

Claims

1. A computer-implemented method for defense against social engineering attack comprising:

identifying, by a computing device, potential social engineering activity associated with one or more communications on a first communication channel of a plurality of communication channels, wherein the potential social engineering activity is directed towards a user target on the first communication channel, wherein the user target is a first user, wherein the first communication channel includes a first type of communication;

requesting a restriction of at least partial access of the user target to at least a second communication channel of the plurality of communication channels based upon, at least in part, the identification of the potential social engineering activity associated with the one or more communications on the first communication channel, wherein the second communication channel includes a second type of communication, and wherein both the first communication channel and the second communication channel are different communication platforms;

restricting at least the partial access of the user target to at least the second type of communication on the second communication channel of the plurality of communication channels based upon, at least in part, requesting the restriction; and

performing an action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the action includes implementing a quarantine action on the user target, wherein implementing the quarantine action on the user target includes temporarily accessing and changing user permissions of the user target associated with one of a file and an application.

2. The computer-implemented method of claim 1 wherein identifying the potential social engineering activity occurs in real-time.

3. The computer-implemented method of claim 1 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes automatically connecting a second user to at

least partially participate in the one or more communications on the first communication channel.

4. The computer-implemented method of claim 1 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes providing one or more characteristics of the one or more communications used to identify the potential social engineering activity.

5. The computer-implemented method of claim 1 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes providing aggregated information about at least one user participating with the one or more communications on the first communication channel.

6. The computer-implemented method of claim 1 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes verifying social engineering activity associated with the potential social engineering activity.

7. The computer-implemented method of claim 1 wherein the different communication platforms include one of a social messaging system, an instant messaging system, a voice service, a voice chat application, an electronic mail application, and an SMS application.

8. A computer program product residing on a non-transitory computer readable storage medium having a plurality of instructions stored thereon which, when executed across one or more processors, causes at least a portion of the one or more processors to perform operations comprising:

identifying potential social engineering activity associated with one or more communications on a first communication channel of a plurality of communication channels, wherein the potential social engineering activity is directed towards a user

target on the first communication channel, wherein the user target is a first user, wherein the first communication channel includes a first type of communication;

requesting a restriction of at least partial access of the user target to at least a second communication channel of the plurality of communication channels based upon, at least in part, the identification of the potential social engineering activity associated with the one or more communications on the first communication channel, wherein the second communication channel includes a second type of communication, and wherein both the first communication channel and the second communication channel are different communication platforms;

restricting at least the partial access of the user target to at least the second type of communication on the second communication channel of the plurality of communication channels based upon, at least in part, requesting the restriction; and

performing an action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the action includes implementing a quarantine action on the user target, wherein implementing the quarantine action on the user target includes temporarily accessing and changing user permissions of the user target associated with one of a file and an application.

9. The computer program product of claim 8 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes automatically connecting a second user to at least partially participate in the one or more communications on the first communication channel.

10. The computer program product of claim 8 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the action second includes providing one or more characteristics of the one or more communications used to identify the potential social engineering activity.

11. The computer program product of claim 8 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein

performing the second action includes providing aggregated information about at least one user participating with the one or more communications on the first communication channel.

12. The computer program product of claim 8 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes verifying social engineering activity associated with the potential social engineering activity.

13. The computer program product of claim 8 wherein the different communication platforms include one of a social messaging system, an instant messaging system, a voice service, a voice chat application, an electronic mail application, and an SMS application.

14. A computing system including one or more processors and one or more memories configured to perform operations comprising:

- identifying potential social engineering activity associated with one or more communications on a first communication channel of a plurality of communication channels, wherein the potential social engineering activity is directed towards a user target on the first communication channel, wherein the user target is a first user, wherein the first communication channel includes a first type of communication;

- requesting a restriction of at least partial access of the user target to at least a second communication channel of the plurality of communication channels based upon, at least in part, the identification of the potential social engineering activity associated with the one or more communications on the first communication channel, wherein the second communication channel includes a second type of communication, and wherein both the first communication channel and the second communication channel are different communication platforms;

- restricting at least the partial access of the user target to at least the second type of communication on the second communication channel of the plurality of communication channels based upon, at least in part, requesting the restriction; and

- performing an action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the action includes implementing a quarantine action on the user target, wherein implementing the quarantine action on

the user target includes temporarily accessing and changing user permissions of the user target associated with one of a file and an application.

15. The computing system of claim 14 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes automatically connecting a second user to at least partially participate in the one or more communications on the first communication channel.

16. The computing system of claim 14 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes providing one or more characteristics of the one or more communications used to identify the potential social engineering activity.

17. The computing system of claim 14 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes providing aggregated information about at least one user participating with the one or more communications on the first communication channel.

18. The computing system of claim 14 further comprising performing a second action based upon, at least in part, identifying the potential social engineering activity associated with the one or more communications on the first communication channel, wherein performing the second action includes verifying social engineering activity associated with the potential social engineering activity.

19. The computing system of claim 14 wherein the different communication platforms include one of a social messaging system, an instant messaging system, a voice service, a voice chat application, an electronic mail application, and an SMS application.

20. The computing system of claim 14 further comprising a virtual agent for at least one of monitoring and controlling the operations.