[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06Q 10/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680029287.4

[43] 公开日 2008 年 8 月 13 日

[11] 公开号 CN 101243463A

[22] 申请日 2006.8.15
[21] 申请号 200680029287.4
[30] 优先权
[32] 2005. 8.16 [33] US [31] 11/205,584
[86] 国际申请 PCT/US2006/032017 2006.8.15
[87] 国际公布 WO2007/022291 英 2007.2.22
[85] 进入国家阶段日期 2008.2.5
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 J·夏维 A·M·米歇尔
B·J·特桑 G·A·赫伯特
H·I·萨瓦斯塔诺 L·汉德尔沃
R·C·J·派格里
R·诺维特斯基 S·格兰特三世
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陈 斌

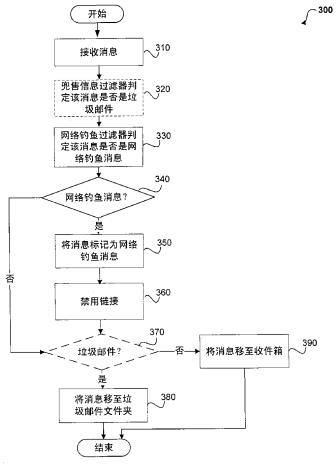
权利要求书 2 页 说明书 6 页 附图 6 页

[54] 发明名称

反网络钓鱼保护

[57] 摘要

反网络钓鱼保持有助于反网络钓鱼攻击。 包含在消息内的已被标识为网络钓鱼消息的所有链接都被禁用。 当该网络钓鱼消息被访问时，显示该警告消息。 当第一次选择该网络钓鱼消息内的禁用链接时，包含与如何启用该消息内链接有关的信息的不予考虑的对话框就会被显示。 在用户不考虑该对话框之后，单击被禁用的链接会引起警告消息闪光来引起用户对该问题潜在严重性的注意。 用户通过选择警告消息并选择适当的可选项可以启用这些链接。 一旦用户启用这些链接，将来对该消息的显示将把链接示出为启用。



1．一种用于保护免受网络钓鱼攻击的计算机实现方法，包括：

判定一消息何时是网络钓鱼消息（330）；以及

禁用所述消息内被判定为网络钓鱼消息的任何链接（360）。

2．．如权利要求 1 所述的方法，其特征在于，还包括将所述消息标记为网络钓鱼消息（350）。

3．如权利要求 1 所述的方法，其特征在于，还包括显示带有所述被禁用链接的所述网络钓鱼消息（410）。

4．如权利要求 3 所述的方法，其特征在于，还包括显示指示所述消息已被判定为网络钓鱼消息的网络钓鱼警告消息（420）。

5．如权利要求 3 所述的方法，其特征在于，还包括判定被禁用的链接何时被选（430），并且响应于所述选择，显示指示所述链接可能不安全的警告框。

6．如权利要求 4 所述的方法，其特征在于，还包括接收用以启用所述被禁用的链接的指示（460），并且响应于指示，以预定速率使所述网络钓鱼警告消息闪光（450）。

7．如权利要求 6 所述的方法，其特征在于，还包括在所述闪光的网络钓鱼警告消息内，在至少两种颜色（530, 540, 550）之间变换。

8．如权利要求 4 所述的方法，其特征在于，还包括判定所述网络钓鱼警告消息何时被选（460）并且响应于所述选择，判定是否启用所述消息内的所述被禁用链接。

9．如权利要求 8 所述的方法，其特征在于，还包括响应于用以启用所述被禁用链接的所述指示，显示次级警告对话框（630）。

10．如权利要求 2 所述的方法，其特征在于，还包括当启用所述被禁用链接时移除指示所述消息是网络钓鱼消息的所述标记（470），以使得当所述消息被再次访问时，所述消息内的所述链接仍被启用。

11．一种具有用以保护免受网络钓鱼攻击的计算机可执行指令的计算机可读介质，所述指令包括：

访问网络钓鱼消息（350）；以及

禁用所述网络钓鱼消息内的任何链接（360）。

12．如权利要求 11 所述的计算机可读介质，其特征在于，还包括显示带有被禁用所述链接的所述网络钓鱼消息（410）以及显示网络钓鱼警告消息（420）。

13．如权利要求 12 所述的计算机可读介质，其特征在于，还包括判定被禁用链接何时被选（430），并且响应于所述选择，显示警告（440）。

14．如权利要求 11 所述的计算机可读介质，其特征在于，还包括接收用以启用所述被禁用的链接的指示（460），并且响应于指示，以预定速率使所述网络钓鱼警告消息闪光（450）。

15．如权利要求 14 所述的计算机可读介质，其特征在于，还包括判定所述网络钓鱼警告消息何时被选（460）并且响应于所述选择，判定是否启用所述消息内的所述被禁用链接。

16．如权利要求 15 所述的计算机可读介质，其特征在于，还包括当启用所述被禁用链接时移除指示所述消息是网络钓鱼消息的标记（470），以使得所述消息被再次访问时，所述消息内的所述链接仍被启用。

17．一种用于保护免受网络钓鱼攻击的系统，包括：

过滤器（220），被配置成用于：

接收包括链接的消息（210）；

判定所述消息是否是网络钓鱼消息（230）；以及

提供所述消息是网络钓鱼消息的指示（230）；以及

消息收发程序（250），被耦合至所述过滤器并被配置成用于：

接收所述消息和所述指示（410）；

当所述指示示出所述消息是网络钓鱼消息时禁用所述消息内的所述链接（360）。

18．如权利要求 17 所述的系统，其特征在于，还包括在被指示时将所述消息标记为网络钓鱼消息（350），以使得只要所述消息被显示为带有指示所述消息是网络钓鱼消息的所述标记，所述链接就被禁用。

19．如权利要求 17 所述的系统，其特征在于，还包括当启用所述被禁用链接时移除指示所述消息是网络钓鱼消息的标记（470），以使得所述消息被再次访问时，所述消息内的所述链接仍被启用。

20．如权利要求 17 所述的系统，其特征在于，还包括在用户不考虑警告对话框（440）之后激活消息的所述链接（460）。

反网络钓鱼保护

背景

网络钓鱼（Phishing）攻击能够盗取没有疑心的用户的个人身份数据和财务账户证书。网络钓鱼者发送欺诈电子邮件，这些电子邮件上带有会将用户引向不安全网站的链接。不安全的网站既可以被设计为哄骗用户泄漏诸如信用卡卡号、账户用户名、口令和社会保险号码之类的财务数据，又可被设计为将恶意代码下载至用户机器以直接获取个人信息。网络钓鱼电子邮件难以标识，因为网络钓鱼者会尽力让他们的电子邮件看上去很正当。这些电子邮件往往周密地模仿由诸如银行、信用卡公司等合法组织例行发出的可辨识的电子邮件。这些电子邮件通常使用户确信以选择包括在该电子邮件内的、将导致用户泄漏他们的个人信息的链接。

概述

提供本概述以便以简化形式引入概念精选，这些概念将在以下的详细描述中被进一步描述。本概述并不旨在标识要求保护主题的关键特征或本质特征，也不旨在用于帮助确定要求保护主题的范围。

反网络钓鱼保持有助于保护用户免受网络钓鱼的攻击。对已被标识为网络钓鱼消息的消息进行标记并禁用包含在该消息内的链接。当访问网络钓鱼消息时，会向用户显示网络钓鱼警告消息，以通知用户该消息内的链接因其可能连接至不安全站点而已被禁用。当第一次选择该网络钓鱼消息内的禁用链接时，包含与如何启用该消息内被禁用链接有关的信息的可不予考虑对话框就会被显示。一旦用户不考虑该对话框，选择被禁用的链接之一会引起网络钓鱼警告消息闪光，从而引起用户对该警告消息的注意。用户随后能够选择启用链接。一旦用户启用了该消息内的链接，将来对该消息的访问会把这些链接显示为启用。

附图说明

图 1 示出了示例性计算设备；

图 2 示出了反网络钓鱼保护系统；

图 3 示出了反网络钓鱼的进程；

图 4 示出了用于与网络钓鱼消息交互的进程；

图 5 示出了网络钓鱼消息的示例性显示；以及

图 6 根据本发明各方面示出了示例性的网络钓鱼对话框。

详细说明

图 2 根据本发明各方面示出了一个反网络钓鱼保护系统。如图所示，系统 200 包括消息 210、包含网络钓鱼过滤器 230 和兜售信息（spam）过滤器 240 的过滤器 220、包含网络钓鱼保护 250 和网络钓鱼设置 260 的消息收发程序 250、以及垃圾邮件文件夹 270 和收件箱 280。该系统可以使用诸如结合图 1 描述的一个或多个计算设备来实现。

虽然接收兜售信息消息让人感到不便，但是通常不会让用户受到伤害或有所花费。一般而言，兜售信息消息会导致的最坏结果是用户需要删除未经要求的邮件。大多数兜售信息消息对用户而言相对容易标识，因为易于快速浏览该消息并做出判断。

然而，网络钓鱼攻击会导致用户泄漏包括财务信息在内的敏感信息，而这可导致隐私的泄漏和/或金钱的损失。没有疑心的用户跟随消息内的网络钓鱼链接（URL）会导致许多有害的情形。用户被会引至模仿合法站点的站点，在那里用户会被提示输入秘密的财务信息。用户可被引至会将恶意代码下载至他们机器上的站点。这些情形比兜售信息的影响要危险的多。 因此，会区别对待网络钓鱼信息与兜售信息消息。

消息 210 可以是任何消息。根据一个实施例，消息 210 是电子邮件消息。最初做出一消息（210）是否是网络钓鱼消息的判定。网络钓鱼消息是可被归类为潜在的网络钓鱼攻击的任何消息。

消息 210 由网络钓鱼过滤器（230）过滤以指示该消息是否是网络钓鱼消息。可以使用任何网络钓鱼检测方法来判定一消息是否是网络钓鱼消息。用于判定网络钓鱼消息的一种方法是检查该消息内包含的 URL 的格式。例如，某些 URL 可以是会引起对该消息怀疑的数值型 URL。根据一个实施例，网络钓鱼过滤器（230）首先考察 URL 内（在<a/>标志内）的某些特性以在忽略该消息内容的其余部分的情况下判定该消息是网络钓鱼消息的可能性。如上所述，任何网络钓鱼检测方法都可使用，只要其能提供将该消息标识为网络钓鱼消息的指示符。根据一个实施例，网

络钓鱼过滤器 230 提供可疑级和中性级。任何被标记为可疑的消息都可认为是网络钓鱼消息。任何由网络钓鱼过滤器 230 标记为中性的消息不被认为是网络钓鱼消息。

过滤任何引入的消息来判定该消息是否是网络钓鱼消息。无论消息是否来自被认为安全的个体，每条消息都被过滤。例如，一消息可能来自于被包括在安全发件人列表上的用户。根据一个实施例，虽然不推荐，但是用户即使在一消息被认为是网络钓鱼消息时仍可关闭对各链接的禁用。即使在该可选项被关闭时，每条消息仍被过滤并且适当地被标记为网络钓鱼消息，从而在用户再打开该可选项的情况下，该消息仍将被显示为链接被禁用。

一旦消息（210）已被过滤，消息收发程序 250 就接收带有该消息是否是网络钓鱼消息的指示的消息。网络钓鱼保护 250 对该消息作标记并且禁用已被判定为网络钓鱼消息的任何消息内的任何链接。随后取决于该消息是否被兜售信息过滤器 240 判定为兜售信息而将该消息递送入垃圾邮件文件夹（270）或收件箱（280）。被判定为兜售信息的消息被递送入垃圾邮件文件夹。不被认为是兜售信息，但被认为是网络钓鱼消息的消息则被递送至收件箱（280）。

与一并禁用链接和图像不同，一消息内包含的链接和图像被独立禁用。一般而言，从外部源阻止图像以防止某些人标识活动的电子邮件账户。标识一账户是否是活动的比用户点击网络钓鱼链接的危险要小。

任何已被标记为网络钓鱼消息的消息，在其内的链接将被禁用。无论网络钓鱼消息被递送至垃圾邮件文件夹（270）还是收件箱（280）的情况下都是这样。根据一个实施例，任何被认为是兜售信息的消息，其链接也被禁用。即使应将该消息移入收件箱，取决于由网络钓鱼过滤器生成的结果，各链接仍将保持被禁用。

图 3 根据本发明各方面示出了反网络钓鱼保护的进程。在起始框之后，进程行进至在其中消息被接收的框 310。根据一个实施例，该消息是电子邮件消息。

行进至可选框 320，该消息被传递通过兜售信息过滤器以判定该消息是否是垃圾邮件。

移至框 330，该消息被传递通过网络钓鱼过滤器以判定该消息是否是网络钓鱼消息。网络钓鱼消息是被认为是包括潜在的网络钓鱼攻击的任何消息。根据一个实施例，通过检查包括在一消息内的链接来将该消息判定为网络钓鱼消息。

转换至判定框 340，做出该消息是否是网络钓鱼消息的判定。当该消息不是网络钓鱼消息，则进程行进至判定框 370。

当该消息是网络钓鱼消息，进程行进至框 350，在其中用显示该消息是网络钓鱼消息的指示符对该消息作标记。指示该消息是网络钓鱼消息的标记与该消息一并被存储，以使该消息在被访问时，能被轻易判定其是网络钓鱼消息。

移至框 360，禁用网络钓鱼消息内的链接，以避免链接被漫不经心地选择从而避免将用户导向网络钓鱼攻击。根据一个实施例，消息内的每个链接都被禁用。这包括可选择的图形以及 URL。根据一个实施例，一个可选项可被设置而从不禁止该消息内的链接。在此实例中，该消息仍然被过滤并被标记为网络钓鱼。以此方式，如果用户再次打开网络钓鱼保护，则链接会被主动禁用而无需重复过滤该消息。

在可选判定框 370 处，做出该消息是否是垃圾邮件的判定。当该消息是垃圾邮件时，进程移至框 380，在其中该消息被移至垃圾邮件文件夹。当该消息不是垃圾邮件时，进程移至框 390，在其中该消息被移至收件箱。随后该进程移至结束框并返回以处理其它动作。

图 4 根据本发明各方面示出了用于与网络钓鱼消息交互的进程。在起始框之后，该进程行进至框 410，在其中已被标记为网络钓鱼消息的消息被访问。根据一个实施例，访问该网络钓鱼消息包括显示该消息。

移至框 420，网络钓鱼警告连同该消息一并显示。网络钓鱼警告向用户提供出于安全考虑已禁用该消息内链接的指示。根据一个实施例，在消息显示区域内的消息之上显示该网络钓鱼警告。可以按各种不同的方式来显示该警告。例如，警告消息可以覆盖在该消息之上。

行进至框 430，选择该网络钓鱼消息内的被禁用链接。例如，用户可以选择该消息内的链接之一，从而被导向至由该被禁用 URL 所指定的网络位置。

转换至框 440，向用户显示警告对话框。根据一个实施例，警告对话框是通知用户该消息内的至少某些链接可能是不安全的可不予考虑的对话框。用户可以不考虑该警告对话框。

移至框 450，只要有被禁用的链接被选中，网络钓鱼警告就闪光以引起对潜在网络钓鱼攻击的严重性的注意。根据一个实施例，该网络钓鱼消息可按预定速率闪光并且该警告每次闪光时，该警告的颜色都会改变。

行进至判定框 460，做出是否要激活该消息内各链接的判定。可以按消息来启用消息上的链接。当链接被激活时，该进程就行进至框 470，在其中用附加属性来对该消息作标记，该属性指示所有将来对该消息的访问都将显示该消息内被启用的链接。

随后该进程移至结束框并返回以处理其它动作。

图 5 根据本发明各方面示出了网络钓鱼消息的示例性显示。

显示 500 包括了网络钓鱼警告消息（520）和包含有被禁用的链接（525）的消息。根据一个实施例，与其它活动链接相比，链接（525）显现出灰晕。

当一消息首先被该消息程序访问时，该消息程序检查已标记在该消息上的指示符，从而判定该消息是否是网络钓鱼消息。此刻，网络钓鱼消息内的任何链接（525）都被禁用，而网络钓鱼警告 520 被显示。

根据一个实施例，网络钓鱼警告 520 包括一消息用来陈述："单击此处以启用链接。为了您的安全，该消息内的链接已被禁用。"

当被禁用的链接（525）被选中时，网络钓鱼警告（520）就以预定速率闪烁以引起注意。根据一个实施例，警告对话框在被禁用的链接被首次访问之时呈现（参见图 6 及其相关讨论）。根据另一实施例，网络钓鱼警告（520）在网络钓鱼警告消息 530、网络钓鱼警告消息 540 和网络钓鱼警告 550 消息之间切换。该警告不仅闪光，其颜色也改变以进一步引起注意。

用户可以选择网络钓鱼警告 520 来启用该消息内的链接。选择该网络钓鱼警告消息会显示上下文菜单 560。选择"打开链接（不推荐）"来启用该消息内的所有链接。此刻，从菜单 560 中移除打开链接菜单项。一旦链接被启用，这些链接只要在重开该消息时都保持启用。

图 6 根据本发明各方面示出了示例性的网络钓鱼对话框。

当用户第一次选择诸如图 5 所示链接 525 的被禁用 URL 时，就显示警告对话框 610。警告对话框 610 是让用户知道一链接为何被禁用以及任何启用有关该消息的链接的信息对话框。如果用户选择"请不要再向我显示该对话框"复选框 615，则随后该对话框在对该消息内的各链接的后续选择中就不再显示。

可以显示可选警告对话框 630 来确保用户认识到该警告的重要性。例如，对话框 630 可以是在用户使用图 5 中显示的上下文菜单 560 选择打开各链接之后显示的次级对话框。

示例性操作环境

参加图 1，用于实现本发明的一个示例性系统包括计算设备，诸如计算设备 100。在一个非常基本的配置中，计算设备 100 通常包括至少一个处理单元 102 和系统存储器 104。取决于计算设备的确切配置和类型，系统存储器 104 可以是易失性的（诸如 RAM）、非易失性的（诸如 ROM、闪存等）或是两者的某种组

合。系统存储器 104 通常包括操作系统 105、一个或多个应用程序 104，并且可以包括程序数据 107。在一个实施例中，应用程序 106 可以包括正被启动的程序 120。这一基本配置在图 1 中由虚线 108 中的那些组件示出。

计算设备 100 也可具有其它特征或功能性。例如，计算设备 100 也可含有附加的数据存储设备（可移动和/或不可移动），诸如磁盘、光盘或磁带。这样的额外存储在图 1 中由可移动存储 109 和不可移动存储 110 示出。计算机存储介质可包括易失性和非易失性、可移动和不可移动介质，它们以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据这样的信息的任意方法或技术来实现。系统存储器 104、可移动存储 109 和不可移动存储 110 都是计算机存储介质的示例。计算机存储介质包括，但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘（DVD）或其它光存储、磁带盒、磁带、磁盘存储或其它磁性存储设备、或能用于存储所需信息且可以由计算设备 100 访问的任何其它介质。任何这样的计算机存储介质都可以是设备 100 的一部分。计算设备 100 也可以具有诸如键盘、鼠标、笔、语音输入设备、触摸输入设备等输入设备 112。也可以包括诸如显示器、扬声器、打印机等的输出设备 114。

计算设备 100 也可以包含允许该系统与其它计算设备 118 诸如经网络通信的通信连接 116。通信连接 116 是通信介质的一个示例。通信介质通常可具体化为诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据，并且包括任何信息传递介质。术语“已调制数据信号”是指以在该信号中编码信息的方式来设置或改变其一个或多个特性的信号。作为示例，而非限制，通信介质包括有线介质，诸如有线网络或直接线连接，以及无线介质，诸如声学、RF、红外线和其它无线介质。如此处所用的术语计算机可读介质既包括存储介质又包括通信介质。

以上说明、示例和数据提供了对本发明成分的制造和使用的全面描述。因为可以在不背离本发明的精神和范围的情况下做出本发明的许多实施例，所以本发明位于所附权利要求的范围内。

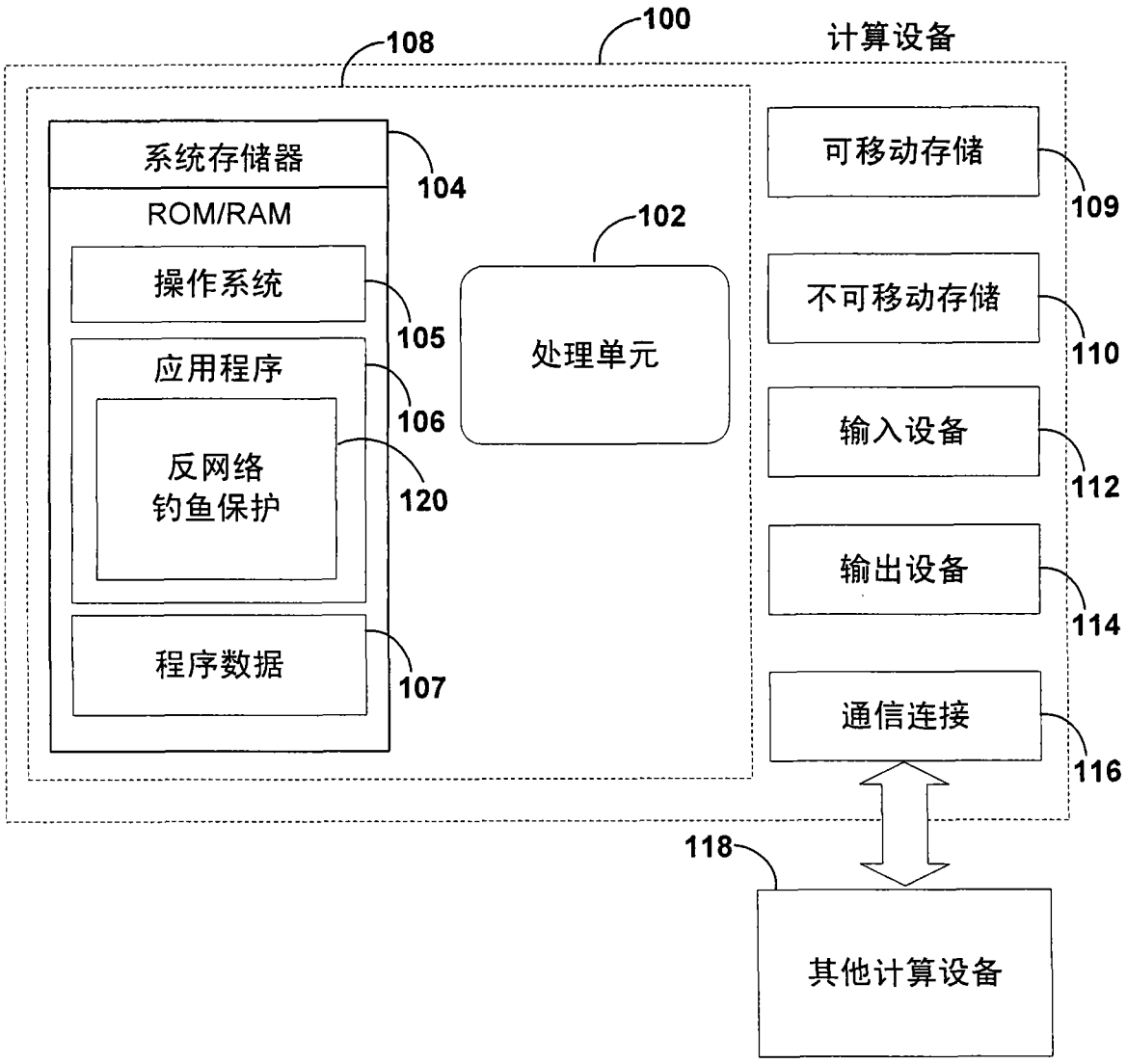

100
计算设备
108
系统存储器
104
ROM/RAM
操作系统
105
应用程序
106
反网络
钓鱼保护
120
程序数据
107
102
处理单元
可移动存储
109
不可移动存储
110
输入设备
112
输出设备
114
通信连接
116
118
其他计算设备

图 1

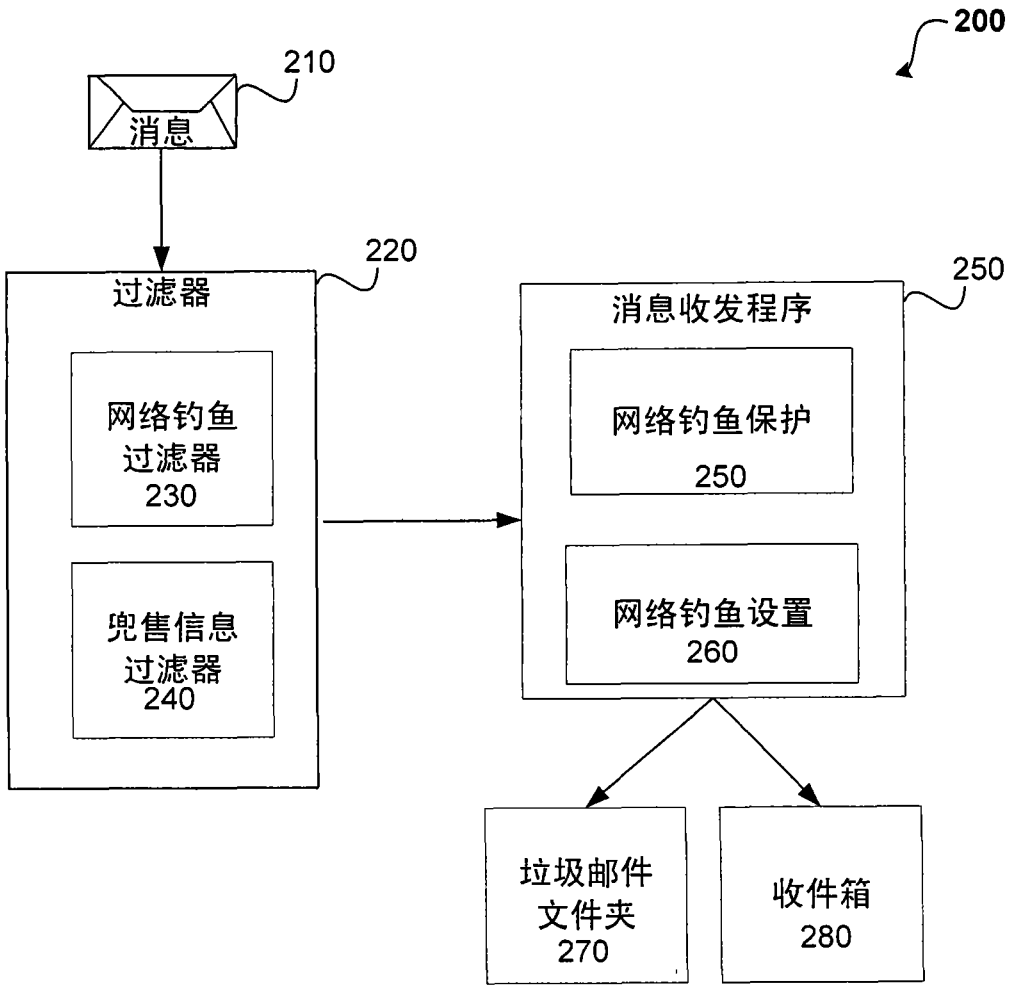

200
210
消息
220
过滤器
网络钓鱼
过滤器
230
兜售信息
过滤器
240
250
消息收发程序
网络钓鱼保护
250
网络钓鱼设置
260
垃圾邮件
文件夹
270
收件箱
280

图 2

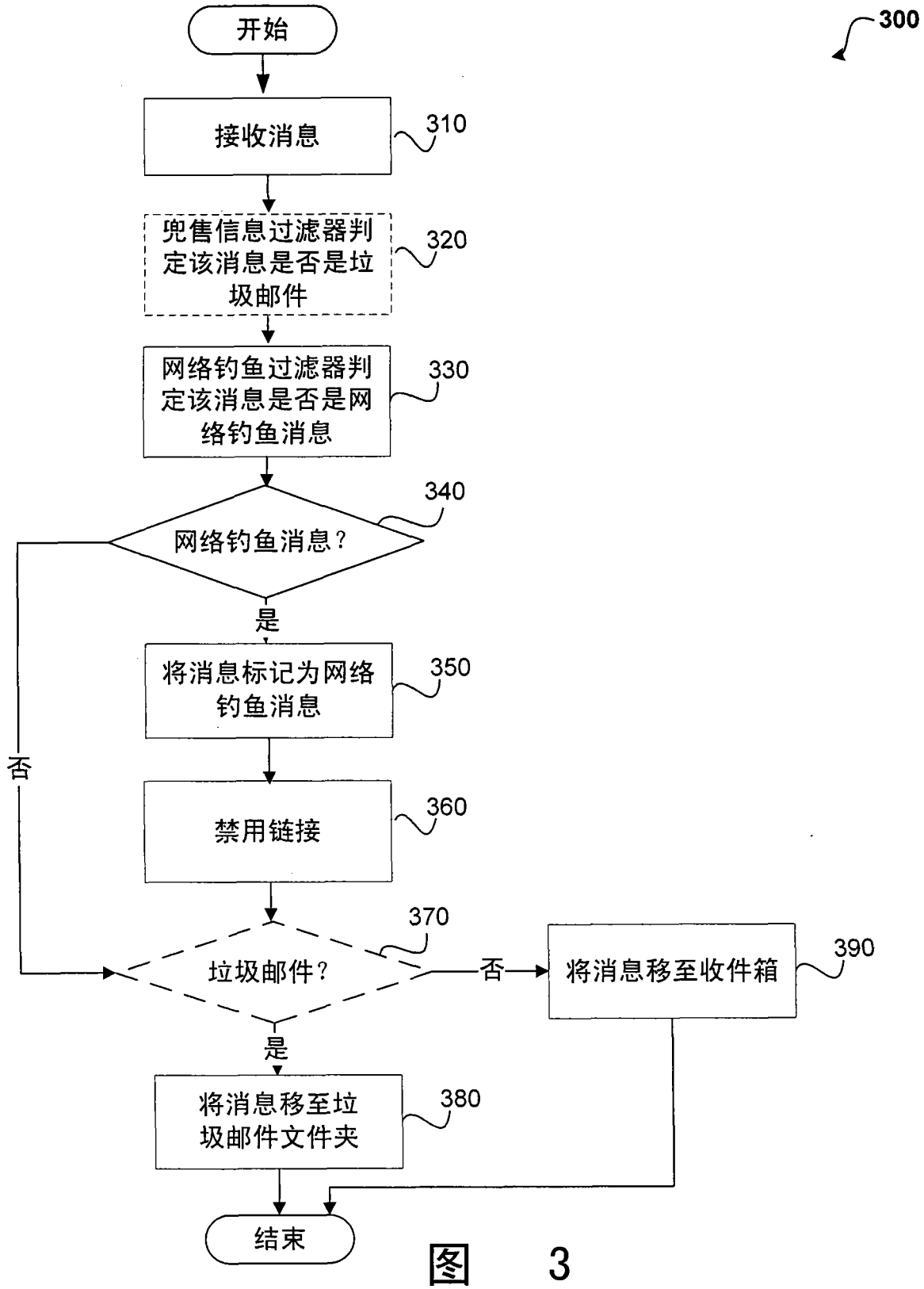

300
开始
接收消息
310
兜售信息过滤器判定该消息是否是垃圾邮件
320
网络钓鱼过滤器判定该消息是否是网络钓鱼消息
330
网络钓鱼消息？
340
是
否
将消息标记为网络钓鱼消息
350
禁用链接
360
垃圾邮件？
370
否
将消息移至收件箱
390
是
将消息移至垃圾邮件文件夹
380
结束

图 3

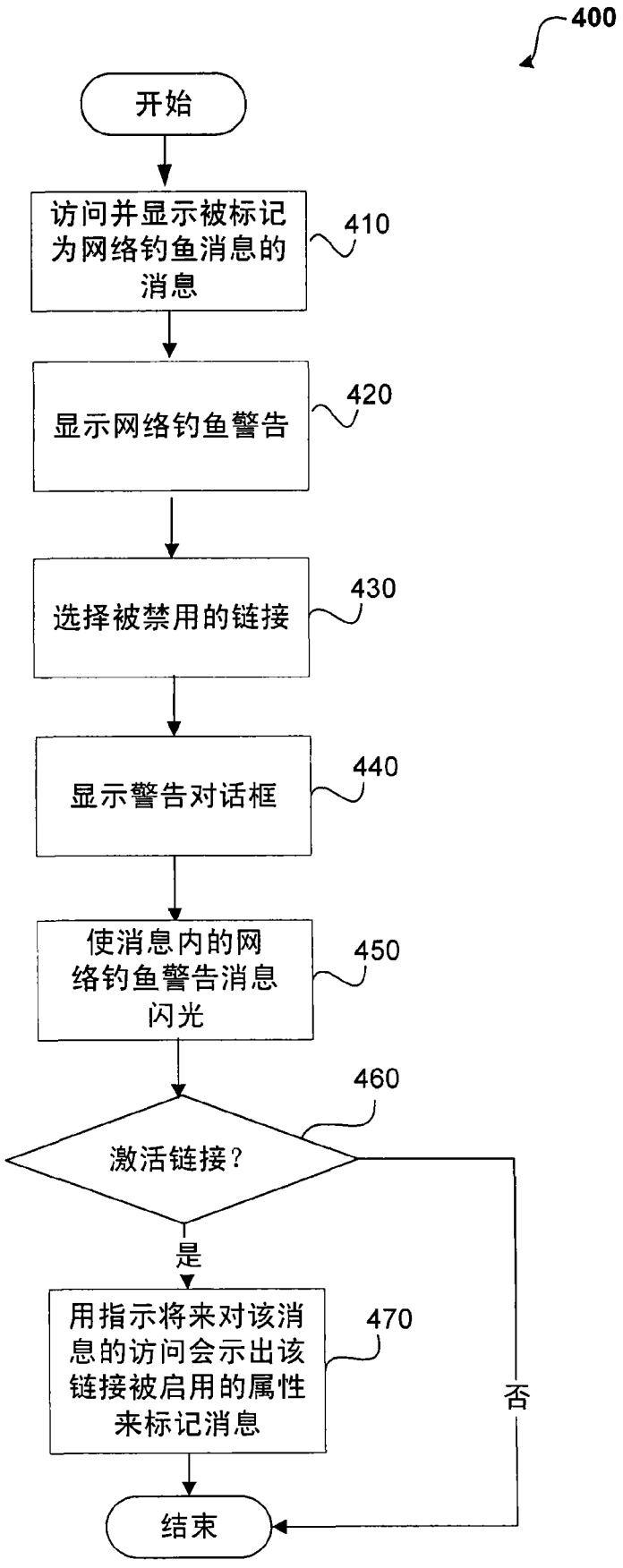

400
开始
访问并显示被标记为网络钓鱼消息的消息
410
显示网络钓鱼警告
420
选择被禁用的链接
430
显示警告对话框
440
使消息内的网络钓鱼警告消息闪光
450
460
激活链接？
是
否
用指示将来对该消息的访问会示出该链接被启用的属性来标记消息
470
结束

图 4

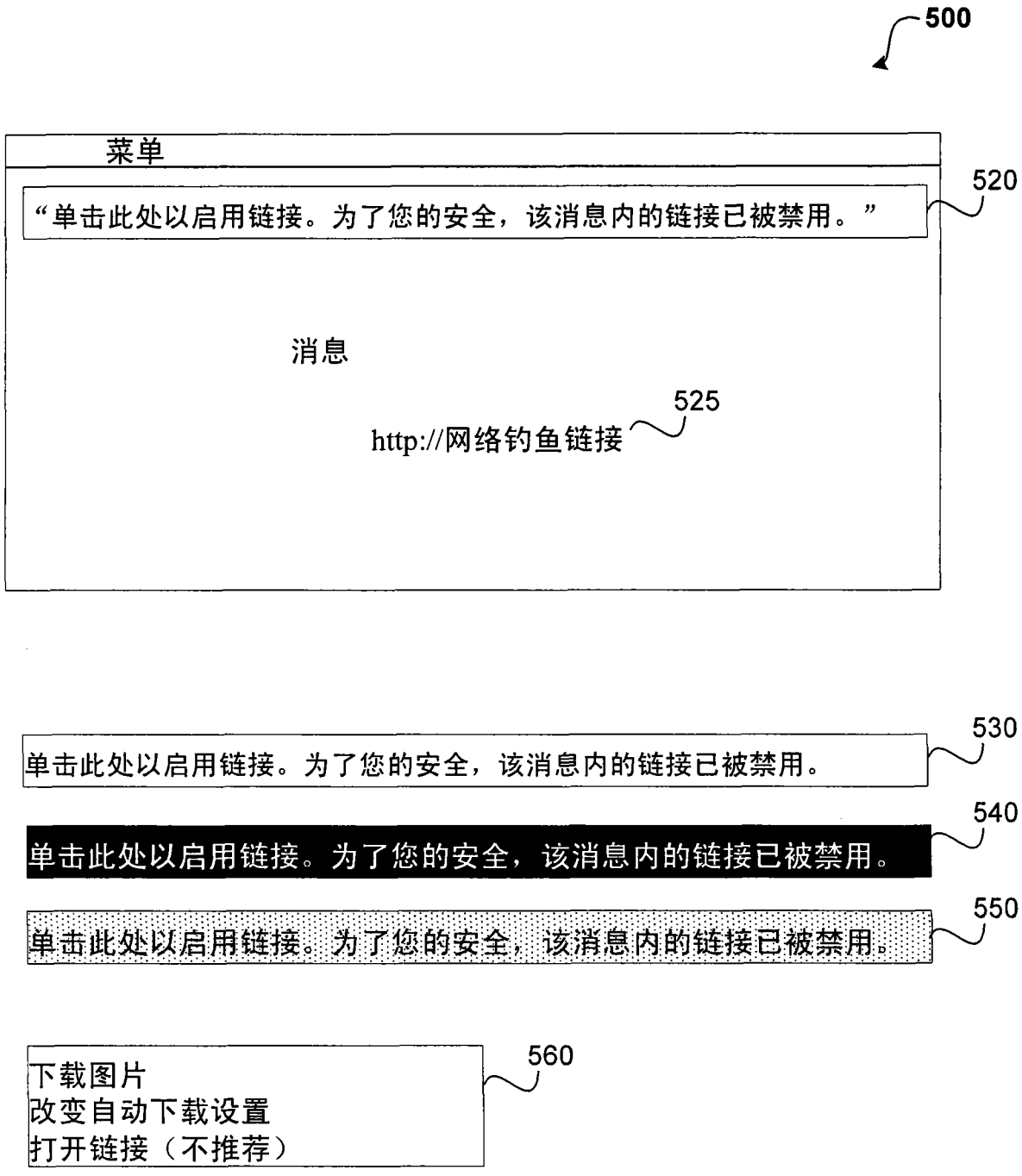

500
菜单
“单击此处以启用链接。为了您的安全，该消息内的链接已被禁用。”
520
消息
525
http://网络钓鱼链接
530
单击此处以启用链接。为了您的安全，该消息内的链接已被禁用。
540
单击此处以启用链接。为了您的安全，该消息内的链接已被禁用。
550
单击此处以启用链接。为了您的安全，该消息内的链接已被禁用。
560
下载图片
改变自动下载设置
打开链接（不推荐）

图 5

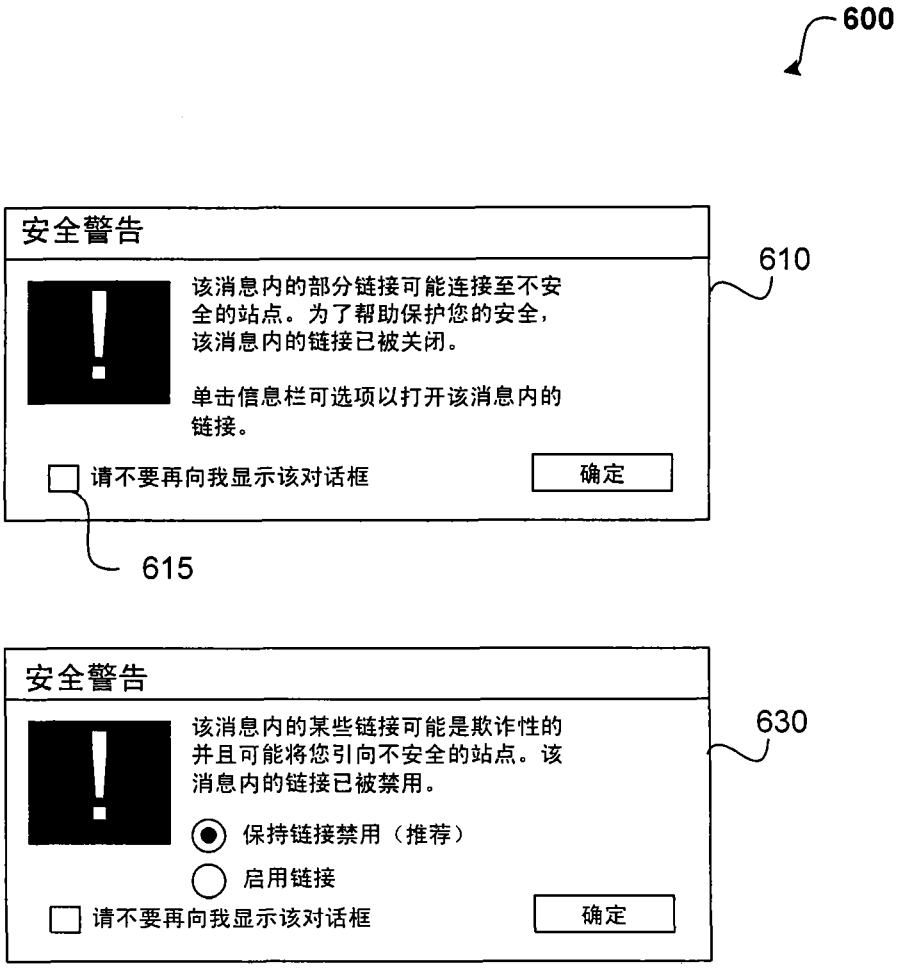

600
安全警告
610
该消息内的部分链接可能连接至不安全的站点。为了帮助保护您的安全，该消息内的链接已被关闭。
单击信息栏可选项以打开该消息内的链接。
请不要再向我显示该对话框
确定
615
安全警告
630
该消息内的某些链接可能是欺诈性的并且可能将您引向不安全的站点。该消息内的链接已被禁用。
保持链接禁用（推荐）
启用链接
请不要再向我显示该对话框
确定

图 6