可包括說明 720，其用於以警告訊息 700 取代該初始內容，

及/或清楚描繪使用者應採取以觀看該初始內容的該等步驟之指示。在一例子中，該等指示可指示該使用者應登入網頁瀏覽器，以觀看該標籤化訊息的初始內容。在此例子中，未提供 URL 鏈結於警告訊息 700 的主體中。有利的是，藉由省略該 URL 鏈結，避免詐騙行為者於作為網路釣魚向量的假警告訊息內，使用 URL 鏈結的任何機會。

在另一例子中，如例示於第 7 圖中，顯露 URL 鏈結 740 於警告訊息 700 中。URL 鏈結 740 的選擇引導該使用者至網頁瀏覽器，其將允許該使用者觀看該選定訊息的初始內容，以查驗該訊息是否係恰當識別為潛在網路釣魚電子郵件。一般而言，該網頁瀏覽器包括讓其成為用於觀看可能的網路釣魚內容之安全論壇(forum)的抗網路釣魚控制。

在又另一例子中，具體修改警告訊息 700。在一具體實施例中，基於與該使用者試圖觀看該標籤化訊息有關的資訊，具體修改警告訊息 700，其中該資訊係取自該服務提供者可存取的來源。舉例來說，基於與該使用者相關的區域/市場之指示，修改警告訊息 700 的語言給該使用者，其中該使用者的區域/市場之指示係取自該使用者的線上輪廓。在第二具體實施例中，基於與該標籤化訊息有關的資訊，具體修改警告訊息 700，其中該資訊

係取自該標籤化訊息的初始內容或特性。舉例來說，顯露來自該標籤化訊息的一段內容730於警告訊息700中。

已參照特定具體實施例說明本發明，該等具體實施例係以為例示而非限制的方式呈現於所有態樣中。熟習本技術者在不悖離本發明範疇下顯然將可察知與本發明有關之替代性具體實施例。

自以上所述，將可發現此發明係非常適合達到以上所提出之所有目標與目的，以及達到該系統與方法顯著與固有的其他優點功效。將可了解特定特徵與次組合係為了實用，且可被採用而不參照其他的特徵與次組合。此係由申請專利範圍的範疇所列入考慮，且落於其內。

【圖式簡單說明】

以下參照附屬圖式詳細說明本發明，其中：

第1圖係適合用來實行本發明具體實施例之示例性運算環境之區塊圖；

第2圖係例示適合用來實行本發明具體實施例之分佈式運算環境之區塊圖，該運算環境係配置成在非網頁郵件用戶上下文中，管理潛在網路釣魚電子郵件；

第3圖係例示用於識別與組織本發明一具體實施例的潛在網路釣魚電子郵件技術的高階概述之操作流程圖；

第4圖係根據本發明一具體實施例，例示在該使用者

透過非網頁郵件用戶存取帳戶後，用於警示使用者潛在網路釣魚電子郵件的綜合方法之流程圖；

第 5 圖係根據本發明一具體實施例，例示當透過非網頁郵件用戶存取時，用於管理一個或多個數位通訊的處理的綜合方法之流程圖。

第 6 圖係用於呈現文件夾之示例性使用者介面的例示性螢幕顯示屏，其映射至專用於存留潛在網路釣魚電子郵件的儲存位置；以及

第 7 圖係用於呈現警告訊息之示例性使用者介面的例示性螢幕顯示屏，其被顯現來替代揭露潛在網路釣魚電子郵件的內容。

【主要元件符號說明】

100 運算裝置
110 匯流排
112 記憶體
114 處理器
116 展示組件
118 輸入/輸出(I/O)埠
120 I/O 組件
122 電源供應器
200 系統架構
205 網路
210 來源
215 數位通訊
220 網頁伺服器
221 接收組件
222 管理組件
223 儲存組件
224 評估組件
230 資料儲存庫(結構化可

搜尋資料庫)

240 非網頁郵件用戶

241 映射組件

242 顯現組件

243 互動組件

250 使用者

260 用戶裝置

270 需求

300 流程圖

310 服務提供者

315、320、325、330、340、350、360、370、380 步驟

400 方法

410、420、430、440 區塊

500 方法

510、520、530、540、550 區塊

600 使用者介面

620 收件匣文件夾

630 網路釣魚郵件文件夾

640 文件夾列表

660、665、675 訊息

680 收件匣

700 警告訊息

710 警告發表

720 說明

730 內容

740 URL 鏈結

201044836

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：99112950

※ 申請日期：2010 年 4 月 23 日　　※IPC 分類：H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

在非網頁郵件用戶上下文中管理潛在的網路釣魚訊息 / MANAGING POTENTIALLY PHISHING MESSAGES IN A NON-WEB MAIL CLIENT CONTEXT

二、中文發明摘要：

本發明揭示在識別通訊為潛在網路釣魚電子郵件後，提供用於管理該等數位通訊(例如電子郵件與即時訊息)的處理之電腦可讀取媒體與電腦化方法。服務提供者係用來控制帳戶行為，其被指定給該等通訊之預期的接受者。控制該帳戶行為係說明於顯現使用者介面(User interface，“UI”)顯示屏的非網頁郵件伺服器上下文中，其無法由該服務提供者動態配置。在一種技術方案中，控制行為藉由將這些通訊聚集於分開的文件夾中，警示使用者識別為潛在網路釣魚之通訊的存在。在另一種技術方案中，控制行為藉由以警告訊息取代該等潛在網路釣魚通訊之內容，以便保護該使用者。此警告訊息視需要包括統一資源定位符(Uniform-resource locator，“URL”)，其鏈結至該使用者可觀看該等潛在網路釣魚通訊的原始內容之網頁瀏覽器。

三、英文發明摘要：

Computer-readable media and computerized methods

for governing treatment of digital communications (e.g., emails and instant messages) upon identifying the communications as potentially phishing emails are provided. A service provider is employed to control behavior of an account that is assigned to an intended recipient of the communications. Controlling the behavior of the account is described in the context of a non-web mail server that renders a UI display, which is not dynamically configurable by the service provider. In one solution, controlling behavior alerts a user to the presence of communications identified as potentially phishing by aggregating these communications in a separate folder. In another solution, controlling behavior facilitates protecting the user by replacing the content of the potentially phishing communications with a warning message. This warning message optionally includes a URL link to a web browser where the user can view the original content of the potentially phishing communications.

七、申請專利範圍：

1. 一個或多個電腦可讀取媒體，其具有電腦可執行指令體現於其上，當執行時，在一使用者透過一非網頁郵件用戶存取一帳戶後，執行用於警示該使用者一潛在網路釣魚電子郵件的一方法，該方法包含下列步驟：

在與該使用者相關的該帳戶處接收一數位通訊；

附隨識別該數位通訊為一潛在網路釣魚電子郵件，附加一元資料標籤於該數位通訊；

放置該標籤化數位通訊於一儲存位置中，其係專用於存留經識別為潛在網路釣魚電子郵件的數位通訊；以及

在該使用者透過該非網頁郵件用戶存取該帳戶後，呈現該儲存位置的一視覺代表項給該使用者，其中該視覺代表項提供一個或多個潛在網路釣魚電子郵件已抵達該使用者帳戶的一指示給該使用者。

2. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該方法更包含以下步驟：存留該附加的標籤，其在該等一個或多個電腦可讀取媒體上的一隔離列表中，與識別為該潛在網路釣魚電子郵件的該數位通訊相關，其中該隔離列表列舉已抵達該使用者帳戶的該等一個或多個潛在網路釣魚電子郵件之每一

者。

3. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該方法更包含以下步驟：施加過濾試探(filtering heuristics)，以查明該數位通訊是否係該潛在網路釣魚電子郵件，其中該潛在網路釣魚電子郵件係一訊息，其騙取引誘該使用者洩露個人資訊。

4. 如申請專利範圍第 3 項所述之一個或多個電腦可讀取媒體，其中該方法更包含以下步驟：在查明該數位通訊係該潛在網路釣魚電子郵件後，產生該專用的儲存位置。

5. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該數位通訊包含：一電子郵件訊息或一即時訊息之至少一者，且其中該數位通訊係自一來源接收，其係自該等一個或多個電腦可讀取媒體移除。

6. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該非網頁郵件用戶藉由顯現一使用者介面(UI)顯示屏給該使用者，提供該使用者存取至該帳戶，其中發表在該 UI 顯示屏上的元件並非由管理該

使用者帳戶的一服務提供者控制。

7. 如申請專利範圍第 6 項所述之一個或多個電腦可讀取媒體，其中該方法更包含以下步驟：透過該 UI 顯示屏，攔截該使用者所啟動之一請求，以執行關於該潛在網路釣魚電子郵件的一動作。

8. 如申請專利範圍第 7 項所述之一個或多個電腦可讀取媒體，該方法更包含下列步驟：

藉由檢查附加於該數位通訊的該元資料標籤，查明該使用者所啟動之請求係指向識別為該潛在網路釣魚電子郵件的該數位通訊；以及

查明於該請求中通訊的該動作是否係一受限的動作。

9. 如申請專利範圍第 8 項所述之一個或多個電腦可讀取媒體，其中該方法更包含下列步驟：

在查明該使用者所啟動之請求係指向識別為該潛在網路釣魚電子郵件的該數位通訊，且於該請求中通訊的該動作係一受限的動作時，阻止該動作的執行；以及

回應該請求而傳送一操作失效指示至該非網頁

郵件用戶。

10. 如申請專利範圍第 9 項所述之一個或多個電腦可讀取媒體，其中該受限的動作包含：一回應指令、一對所有指令的回應、或一前向指令之至少一者。

11. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該動作包含：一指令，其試圖自該專用的儲存位置移動該數位通訊至一儲存位置，其持有識別為合法的數位通訊，其中該方法更包含下列步驟：

檢測源自於該非網頁郵件用戶的一同步操作；

查明該動作係該試圖移動指令；以及

不允許該數位通訊在該專用的儲存位置外部的移動。

12. 如申請專利範圍第 1 項所述之一個或多個電腦可讀取媒體，其中該方法更包含下列步驟：

呈現該儲存位置的該視覺代表項為一文件夾，其位在由該非網頁郵件用戶所顯現之該 UI 顯示屏上；以及

在接收該文件夾的一選擇後，呈現該等一個或多個潛在網路釣魚電子郵件的代表項，其已抵達該使用

者帳戶且存留於該專用的儲存位置。

13. 如申請專利範圍第 12 項所述之一個或多個電腦可讀取媒體，其中該方法更包含下列步驟：

撤銷納入該等一個或多個潛在網路釣魚電子郵件的內容中之統一資源定位符(URL)鏈結，其係存留於該專用的儲存位置；

接收該等一個或多個潛在網路釣魚電子郵件的該等代表項之一選擇；以及

傳遞該等一個或多個選定潛在網路釣魚電子郵件的該內容至用於顯現的該非網頁郵件用戶。

14. 一種電腦化方法，其由容納於一伺服器上的一服務提供者實行，且用於當透過一非網頁郵件用戶存取時，管理一個或多個數位通訊的處理，該方法包含下列步驟：

在與該數位通訊的一預期的接受者相關的一帳戶處接收一數位通訊後，施加過濾試探以判定該數位通訊是否係一未經要求的訊息或一合法的訊息；

當判定該數位通訊係一未經要求的訊息時，標示該數位通訊為危險的；

以一警告訊息取代該危險的數位通訊；

指示該非網頁郵件用戶，以顯露該危險的數位通訊的一代表項於一使用者介面(UI)顯示屏中所顯現之一列表中，其中該列表包括：經判定為合法訊息的數位通訊之一個或多個代表項，且其中由該非網頁郵件用戶所顯現之該 UI 顯示屏，無法由管理該使用者帳戶的該服務提供者再配置；以及

在接收該危險的數位通訊的該代表項之一使用者所啟動之選擇後，傳遞指令至該非網頁郵件用戶，以呈現該警告訊息給該接收者，並阻擋揭露該危險的數位通訊的內容。

15. 如申請專利範圍第 14 項所述之電腦化方法，更包含以下步驟：存留該危險的數位通訊於一儲存位置中，其持有經判定為合法通訊的一個或多個數位通訊。

16. 如申請專利範圍第 14 項所述之電腦化方法，其中該警告訊息傳遞該危險的數位通訊係識別為一潛在網路釣魚電子郵件的一通知，且其中該警告訊息透過一網頁瀏覽器提供指示來存取該危險的數位通訊的內容。

17. 如申請專利範圍第 14 項所述之電腦化方法，其中該警告訊息包括：鏈結至一網頁瀏覽器的一統一資源定位符(URL)，其在選擇後，允許該接受者存取該危險的數位通訊的內容。

18. 一個或多個電腦可讀取媒體，其具有電腦可執行指令體現於其上，當執行時，透過由一非網頁郵件用戶所顯現之一使用者介面(UI)顯示屏，執行用於通知一使用者一潛在網路釣魚電子郵件已抵達該使用者的一帳戶的一方法，該方法包含下列步驟：

產生一儲存位置，其專用於存留識別為潛在網路釣魚電子郵件的一個或多個數位通訊；

指示該非網頁郵件用戶來顯現一文件夾於該 UI 顯示屏內，其中該文件夾映射至該專用的儲存位置；

檢測一指令，其由該使用者實行以存取該文件夾；以及

指示該非網頁郵件用戶以顯現該等一個或多個經識別的數位通訊之代表項，其中該等代表項包括：關於該等一個或多個經識別的數位通訊之內容的元資料。

19. 如申請專利範圍第 18 項所述之一個或多個電腦可讀

取媒體，其中指示該非網頁郵件用戶以顯現一文件夾於該 UI 顯示屏內之步驟，包含以下步驟：指示該非網頁郵件用戶以顯現該文件夾於一列表中，其包括：映射至存留一個或多個識別為合法電子郵件的數位通訊之儲存位置的其他文件夾，藉此在視覺上將該等潛在網路釣魚電子郵件與該等合法電子郵件分開。

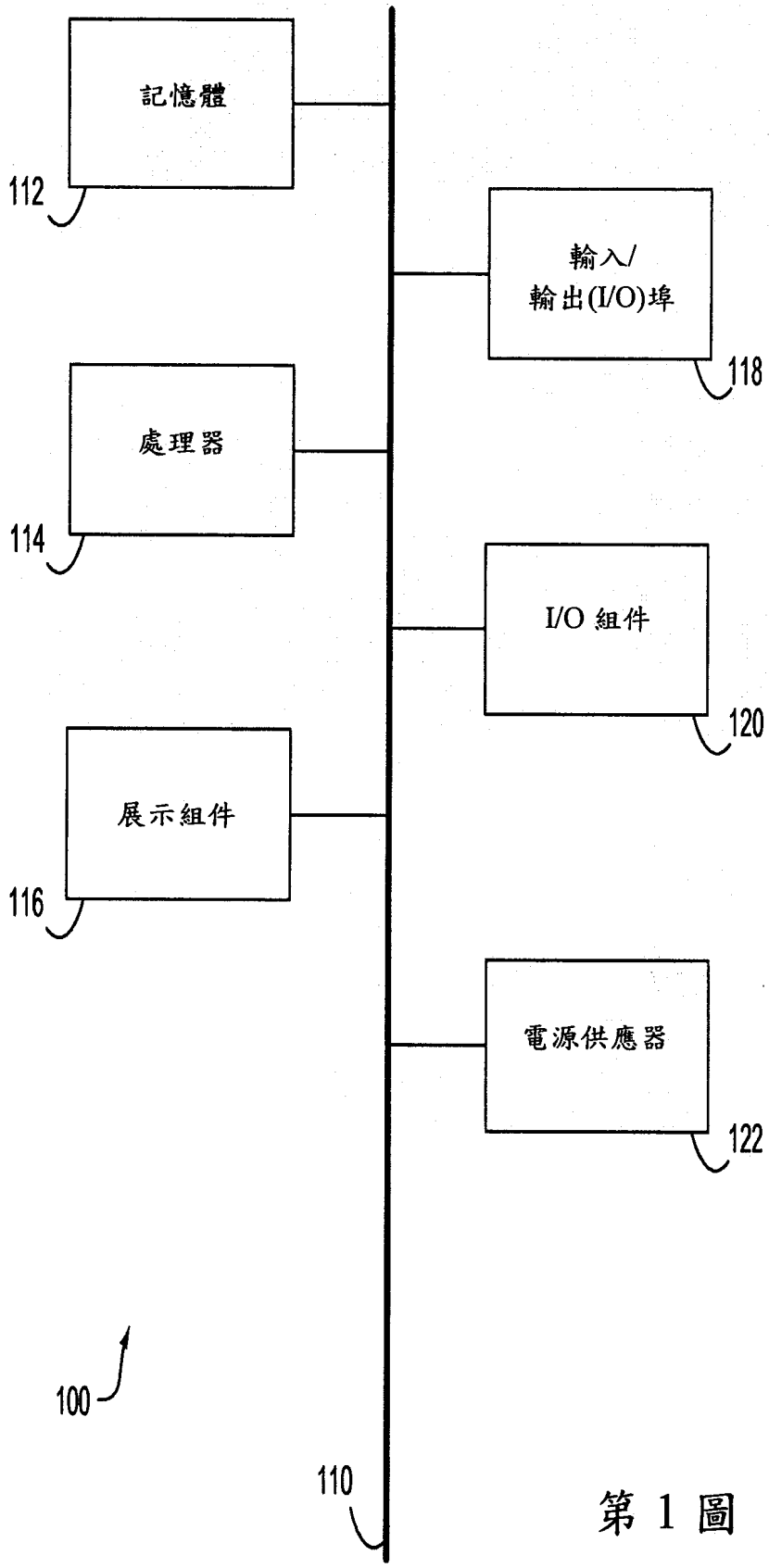
20. 如申請專利範圍第 18 項所述之一個或多個電腦可讀取媒體，其中該方法更包含下列步驟：

接收由該使用者所啟動之一動作，其指向該等一個或多個經識別的數位通訊；

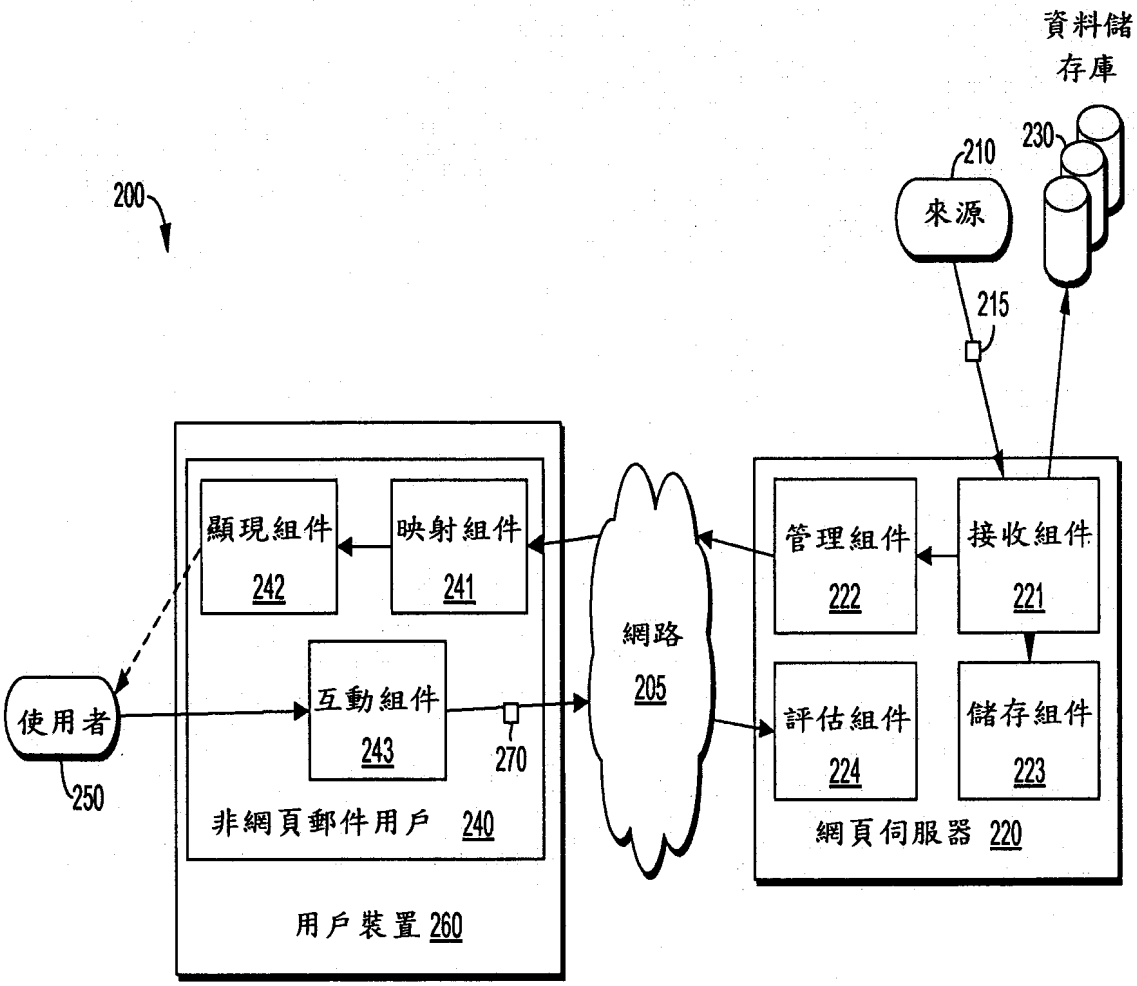
藉由阻止該動作的執行，使該使用者所啟動之動作失效；以及

傳送一操作失效指示至該非網頁郵件用戶，其中該操作失效指示通知該動作之失效。

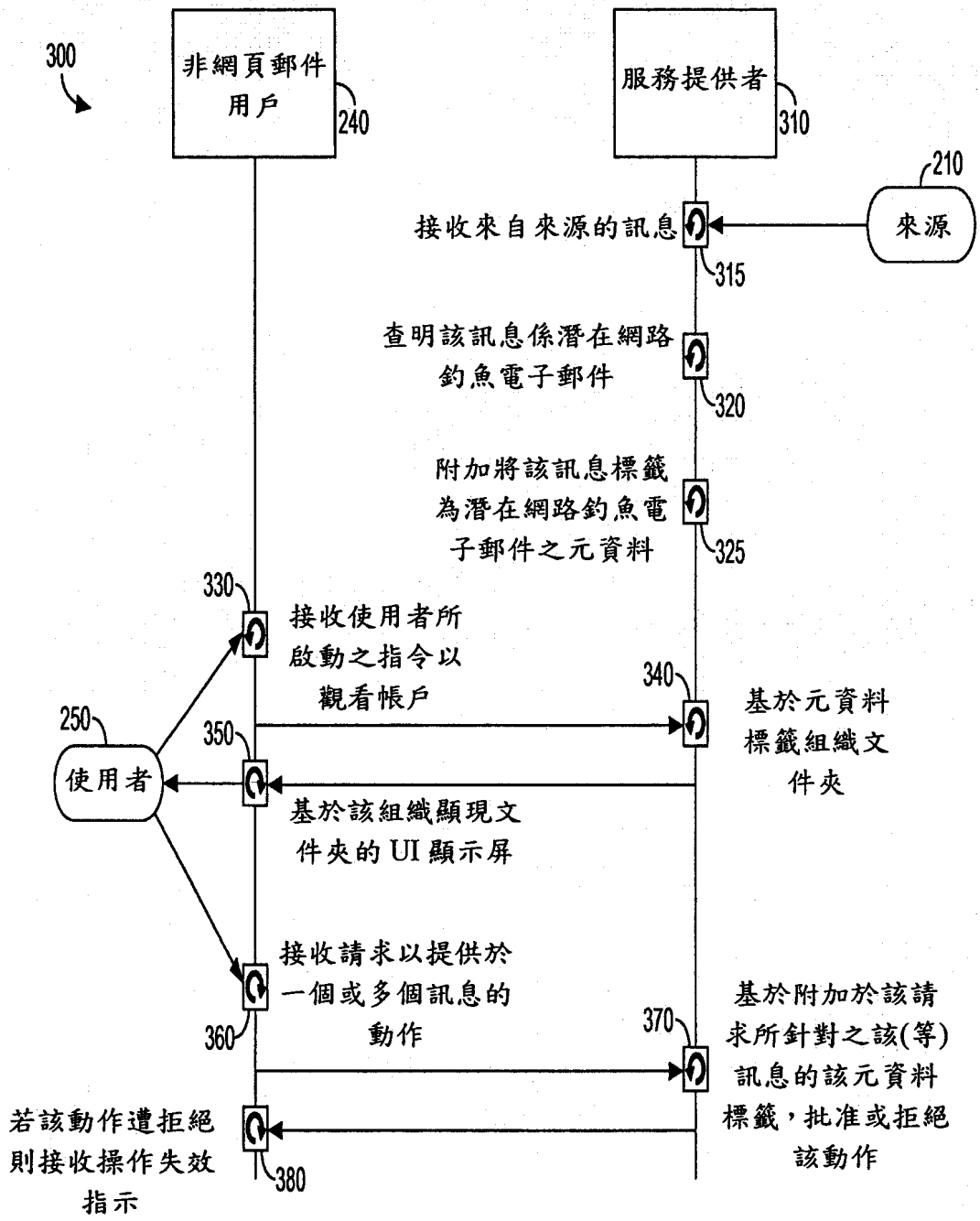
八、圖式：


記憶體
112
處理器
114
展示組件
116
輸入/
輸出(I/O)埠
118
I/O 組件
120
電源供應器
122
100
110

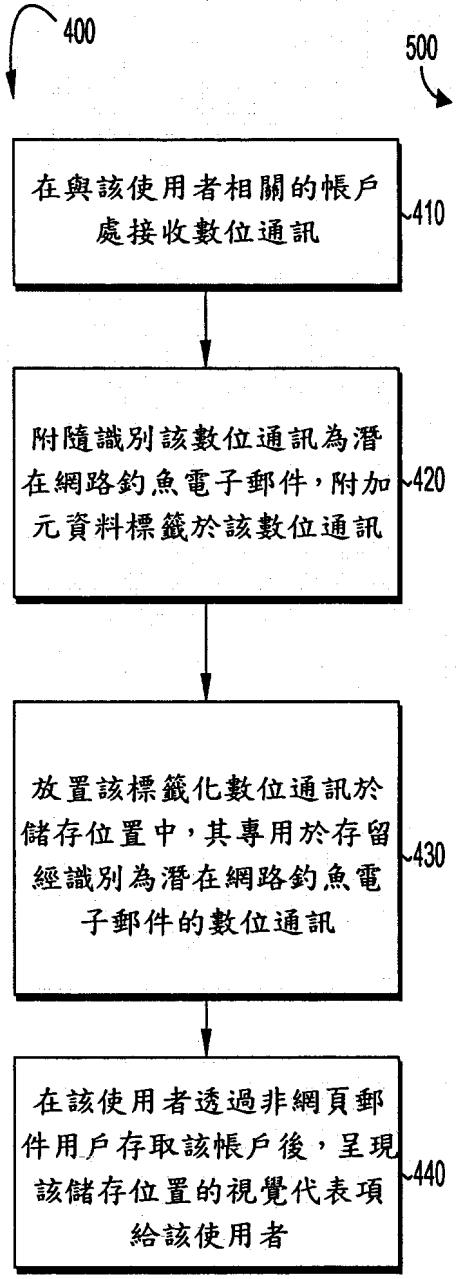
第 1 圖


資料儲
存庫
230
210
來源
200
215
顯現組件
242
映射組件
241
管理組件
222
接收組件
221
網路
205
互動組件
243
270
使用者
250
評估組件
224
儲存組件
223
非網頁郵件用戶 240
網頁伺服器 220
用戶裝置 260

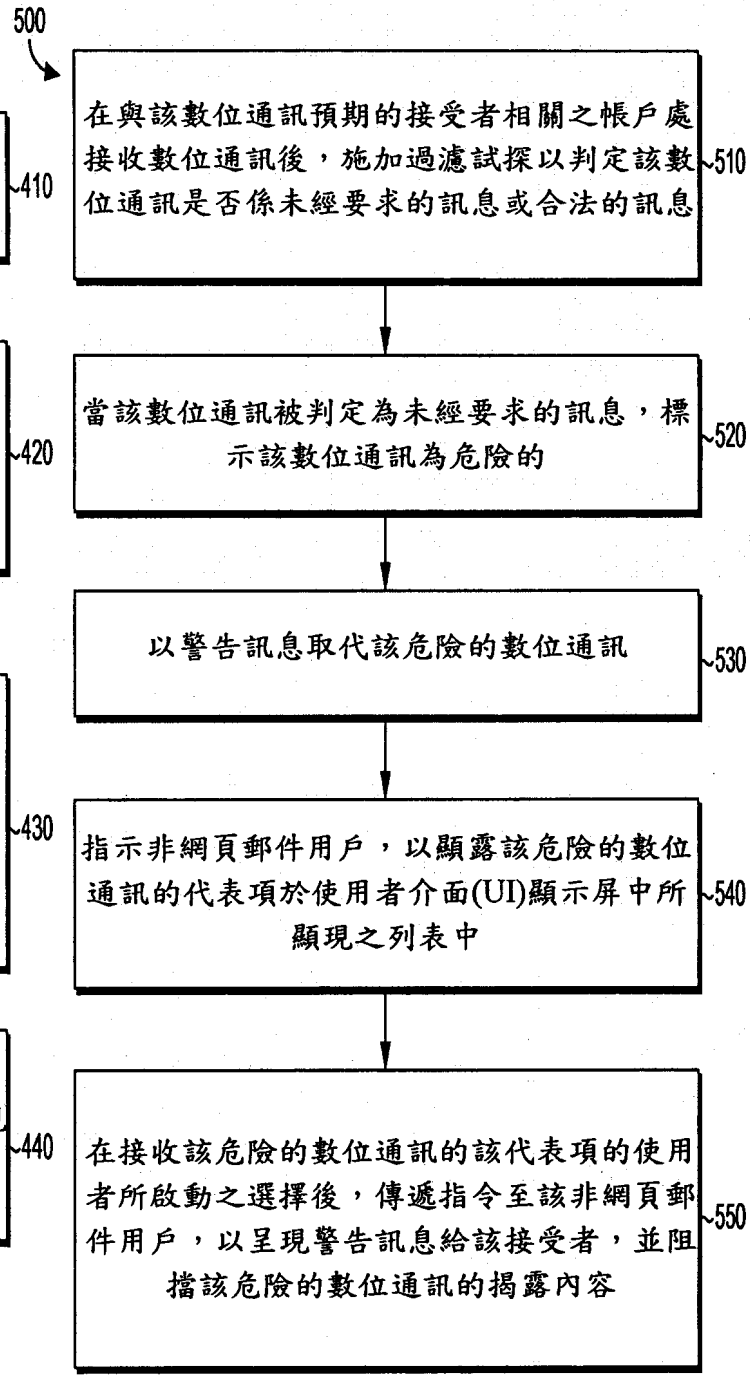
第 2 圖


300
非網頁郵件用戶
240
服務提供者
310
210
來源
接收來自來源的訊息
315
查明該訊息係潛在網路釣魚電子郵件
320
附加將該訊息標籤為潛在網路釣魚電子郵件之元資料
325
330
接收使用者所啟動之指令以觀看帳戶
340
基於元資料標籤組織文件夾
250
使用者
350
基於該組織顯現文件夾的UI顯示屏
接收請求以提供於一個或多個訊息的動作
360
370
基於附加於該請求所針對之該(等)訊息的該元資料標籤，批准或拒絕該動作
若該動作遭拒絕則接收操作失效指示
380

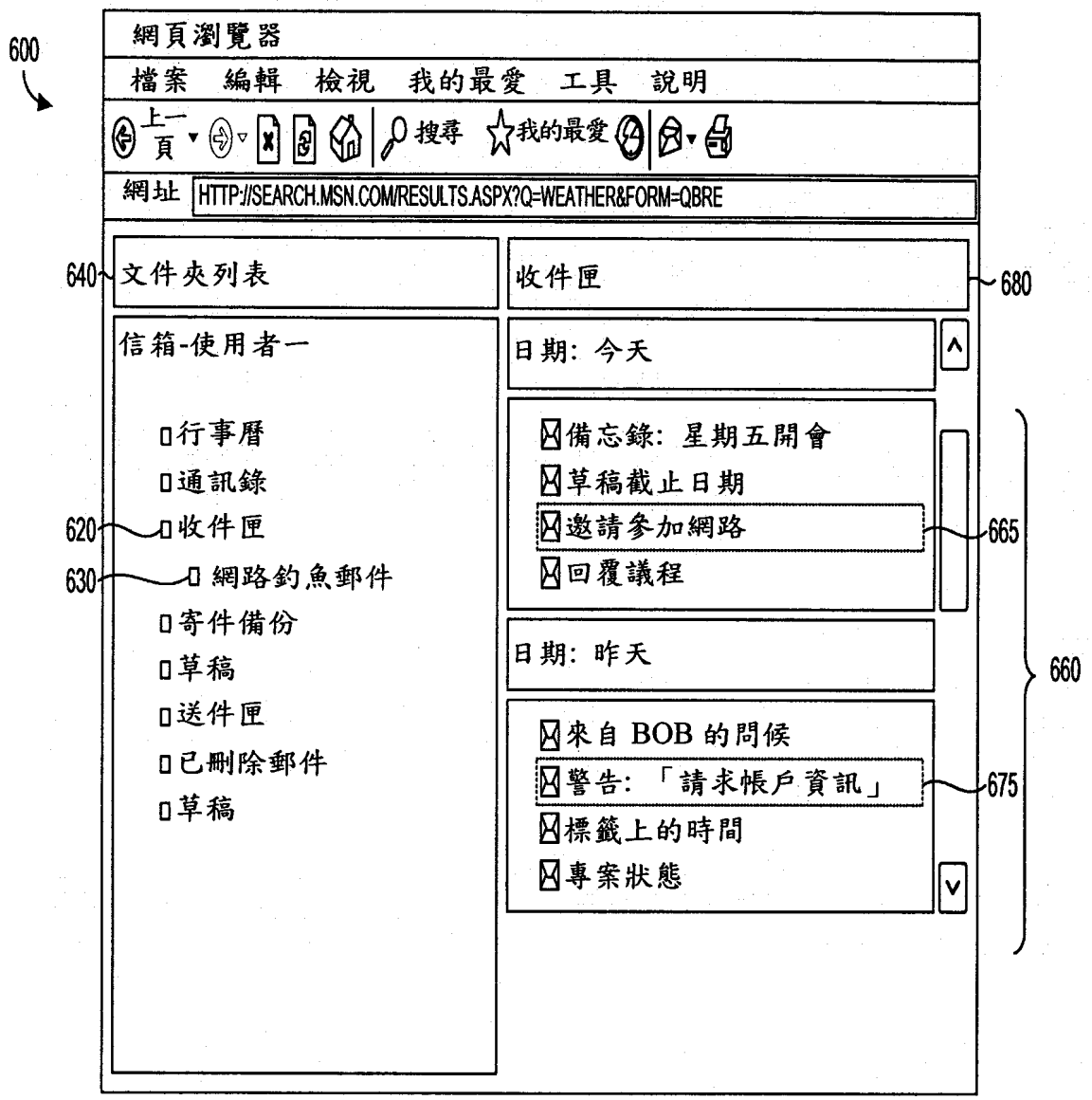
第 3 圖


400
在與該使用者相關的帳戶處接收數位通訊
410
附隨識別該數位通訊為潛在網路釣魚電子郵件，附加元資料標籤於該數位通訊
420
放置該標籤化數位通訊於儲存位置中，其專用於存留經識別為潛在網路釣魚電子郵件的數位通訊
430
在該使用者透過非網頁郵件用戶存取該帳戶後，呈現該儲存位置的視覺代表項給該使用者
440

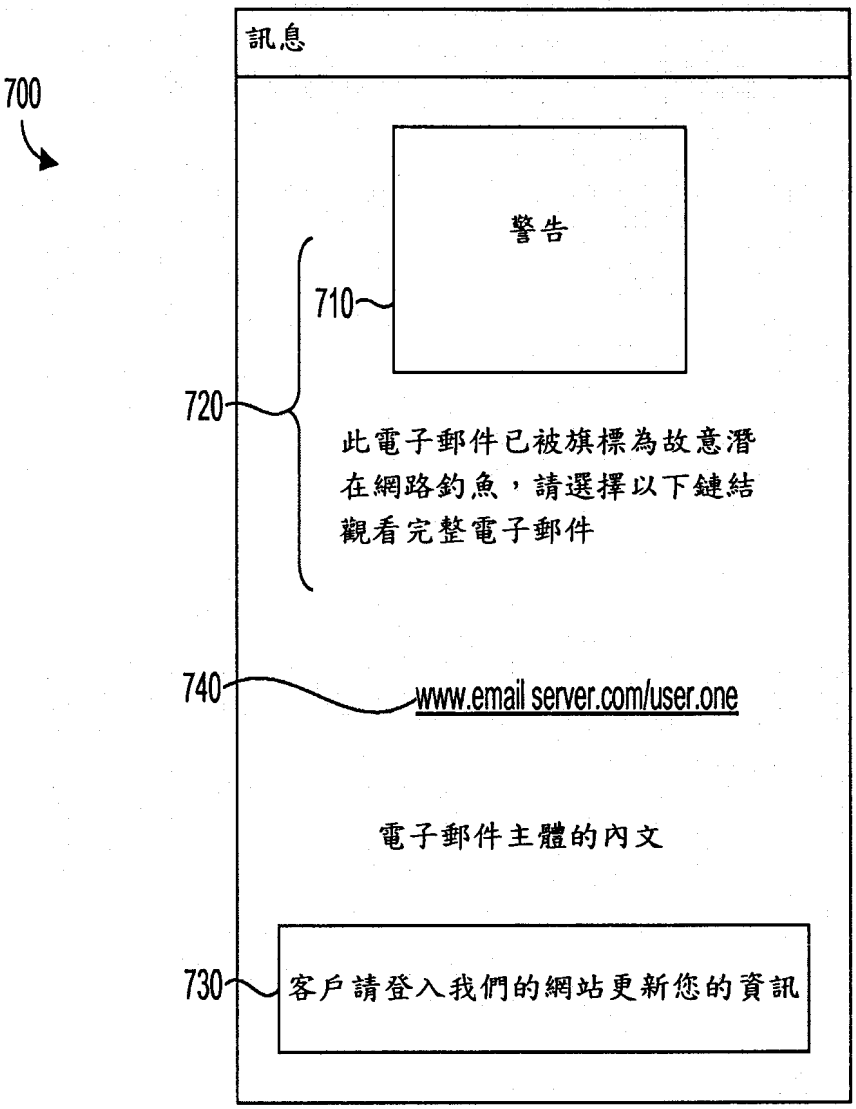
第 4 圖


500
在與該數位通訊預期的接受者相關之帳戶處接收數位通訊後，施加過濾試探以判定該數位通訊是否係未經要求的訊息或合法的訊息
510
當該數位通訊被判定為未經要求的訊息，標示該數位通訊為危險的
520
以警告訊息取代該危險的數位通訊
530
指示非網頁郵件用戶，以顯露該危險的數位通訊的代表項於使用者介面(UI)顯示屏中所顯現之列表中
540
在接收該危險的數位通訊的該代表項的使用者所啟動之選擇後，傳遞指令至該非網頁郵件用戶，以呈現警告訊息給該接受者，並阻擋該危險的數位通訊的揭露內容
550

第 5 圖


600
網頁瀏覽器
檔案 編輯 檢視 我的最愛 工具 說明
上一頁
搜尋
我的最愛
網址
HTTP://SEARCH.MSN.COM/RESULTS.ASPX?Q=WEATHER&FORM=QBRE
640
文件夾列表
收件匣
680
信箱-使用者一
行事曆
通訊錄
620
收件匣
630
網路釣魚郵件
寄件備份
草稿
送件匣
已刪除郵件
草稿
日期: 今天
備忘錄: 星期五開會
草稿截止日期
邀請參加網路
665
回覆議程
日期: 昨天
660
來自 BOB 的問候
警告: 「請求帳戶資訊」
675
標籤上的時間
專案狀態

第 6 圖


訊息
700
警告
710
720
此電子郵件已被旗標為故意潛在網路釣魚，請選擇以下鏈結觀看完整電子郵件
740
www.email server.com/user.one
電子郵件主體的內文
730
客戶請登入我們的網站更新您的資訊

第 7 圖

四、指定代表圖：

(一)本案指定代表圖為：第（2）圖。

(二)本代表圖之元件符號簡單說明:

200 系統架構

205 網路

210 來源

215 數位通訊

220 網頁伺服器/裝置

221 接收組件

222 管理組件

223 儲存組件

224 評估組件

230 資料儲存庫

240 非網頁郵件用戶

241 映射組件

242 顯現組件

243 互動組件

250 使用者

260 用戶裝置

270 需求

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無