## CLAIMS

We Claim:

1. A mobile device, comprising:

a gyroscope;

a proximity sensor;

a camera;

a screen;

a memory; and

a processor executing an anti-hacking application, which when executed is configurable to cause the processor to:

parse a window or page having one or more fields displayed on the screen, and use at least labels of the one or more fields to classify the window or page as having one or more fields that display sensitive information;

responsive to determining that the one or more fields display sensitive information:

access data from the gyroscope to detect roll and pitch viewing angles of the screen of the mobile device;

access data from the proximity sensor to detect a distance between the mobile device and a user;

activate the camera to take an image of the user and detect a number of faces visible in the image; obscure at least a portion of the sensitive information displayed in the one or more fields when any predefined conditions are not met, including: determining that the roll and pitch viewing angles are not within pitch and roll threshold values, or that the detected distance between the mobile device and the

user is not within distance threshold values, or that multiple faces are detected in the image; and

once all the predefined conditions are met, enable the window or page to display the sensitive information in the one or more fields to the user.

2. The mobile device of claim 1, wherein the window or page is displayed by a graphical user interface of an operating system or an application, the window or page comprising one or more data fields and corresponding field labels.

3. The mobile device of claim 1, wherein the portion of the sensitive information displayed in the one or more fields is obscured until a predefined time limit is reached or until the roll and pitch viewing angles are within the pitch and roll threshold values and that the detected the distance between the mobile device and the user is within the distance threshold values.

4. The mobile device of claim 1, wherein once invoked for a first time or the user indicates they a new user, the anti-hacking application enrolls the new user, including taking one or more images of a face of the user, converting the one or more images into one or more face templates, and storing the one or more face templates in a face template database.

5. The mobile device of claim 1, wherein the anti-hacking application searches for the parsed to data in a classification data store of labels, keywords, and metadata that indicate or are associated with the sensitive information, wherein a match indicates the window or page displays the sensitive information and needs protection, while a

non-match indicates the window or page does not display the sensitive information and is safe or insensitive.

6. The mobile device of claim 1, wherein the anti-hacking application uses one or more of machine learning (ML) models that are trained to process the parsed data and return a classification of whether the window or page is sensitive or in-sensitive.

7. The mobile device of claim 1, wherein the anti-hacking application classifies a viewing environment to be unsafe responsive to determining that the roll and pitch viewing angles are not within the pitch and roll threshold values, or that the detected distance between the mobile device and the user is not within the distance threshold values, or that multiple faces are detected in the image, and displays an override prompt to the user with a UI element to enable the user to override the unsafe viewing environment classification and view the sensitive information.

8. A method, comprising:

parsing, by a processor of a mobile device, a window or page having one or more fields displayed on a screen of the mobile device, and using at least labels of the one or more fields to classify the window or page as having one or more fields that display sensitive information;

responsive to determining that one or more fields display sensitive information:

accessing, by the processor, data from a gyroscope of the mobile device to detect roll and pitch viewing angles of the screen of the mobile device;

accessing, by the processor, data from a proximity sensor to detect a distance between the mobile device and a user;

activating a camera to take an image of the user and detect a number of faces visible in the image;

obscuring at least a portion of the sensitive information displayed in the one or more fields when any predefined conditions are not met, including: determining that the roll and pitch viewing angles are not within pitch and roll threshold values, or that the detected distance between the mobile device and the user is not within distance threshold values, or that multiple faces are detected in the image; and

once all the predefined conditions are met, enabling the window or page to display the sensitive information in the one or more fields to the user.

9. The method of claim 8, further comprising displaying the window or page by a graphical user interface of an operating system or an application, the window or page comprising one or more data fields and corresponding field labels.

10. The method of claim 8, further comprising obscuring the portion of the sensitive information displayed in the one or more fields until a predefined time limit is reached or until the roll and pitch viewing angles are within the pitch and roll threshold values angles and that the detected the distance between the mobile device and the user is within the distance threshold values.

11. The method of claim 8, further comprising once invoked for a first time or the user indicates they a new user, enrolling the new user, including taking one or more images of a face of the user, converting the one or more images into one or more face templates, and storing the one or more face templates in a face template database.

12. The method of claim 8, further comprising searching for the parsed to data in a classification data store of labels, keywords, and metadata that indicate or are associated with the sensitive information, wherein a match indicates the window or page displays the sensitive information and needs protection, while a non-match indicates the window or page does not display the sensitive information and is safe or insensitive.

13. The method of claim 8, further comprising using one or more of machine learning (ML) models that are trained to process the parsed data and return a classification of whether the window or page is sensitive or in-sensitive.

14. The method of claim 8, further comprising responsive to determining that the roll and pitch viewing angles are within the pitch and roll threshold values, and that the detected distance between the mobile device and the user is within the distance threshold values, and that a single face is detected in the image, allowing an application to display the sensitive information.

15. The method of claim 8, further comprising classifying a viewing environment to be unsafe responsive to determining that the roll and pitch viewing angles are not within the pitch and roll threshold values, or that the detected distance between the mobile device and the user is not within the distance threshold values, or that multiple faces are detected in the image, and displaying an override prompt to the user with a UI element to enable the user to override the unsafe viewing environment classification and view the sensitive information.

16. A non-transitory computer-readable medium containing program instructions for protecting a mobile device users from visual hacking, the program instructions when executed by a processor of the mobile device, cause the processor to:

automatically activate an anti-hacking application when the processor displays a window or page on a screen of the mobile device that includes one or more data fields for viewing or entry of sensitive information; and

responsive to determining that the one or more fields display sensitive information:

using, by the anti-hacking application, a combination of a gyroscope, a camera and a proximity sensor of the mobile device to reduce a potential of visual hacking by:

using the gyroscope to detect horizontal and vertical viewing angles of the mobile device as held by a user;

using the proximity sensor to detect a distance between the mobile device and the user;

causing the camera to capture an image of the user and detecting a number of faces in the image; and

responsive to the anti-hacking application detecting that the mobile device is not held at correct horizontal and vertical viewing angles or is not held at a correct distance, or detecting multiple faces in the image, temporarily hiding the sensitive information from view.

17. The non-transitory computer-readable medium of claim 16, wherein the anti-hacking application begins by parsing the data fields displayed on the screen of the mobile device, and using at least labels of the one or more data fields to classify the window or page as having one or more fields that display the sensitive information.

18. The non-transitory computer-readable medium of claim 16, wherein the anti-hacking application compares the horizontal and vertical viewing angles to pitch and roll threshold values and compares the distance to distance threshold values.

19. The non-transitory computer-readable medium of claim 18, wherein the anti-hacking application hides the sensitive information from view responsive to determining that the horizontal and vertical viewing angles are not with pitch and roll threshold values, or that the detected distance between the mobile device and the user is not within the distance threshold values.