~~CLAIMS~~

The invention claimed is:

1. One or more computer-readable device~~media~~ having computer-executable instructions embodied thereon that, when executed, perform a method for alerting a user of a potentially phishing email upon the user accessing an account via a non-web mail client, the method comprising:

receiving ~~(410)~~ a digital communication at the non-web mail client~~account~~ associated with the user, wherein the non-web mail client has no association with a service provider;

incident to identifying the digital communication as a potentially phishing email, appending ~~(420)~~ a metadata tag to the digital communication;

placing ~~(430)~~ the tagged digital communication in a first storage location that is dedicated to persist digital communications that are identified as potentially phishing emails, wherein the first storage location provides a physical memory location separate from a second storage location that persists digital communications identified as legitimate; and

presenting ~~(440)~~ a visual representation of the first storage location to the user upon the user accessing the account via the non-web mail client, wherein the visual representation provides an indication to the user that one or more potentially phishing emails have arrived at the user's account.

2. The one or more computer-readable device~~media~~ of claim 1, wherein the method further comprises persisting the appended tag in association with the digital communication identified as the potentially phishing email in a quarantine listing on the one or more computer-readable media, wherein the quarantine listing enumerates each of the one or more potentially phishing emails that have arrived at the user's account.

3. The one or more computer-readable device~~media~~ of claim 1, wherein the method further comprises applying filtering heuristics to ascertain whether the digital communication is the potentially phishing email, wherein the potentially phishing email is a message that fraudulently solicits the user to divulge personal information.

4. The one or more computer-readable device~~media~~ of claim 3, wherein the method further comprises generating the first~~dedicated~~ storage location upon ascertaining that the digital communication is the potentially phishing email.

5. The one or more computer-readable device~~media~~ of claim 1, wherein the digital communication comprises at least one of an email message or an instant message, and wherein the digital communication is received from a source that is removed from the one or more computer-readable device~~media~~.

6. The one or more computer-readable device~~media~~ of claim 1, wherein the non-web mail client provides the user access to the account by rendering a user interface (UI) display to the user, wherein elements published on the UI display are not controlled by the~~a~~ service provider that manages the user's account.

7. The one or more computer-readable device~~media~~ of claim 6, wherein the method further comprises intercepting a request initiated by the user, via the UI display, to perform an action with respect to the potentially phishing email.

8. ~~A~~The one or more computer-readable device~~media~~ of claim 7, the method further comprising:

ascertaining that the user-initiated request is directed toward the digital communication identified as the potentially phishing email by inspecting the metadata tag appended to the digital communication; and

ascertaining whether the action that is communicated in the request is a restricted action.

9. The one or more computer-readable device~~media~~ of claim 8, wherein the method further comprising:

upon ascertaining that the user-initiated request is directed toward the digital communication identified as the potentially phishing email and that the action that is communicated in the request is a restricted action, preventing execution of the action; and

transmitting an operation-fail indication to the non-web mail client in response to the request.

10. The one or more computer-readable device~~media~~ of claim 9, wherein the restricted action comprises at least one of a reply command, a reply to all command, or a forward command.

11. The one or more computer-readable device~~media~~ of claim 1, wherein the action comprises a command attempting to move the digital communication from the first~~dedicated~~ storage location to the second~~a~~ storage location ~~that holds digital communications identified as legitimate~~, wherein the method further comprising:

~~detecting a synchronization operation originating from the non-web mail client;~~

ascertaining that the action is the move-attempt command; and

disallowing movement of the digital communication outside the first~~dedicated~~ storage location.

12. The one or more computer-readable device of claim 1, wherein the method further comprises:

presenting the visual representation of the first storage location as a folder on the UI display rendered by the non-web mail client; and

upon receiving a selection of the folder, presenting representations of the one or more potentially phishing emails that have arrived at the user's account and that are persisted in the first storage location.

~~12.~~13. The one or more computer-readable device~~media~~ of claim 12, wherein the method further comprises:

deactivating uniform-resource locator (URL) links incorporated within content of the one or more potentially phishing emails that are persisted in the first~~dedicated~~ storage location;

receiving a ~~user-initiated~~ selection of the representations of the one or more potentially phishing emails; and

conveying the content of the one or more selected potentially phishing emails to the non-web mail client for rendering.

~~13.~~14. A computerized method, implemented by a service provider accommodated on a server, for managing treatment of one or more digital communications when accessed via a non-web mail client, the method comprising:

upon receiving a digital communication at the non-web mail client~~an account~~ associated with an intended recipient of the digital

communication, applying ~~(510)~~ filtering heuristics to determine whether the digital communication is an uninvited message or a legitimate message, wherein the non-web mail client has no association with the service provider;

when the digital communication is determined to be an uninvited message, marking ~~(520)~~ the digital communication as unsafe;

replacing ~~(530)~~ the unsafe digital communication with a warning message, wherein content of the unsafe digital communication is not revealed within the warning message;

instructing ~~(540)~~ the non-web mail client to surface a representation of the warning message within~~unsafe digital communication in~~ a listing rendered in a user interface (UI) display, wherein the listing includes one or more representations of digital communications determined to be legitimate messages, and wherein the UI display rendered by the non-web mail client cannot be reconfigured by the service provider that manages the user's account; and

upon receiving a user-initiated selection of the representation of the warning message~~unsafe digital communication~~, communicating ~~(550)~~ instructions to the non-web mail client to present the warning message to the recipient and withhold revealing content of the unsafe digital communication, wherein the warning message provides directions to access the content of the unsafe digital communication.

15. The computerized method of claim 14, further comprising persisting the unsafe digital communication in a storage location that holds one or more digital communications that are determined to be legitimate communications.

~~14.~~16. The computerized method of claim 14~~13~~, wherein the warning message conveys a notification that the unsafe digital communication is identified as a potentially phishing email~~, wherein the warning message provides directions to access content of the unsafe digital communication via a web browser, and wherein the warning message includes a uniform-resource locator (URL) link to a web browser that, upon selection, allows the recipient to access content of the unsafe digital communication~~.

17. The computerized method of claim 14, wherein the warning message includes a uniform-resource locator (URL) link to a web browser that, upon selection, allows the recipient to access content of the unsafe digital communication.

~~15.~~18. One or more computer-readable device~~media~~ having computer-executable instructions embodied thereon that, when executed, perform a method for notifying a user, via a user-interface (UI) display rendered by a non-web mail client, that a potentially phishing email has arrived at an account of the user, the method comprising:

generating ~~(430)~~ a first storage location ~~(230)~~ that is dedicated to persist one or more digital communications ~~(215)~~ identified as potentially phishing emails, wherein the first storage location provides a physical memory location separate from a second storage location that persists digital communications identified as legitimate;

instructing ~~(340)~~ the non-web mail client ~~(240)~~ to render a first folder within the UI display, wherein the first folder maps to the first~~dedicated~~ storage location, wherein the non-web mail client has no association with a service provider;

detecting ~~(330)~~ an indication implemented by the user to access the first folder; and

instructing ~~(350)~~ the non-web mail client ~~(240)~~ to render representations of the one or more identified digital communications, wherein the representations include metadata related to content of the one or more identified digital communications.

19. The one or more computer-readable device of claim 18, wherein instructing the non-web mail client to render a first folder within the UI display comprises instructing the non-web mail client to render the first folder in a listing that includes a second folder that map to the second storage location that persists the digital communications identified as legitimate emails, thereby visually separating the potentially phishing emails from the legitimate emails.

20. The one or more computer-readable device of claim 18, wherein the method further comprises:

receiving an action initiated by the user that is directed toward the one or more identified digital communications;

failing the user-initiated action by preventing the action from being executed; and

transmitting an operation-fail indication to the non-web mail client, wherein the operation-fail indication notifies of the failure of the action.