November 2023

SYSTEM AND METHOD FOR DYNAMIC LINK ACTIVATION IN EMAIL MESSAGES FOR PHISHING PREVENTION

ALOK ROY
VISA

“SYSTEM AND METHOD FOR DYNAMIC LINK ACTIVATION IN EMAIL MESSAGES FOR PHISHING PREVENTION”

VISA

INVENTOR:

ALOK ROY

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to the field of cyber security, but not exclusively, to a system and a method for dynamic link activation in email messages to prevent phishing attacks.

BACKGROUND

[0002] Phishing is a type of social engineering attack, which seeks to trick victims into disclosing account credentials or other sensitive information through a fraudulent message, for example, an email which leads to a website that impersonates a real organization. In a phishing attack, an individual, for example, a person, an employee of a company, or an individual of a computing device, receives a message commonly in the form of an e-mail, directing the individual to perform an action. The action may be opening an e-mail attachment or downloading the attachments or a malicious link.

[0003] There may be scenarios where the user receives an email from an attacker (for example, from an individual, disguised as a trusted source, using a computing device to perform a malicious act on another computer device user), which contains harmful and/or malicious links. The user may end up revealing personal information, financial information, and login credentials by clicking such links, which include links to fake websites that mimic legitimate sites. In other words, by opening an attachment via an embedded link in an e-mail forwarded to a webpage, which is made to look like an authentic webpage, the user might be deceived into submitting his/her username, password, or other sensitive information to an attacker.

[0004] The traditional approaches to phishing prevention have limitations in enabling users to safely interact with legitimate links. Hence, there is a need for a system to enhance email security and reduce unauthorized access to sensitive information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system

and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0006] **FIG. 1** illustrates an exemplary system architecture which may be configured for dynamic link activation in email messages to prevent phishing attacks, in accordance with some embodiments of the present disclosure.

[0007] **FIG. 2** illustrates an exemplary flow diagram of a method for dynamic link activation in email messages to prevent phishing attacks, in accordance with some embodiments of the present disclosure.

[0008] **FIG. 3a** shows an exemplary email overview, in accordance with some embodiments of the present disclosure.

[0009] **FIG. 3b** shows an exemplary view of link details on a user interface, in accordance with some embodiments of the present disclosure.

[0010] **FIG. 3c** shows an exemplary view displaying user feedback options on a user interface, in accordance with some embodiments of the present disclosure.

[0011] **FIG. 4** is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0012] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0013] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0014] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0015] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0016] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0017] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0018] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0019] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit can receive information directly or indirectly from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication

connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0020] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to communicate with directly or indirectly or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers.

[0021] As used herein, “interface” refers to a generated display, such as one or more Graphical User Interfaces (GUIs) with which a user may interact, either directly or indirectly (for example, through a keyboard, mouse, touchscreen, and so on).

[0022] As used herein, the term "user" may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or user devices.

[0023] As used herein, the term "server computer" is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0024] As used herein, the term "processor" may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include CPU comprises at least one high-

speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale, and/or the like processor(s).

[0025] As used herein, the term "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0026] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0027] **FIG. 1** illustrates an exemplary environment 100 of a link activation system 107, which is configured for dynamic link activation in email messages to prevent phishing attacks. In an embodiment, environment 100 for link activation in email messages includes, without limitation, an input unit 101, an email analysis unit 103, the link activation system 107, a user interface 109, and a user behavior learning unit 111. The input unit 101 is associated with a user/customer. The input unit 101 may refer to a device which is operated by the user. For example, the input unit may be any computing device such as, without limiting to, tablet computers, netbooks, smartphones, or laptops. The email analysis unit 103, the user behavior learning unit 111, and the link activation system 107 may be connected via a predefined communication network 105. Such a communication network 105 may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (for example, using Wireless Application Protocol), the Internet, and the like.

[0028] Consider a scenario, when the input unit 101, associated with the user or an employee, of a company receives incoming emails from an individual or a user’s computing device. For

example, emails are received from a well-known website or from the user's bank. In an embodiment, the email analysis unit 103 analyzes the received emails and identifies them as suspicious emails, for example, when there are any inconsistencies in the sender's domain. After detecting the suspicious emails, the email analysis unit 103 sends those suspicious emails to the link activation system 107. Thereafter, the link activation system 107 automatically disables all the embedded links within the suspicious email and generates a user interface 109. When the user opens the email, they are presented with the user interface 109, which displays disabled links and one or more information. The one or more information includes, without limiting to, sender identity, destination identity or a Universal Resource Locater (URL). Subsequently, the user reviews the disabled links and decides to enable the link, if the user decides that the links are safe and lead to a genuine site, such as the bank's official website or other well-known websites. Further, the user behavior learning unit 111 monitors the interactions between the user interface 109 and the link activation system 107 and refines rules for the email analysis unit 103. For example, the user behavior learning unit 111 monitors the interactions and learns that the user has confidence in links originating from the bank's domain. As a result, the method disclosed in the present disclosure aims to identify, as well as mitigate suspicious emails or email messages and reduce the risk of phishing attacks.

[0029] In an embodiment, the link activation system 107 may include one or more processors 113, an Input/Output (I/O) interface 115, and a memory 117. In some embodiments, the memory 117 may be communicatively coupled to the one or more processors 113. The memory 117 may be configured to store instructions, when executable by the one or more processors 113, enable the link activation system 103 to perform dynamic link activation in email messages to prevent phishing attacks. In an embodiment, the memory 117 may include one or more modules 119 and data 121. The one or more modules 119 may be configured to perform the required processing steps using the data 121. In an embodiment, each of the one or more modules 119 may be a hardware unit, which may be present outside the memory 117 and externally coupled with the link activation system 107. The link activation system 107 may be implemented in a variety of computing systems, such as a laptop computer, a desktop computer, a Personal Computer (PC), a notebook, a smartphone, a tablet, e-book readers, a server, a network server, a cloud-based server and the like. In some embodiments, the link activation system 107 may be implemented in a server configured to perform dynamic link activation in email messages. In an embodiment, such a server may be a dedicated server or maybe a cloud-based server.

[0030] **FIG. 2** illustrates an exemplary flow diagram of a method for dynamic link activation in email messages to prevent phishing attacks, in accordance with some embodiments of the present disclosure.

[0031] In an embodiment, at block 201, the method comprises receiving, by an input unit 101, incoming emails from a user's computing device. Thereafter, in block 203, the method comprises analyzing, by an email analysis unit 103, the received emails to detect suspicious emails and sending the detected suspicious emails to a link activation system 107 via a network 105. The email analysis unit 103 is configured for performing an initial analysis of incoming emails. The email analysis unit 103 employs various techniques, models, and rules to detect suspicious emails or malicious emails. Subsequently, in block 205, the method comprises disabling, by the link activation system 107, all the embedded links in suspicious emails. For example, when a suspicious email is detected, the link activation system 107 disables all embedded links.

[0032] In an embodiment, the method comprises generating a user interface 109 which allows users to review information which is related to disabled links at block 207. The user interface 109 acts as a user-friendly interface for users to interact with the link activation system 107. For example, **FIG. 3a** demonstrates, without limiting to, how the suspicious emails may be displayed at the user interface 109. **FIG. 3a** displays essential information related to the email, including the sender's name and sender's email address which helps users quickly assess the email's source. The subject link is provided for context, and the date along time of receipt are displayed to indicate when the email has arrived.

For example: From: [Sender Name] <sender@example.com> Subject: [Email Subject] Received: [Date and Time]

[0033] Further, the list of all disabled links present in the emails is shown in **FIG. 3a**. For each link, the URL text and the destination URL are shown, allowing the user to understand where the link leads before enabling it. If the user ticks the check box of any of the links, a pop-up/prompt window may appear with additional one or more details as shown in **FIG. 3b** for review and final confirmation to proceed or cancel. The one or more details include, without

limiting to, the destination URL, and risk level (for example, ‘safe’ or ‘suspicious’ or ‘known phishing site’). The user may enable the links that are trusted and disable the links which are marked as ‘suspicious’ for their security. Furthermore, the user interface 109 may include a “User Guidance” option which includes best practices for identifying phishing emails along with how to safely activate links, and a “Help and Support” option which is used to find resources to learn more about link activation system 107, email security and contact support in case the user encounters issues or needs assistance. The “Help and Support” may also include Frequently Asked Questions (FAQs), links to additional materials, and so on.

[0034] In an embodiment, at block 209, the method comprises activating the trusted links by the user based on the information provided in the user interface 109. That is, the user reviews the destination URL and sender identity displayed in the user interface. After confirming the legitimacy, the user selectively activates the link, safely proceeding to the bank’s website. Upon activating links, the user may notice the presence of a checkbox or option to provide feedback related to the suspicious email and links. Thereafter, once the user clicks on the checkbox or option, a dialogue box may appear (as shown in **FIG. 3c**), prompting the user to enter feedback or comments or a small report on suspicious emails, phishing attempts, or any other issues.

[0035] Further, at block 211, the method comprises monitoring, by a user behavior learning unit 111, the user interface 109 interactions as well as the link activation system 107 and refining the email analysis unit 103. The user behavior unit 111 is designed to continuously learn from the interaction between the user and the user interface 109 and the feedback received from the user. As a result, the method described in the present disclosure helps in improving the system's accuracy in identifying suspicious emails in the future.

Advantages of the present invention:

[0036] In an embodiment, the present disclosure method helps in reducing the risk of users falling victim to phishing attacks inadvertently.

[0037] In an embodiment, the present disclosure method improves the ability to differentiate between legitimate and malicious emails and helps control over-link activation.

[0038] In an embodiment, the present disclosure method improves the ability to accurately identify phishing attempts.

[0039] In an embodiment, the present disclosure method protects the users from cyber-attacks by disabling the links and providing an interface for selective enabling.

General computer system:

[0040] **FIG. 4** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0041] In an embodiment, **FIG. 4** illustrates a block diagram of an exemplary computer system 400 for implementing embodiments consistent with the present disclosure. In some embodiments, the computer system 400 may be a link activation system 107 for dynamic link activation in email messages to prevent phishing attacks. In an embodiment, the computer system 400 may include a central processing unit ("CPU" or "processor") 402. The processor 402 may include at least one data processor for executing processes in Virtual Storage Area Network. The processor 402 may include at least one data processor for executing program components for executing user or system-generated business processes. The processor 402 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0042] In some embodiments, the processor 402 may be disposed in communication with one or more Input/Output (I/O) devices (412 and 413) via I/O interface 401. The I/O interface 401 may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE-1394 high-speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.11b/g/n/x, Bluetooth, cellular, for example, Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System for Mobile communications (GSM), Long-Term Evolution (LTE), Worldwide Interoperability for Microwave access (WiMax), or the like, etc. Using the I/O interface 401, the computer system 400 may communicate with one or more I/O devices such as input devices 412 and output devices 413. For example, the input devices 412 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 413 may be a printer, fax machine,

video display (e.g., Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), plasma, Plasma Display Panel (PDP), Organic Light-Emitting Diode display (OLED) or the like), audio speaker, etc.

[0043] In some embodiments, the processor 402 may be disposed in communication with a communication network 409 via a network interface 403. The network interface 403 may communicate with the communication network 409. The network interface 403 may employ connection protocols including, without limitation, direct connect, Ethernet (for example, twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 409 may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (for example, using Wireless Application Protocol), the Internet, etc. Using the network interface 403 and the communication network 409, the computer system 400 may communicate with a database 414, which may be the enrolled templates database 413. The network interface 403 may employ connection protocols include, but not limited to, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0044] In some embodiments, the communication network 409 includes, but is not limited to, a direct interconnection, a Peer-to-Peer (P2P) network, Local Area Network (LAN), Wide Area Network (WAN), wireless network (for example, using Wireless Application Protocol), the Internet, Wi-Fi, and such. The communication network 409 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 409 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0045] In some embodiments, the processor 402 may be disposed of in communication with a memory 405 (for example, RAM, ROM, etc. not shown in FIG. 4) via a storage interface 404. The storage interface 404 may connect to memory 405 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fiber channel, Small Computer Systems Interface (SCSI), etc. The memory

drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0046] In some embodiments, the memory 405 may store a collection of program or database components, including, without limitation, a user interface 406, an operating system 407, a web browser 408, and so on. In some embodiments, computer system 400 may store user/application data, such as the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0047] In some embodiments, the operating system 407 may facilitate resource management and operation of the computer system 400. Examples of operating systems include, without limitation, Apple Macintosh OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat, Ubuntu, K-Ubuntu, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows (XP™, Vista/7/8, etc.), Apple iOS, Google Android, BlackBerry operating system (OS), or the like. The User Interface 406 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 400, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, JavaScript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0048] In some embodiments, the computer system 400 may implement web browser 408 stored program components. Web browser 408 may be a hypertext viewing application, such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 408 may utilize facilities such as AJAX, DHTML, Adobe Flash, JavaScript, Application Programming Interfaces (APIs), etc.

[0049] In some embodiments, the computer system 400 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like.

[0050] In some embodiments, the computer system 400 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE® MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0051] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0052] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer-readable medium”, where a processor may read and execute the code from the computer-readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer-readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs,

PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0053] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0054] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0055] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or

circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0056] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

"SYSTEM AND METHOD FOR DYNAMIC LINK ACTIVATION IN EMAIL MESSAGES FOR PHISHING PREVENTION"

ABSTRACT

The present disclosure relates to a system and a method for dynamic link activation in email messages to prevent phishing attacks. The present disclosure suggests receiving incoming emails from a user's computing device. Thereafter, the received emails are analyzed to detect suspicious emails, and the detected suspicious emails are sent to a link activation system. Upon receiving suspicious emails, the link activation system disables all embedded links in the suspicious email and generates a user interface. The user interface allows users to review information related to disabled links. Subsequently, the user may choose to activate or deactivate the links based on the information related to the disabled links. Further, the present disclosure suggests monitoring user interface interactions as well as the link activation system and refining an email analysis unit to make accurate prediction of the suspicious emails.

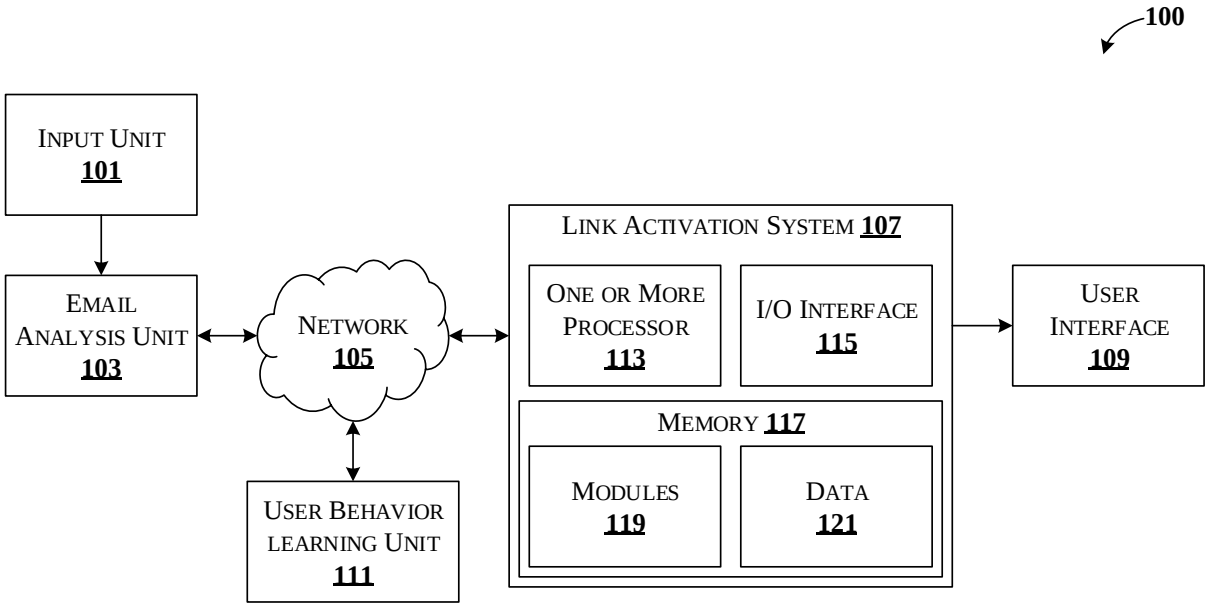

100
INPUT UNIT
101
EMAIL ANALYSIS UNIT
103
NETWORK
105
USER BEHAVIOR LEARNING UNIT
111
LINK ACTIVATION SYSTEM 107
ONE OR MORE PROCESSOR
113
I/O INTERFACE
115
MEMORY 117
MODULES
119
DATA
121
USER INTERFACE
109

FIG. 1

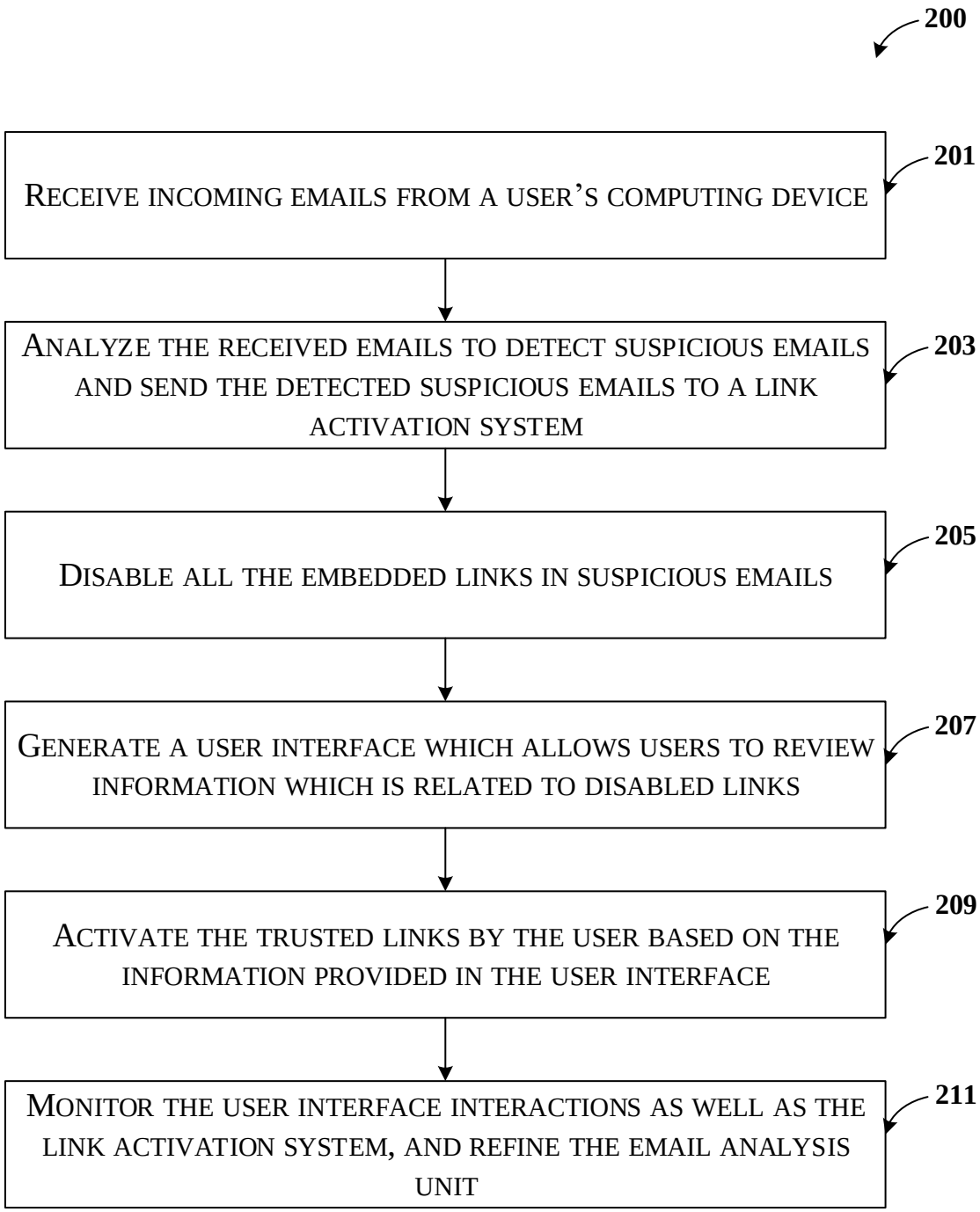
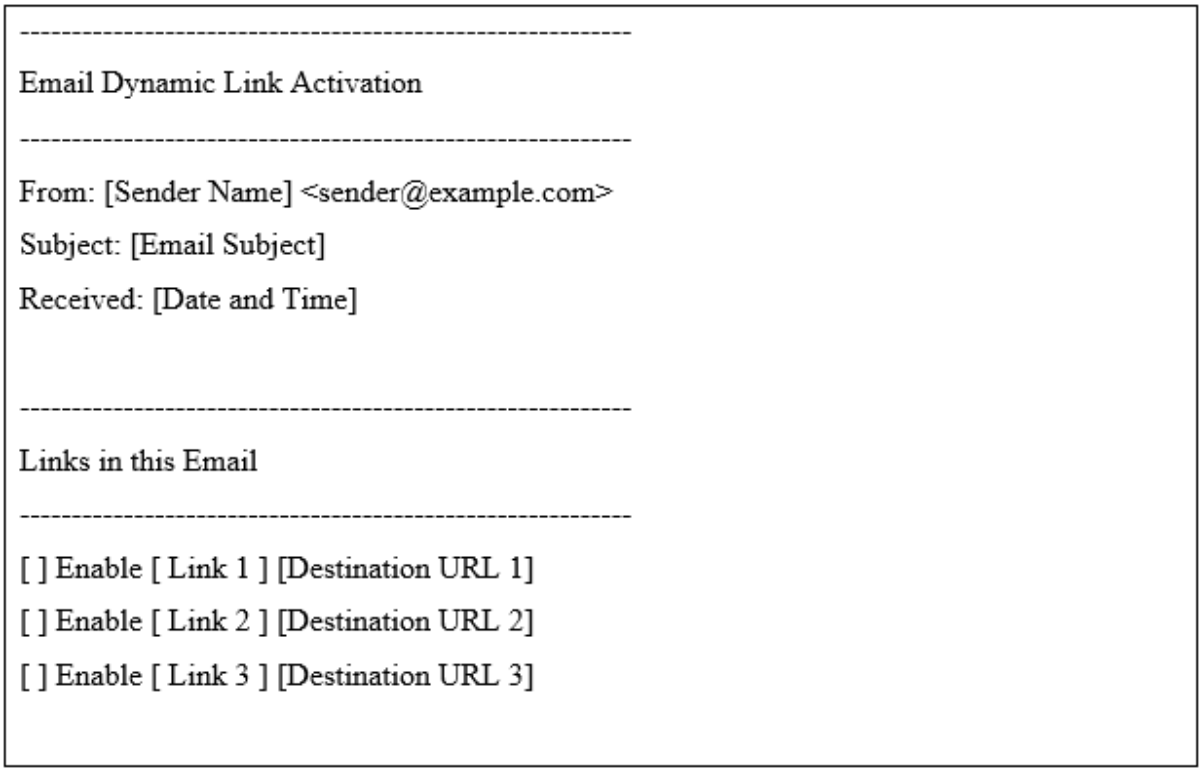

200
RECEIVE INCOMING EMAILS FROM A USER'S COMPUTING DEVICE
201
ANALYZE THE RECEIVED EMAILS TO DETECT SUSPICIOUS EMAILS AND SEND THE DETECTED SUSPICIOUS EMAILS TO A LINK ACTIVATION SYSTEM
203
DISABLE ALL THE EMBEDDED LINKS IN SUSPICIOUS EMAILS
205
GENERATE A USER INTERFACE WHICH ALLOWS USERS TO REVIEW INFORMATION WHICH IS RELATED TO DISABLED LINKS
207
ACTIVATE THE TRUSTED LINKS BY THE USER BASED ON THE INFORMATION PROVIDED IN THE USER INTERFACE
209
MONITOR THE USER INTERFACE INTERACTIONS AS WELL AS THE LINK ACTIVATION SYSTEM, AND REFINE THE EMAIL ANALYSIS UNIT
211

FIG. 2



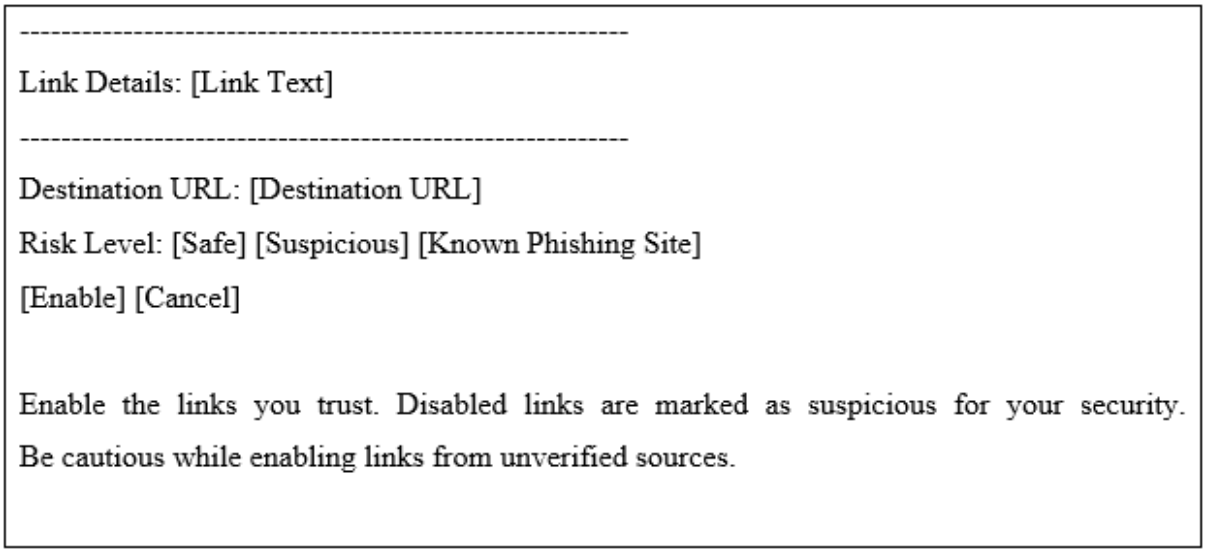
Email Dynamic Link Activation

From: [Sender Name] <sender@example.com>
Subject: [Email Subject]
Received: [Date and Time]

Links in this Email

[ ] Enable [Link 1] [Destination URL 1]
[ ] Enable [Link 2] [Destination URL 2]
[ ] Enable [Link 3] [Destination URL 3]

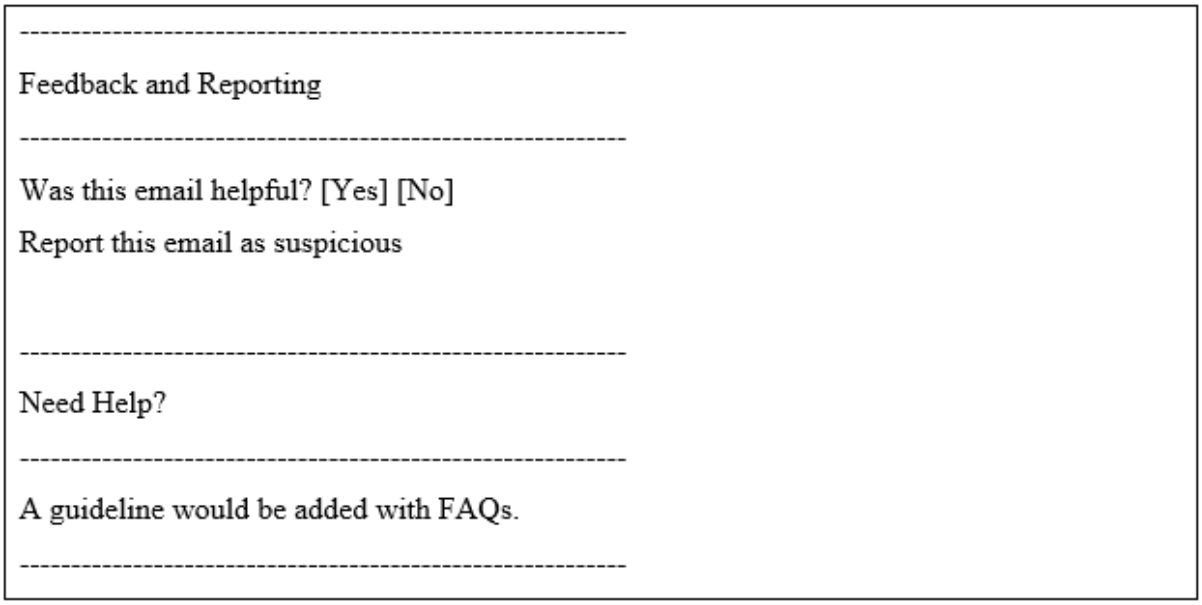
FIG. 3a



Link Details: [Link Text]

Destination URL: [Destination URL]
Risk Level: [Safe] [Suspicious] [Known Phishing Site]
[Enable] [Cancel]
Enable the links you trust. Disabled links are marked as suspicious for your security. Be cautious while enabling links from unverified sources.

FIG. 3b



Feedback and Reporting

Was this email helpful? [Yes] [No]
Report this email as suspicious

Need Help?

A guideline would be added with FAQs.

FIG. 3c

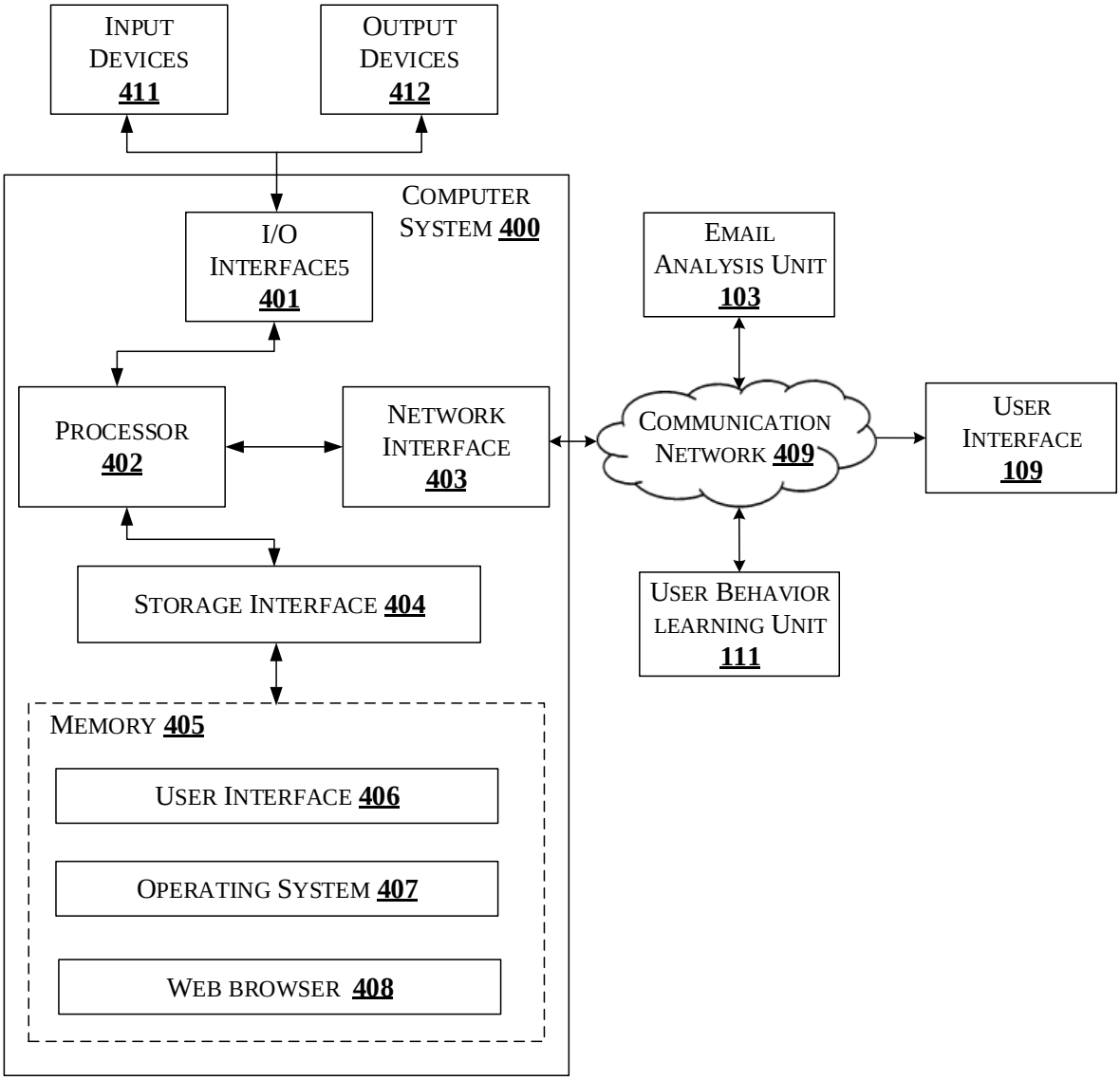

INPUT DEVICES 411
OUTPUT DEVICES 412
COMPUTER SYSTEM 400
I/O INTERFACE5 401
PROCESSOR 402
NETWORK INTERFACE 403
STORAGE INTERFACE 404
MEMORY 405
USER INTERFACE 406
OPERATING SYSTEM 407
WEB BROWSER 408
EMAIL ANALYSIS UNIT 103
COMMUNICATION NETWORK 409
USER INTERFACE 109
USER BEHAVIOR LEARNING UNIT 111

FIG. 4