

One currently available system which was designed to prevent phishing attacks is known as "SiteKey". SiteKey is a web-based security authentication system which ask a series of identity questions to increase security. A user identifies him/herself to a website by entering his/her username (but not password). If the username is valid, an image and accompanying phrase is displayed which has been previously configured to the user. If the user does not recognise the image and phrase as his/her own, the user assumes the site is a phishing site and abandons the login. If the user does recognise the image and phrase, the user may consider the site authentic and proceed with the login process.

However weaknesses have been found in the SiteKey system. Most importantly, it offers no immunity against some of the most common phishing scenarios, as it compromises user privacy by requiring users to disclose personal information in response to the questions, it is susceptible to man-in-the-middle attack, and it allows bulk harvesting of usernames. It has also been found that users are prone to provide their login credentials even in the absence of the SiteKey image and phrase appearing. Accordingly, it has not been entirely successful and has in some cases lead to increased incidents of identity theft because personal information is exposed and the phisher can still illicit information from targets relatively easily.

There is accordingly a need for improving the security to a user when entering login credentials to access a user account, to inhibit at least some of the above described security threats.

SUMMARY OF THE INVENTION

Broadly, the present invention uses a graphical display access interface to display a predetermined character set for the user to select one or more characters which comprise at least one unique security identifier.

In one aspect, there is provided a method for providing access to a user account via an electronic device having a visual display screen, the method including the steps of: issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; providing an access interface on

said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier; allowing said user to input said security identifier by selecting
5 characters on the graphical display character set; and comparing said entered security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

In a second aspect, there is provided a system for providing access to a user account via an electronic device having a visual display screen, including:
10 communication means for issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; a database for storing said at least one security identifier and said predetermined character set; a processor for
15 providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier; and for comparing said security identifier entered by said user on the graphical display character set to the security
20 identifier stored in said database, and for comparing said security identifier entered to a predetermined security identifier stored in said database, and if comparison is successful, providing access to said user account.

In a third aspect, there is provided a system for providing access to a user account via an electronic device having a visual display screen, including: first
25 communication means for receiving at least one security identifier, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; an electronic device having a visual display screen adapted for requesting access to a user account, and for
30 receiving an access interface to input said security identifier, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier, and for

accessing said user account if comparison between said security Identifier entered to a predetermined security identifier stored in a database is successful.

In a fourth aspect, there is provided a system for providing access to a user account, including: communication means for receiving a request to access
5 said user account, and for sending an access interface in response to said request, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising a security Identifier having one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined
10 character set is a non alpha-numeric character; and a processor for receiving and comparing said security Identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

There is further provided a software product operatively adapted to implement the method of the first aspect.

15 In one form, the predetermined character set is unique to a subset of users. This enhances the security of the system since the set of characters is different for different user or subsets of users, increasing the possible number of characters to be guessed in a password guessing program for example.

In another form, the predetermined character set is proprietary to the user
20 account administrator. Again, a password guessing program for example would have difficulty determining the character set for a user since each administrator, for example each institution, can design their own character set. Combined with different character sets for subsets of users provides even more security.

Preferably, the user is required to progressively input more than one
25 security Identifier, ideally with each of these on a separate login screen with separate customised graphical display character set to enhance security. For example, the user may need to enter a username, followed by a password, and followed by a PIN. In other forms, the same character set may be used for each login screen, or there may be only a single login screen.

30 The predetermined character set for each issued security Identifier may be different, again assisting with enhancing security of the access system.

It is preferred that the user inputs the security Identifier by selecting the characters on the graphical display character set via a pointer driven device or a

5a

touch screen. In this way, key loggers are inhibited from recording keystrokes on a traditional keyboard and thereby causing unauthorised access to a user's details. However, in another form a selection of keyboard keys could be used to select the characters displayed, for example the tab and arrow keys.

- 5 Alternatively, the user may input a part of the security identifier by selecting at least one character on the graphical display character set, and part of the security identifier by selecting keys on a traditional keyboard.

Advantageously, the graphical display character set may be displayed in different orders or orientations for each attempted access, to further inhibit key loggers from accessing user details.

5 To inhibit password guessing programs, it is preferred that access to the user account is rejected if an incorrect security identifier is inputted a predetermined number of times. Furthermore, it is also preferred that access to the user account is rejected if an excluded character is selected, *ie* a character that is outside the allowed graphical display character set.

10 In another form, the predetermined character set and security identifier may be variable for each user to increase the numbers of possible options and increase the difficulty in guessing a user's identifier.

For some administrators or institutions, the access interface may further include an advertising display to allow an administrator to obtain additional financial benefits from use of its system.

15 Forms of the present invention improve security to a user when entering identification details to access a user account by inhibiting the threats of keyboard logging, skimming devices, password guessers and/or phishing. For example, phishing scams will be defeated by the use of a customized graphical key character set unique for each user that is linked to their fixed account name and will only be presented to them at logon. In this way if the customer is tricked in to going to an invalid site it will not have the necessary custom character set to enable the client to input their security ID. This is compounded if multiple login screens with different character sets are deployed. Key logging will also be defeated by failing to use known keyboard layouts, and in particular standard
20 keyboards, to enter security IDs. Furthermore, even if key strokes are captured the value of the selected character will be unknown to a third party, and if the character layout is varied for each login, will be very difficult for a third party to log or guess. Password guessers will also be defeated by failing to include standard alphabet and numerical characters in a security ID, and furthermore by using
25 characters proprietary to an administrator/institution will make the guessing a password very difficult. Randomising the order and location of the characters during login inhibits the ability for skimming device access to a security ID.
30

It is envisaged that this invention will also help to protect against domain address spoofing, hijacking and redirection techniques that divert legitimate internet traffic to a false site to harvest user login credentials intermittently, as it will not be possible for the user to enter their codes as the required character sets
5 will not exist.

BRIEF DESCRIPTION OF THE DRAWINGS

An illustrative embodiment of the present invention will now be described with reference to the accompanying figures. Further features and advantages of the invention will also become apparent from the accompanying description.

10 Figure 1 is a contextual diagram providing an overview of the system in one embodiment of the present invention;

Figures 2a to 2j (hereinafter "Figure 2") show a flowchart of an exemplary method for implementing the present invention;

15 Figure 3 is a summary overview of a set up process for implementing the method of Figure 2;

Figure 4 is an exemplary Level 1 entry access interface and graphical display character set using the field name "username";

Figure 5 is an exemplary Level 2 entry access interface and graphical display character set using the field name "password";

20 Figure 6 is an exemplary Level 3 entry access interface and graphical display character set using the field name "PIN";

Figure 7 is an exemplary security ID creation access interface and graphical display character set;

25 Figure 8 is an exemplary administrator database table for security ID settings of a particular user;

Figure 9 is an exemplary administrator database table for logon settings for a particular user;

Figure 10 is an exemplary master character set table;

Figure 11 is another exemplary master character set table; and

30 Figure 12 is an exemplary security ID access interface in another embodiment where traditional keyboard characters are used.

CLAIMS:

1. A method for providing access to a user account via an electronic device having a visual display screen, the method including the steps of:

issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character;

providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier;

allowing said user to input said security identifier by selecting characters on the graphical display character set; and

comparing said entered security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

2. A method according to claim 1, wherein the predetermined character set is unique to a subset of users.

3. A method according to claim 1, wherein the predetermined character set is proprietary to the user's account administrator.

4. A method according to claim 1, wherein the user is required to progressively input more than one security identifier to enhance security.

5. A method according to claim 4, wherein the predetermined character set for each security identifier is different.

6. A method according to any one of claims 4 or 5, wherein each security identifier is entered on a separate interface.

7. A method according to claim 1, wherein the user inputs said security identifier by selecting the characters on the graphical display character set via a pointer driven device or a touch screen.
8. A method according to claim 1, wherein the graphical display character set is displayed in different orders or orientations for each attempted access.
9. A method according to claim 1, further including the step of rejecting access to the user account if an excluded character is selected from the graphical display character set.
10. A method according to claim 1, further including the step of rejecting access to the user account if an incorrect security identifier is inputted a predetermined number of times.
11. A method according to claim 1, wherein the user inputs a part of said security identifier by selecting at least one character on the graphical display character set, and part of said security identifier by selecting keys on a traditional keyboard.
12. A method according to claim 1, wherein the predetermined character set and security identifier is variable for each user.
13. A method according to claim 1, wherein the access interface further includes an advertising display.
14. A method according to claim 1, wherein the characters in the predetermined character set include one or more of character types selected from the group consisting of: alpha-numeric, punctuation marks, images/pictures and colours.
15. A system for providing access to a user account via an electronic device having a visual display screen, including:

communication means for issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character;

a database for storing said at least one security identifier and said predetermined character set;

a processor for providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier; and for comparing said security identifier entered by said user on the graphical display character set to the security identifier stored in said database, and for comparing said security identifier entered to a predetermined security identifier stored in said database, and if comparison is successful, providing access to said user account.

16. A system for providing access to a user account via an electronic device having a visual display screen, including:

communication means for receiving at least one security identifier, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character;

an electronic device having a visual display screen adapted for requesting access to a user account, and for receiving an access interface to input said security identifier, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier, and for accessing said user account if comparison between said security identifier entered to a predetermined security identifier stored in a database is successful.

17. A system for providing access to a user account, including:

communication means for receiving a request to access said user account, and for sending an access interface in response to said request, wherein the access interface includes a graphical display character set which includes a

graphical representation of at least the characters comprising a security identifier having one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; and

a processor for receiving and comparing said security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

18. A system according to any one of claims 15 to 17, wherein the predetermined character set is unique to a subset of users.

19. A system according to any one of claims 15 to 17, wherein the predetermined character set is proprietary to the user's account administrator.

20. A system according to any one of claims 15 to 17, wherein the security identifier is inputted by selecting the characters on the graphical display character set via a pointer driven device or a touch screen.

21. A system according to any one of claims 15 to 17, wherein the graphical display character set is displayed in different orders or orientations for each attempted access.

22. A system according to any one of claims 15 to 17, the processor being further configured for rejecting access to the user account if an excluded character is selected from the graphical display character set.

23. A system according to any one of claims 15 to 17, the processor being further configured for rejecting access to the user account if an incorrect security identifier is inputted a predetermined number of times.

24. A system according to any one of claims 15 to 17, wherein the security identifier is partially inputted by selecting at least one character on the graphical display character set, and partially inputted by selecting keys on a traditional keyboard.

25. A system according to any one of claims 15 to 17, wherein the predetermined character set and security identifier is variable for each user.

26. A system according to any one of claims 15 to 17, wherein the access interface further includes an advertising display.

27. A system according to any one of claims 15 to 17, wherein the characters in the predetermined character set include one or more of character types selected from the group consisting of: alpha-numeric, punctuation marks, images/pictures and colours.

28. A software product operatively adapted to implement the method according to any one of claims 1 to 14.

One currently available system which was designed to prevent phishing attacks is known as “SiteKey”. Sitekey is a web-based security authentication system which ask a series of identity questions to increase security. A user identifies him/herself to a website by entering his/her username (but not password). If the username is valid, an image and accompanying phrase is displayed which has been previously configured to the user. If the user does not recognise the image and phrase as his/her own, the user assumes the site is a phishing site and abandons the login. If the user does recognise the image and phrase, the user may consider the site authentic and proceed with the login process.

However weaknesses have found in the SiteKey system. Most importantly, it offers no immunity against some of the most common phishing scenarios, as it comprises user privacy by requiring users to disclose personal information in response to the questions, it is susceptible to man-in-the-middle attack, and it allows bulk harvesting of usernames. It has also been found that users are prone to provide their login credentials even in the absence of the SiteKey image and phrase appearing. Accordingly, it has not been entirely successful and has in some cases lead to increased incidents of identity theft because personal information is exposed and the phisher can still illicit information from targets relatively easily.

There is accordingly a need for improving the security to a user when entering login credentials to access a user account, to inhibit at least some of the above described security threats.

SUMMARY OF THE INVENTION

The invention is defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

Broadly, the implementation of the techniques disclosed herein uses a graphical display access interface to display a predetermined character set for the user to select one or more characters which comprise at least one unique security identifier.

In one exemplary technique, there is provided a method for providing access to a user account via an electronic device having a visual display screen, the method including the steps of: issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier, allowing said user to input said security identifier by selecting characters on the graphical display

character set; and comparing said entered security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

In a second exemplary technique, there is provided a system for providing access to a user account via an electronic device having a visual display screen, including; communication means for issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; a database for storing said at least one security identifier and said predetermined character set; a processor for providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier; and for comparing said security identifier entered by said user on the graphical display character set to the security identifier stored in said database, and for comparing said security identifier entered to a predetermined security identifier stored in said database, and if comparison is successful, providing access to said user account.

In a third exemplary technique, there is provided a system for providing access to a user account via an electronic device having a visual display screen, including; first communication means for receiving at least one security identifier; said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character, an electronic device having a visual display screen adapted for requesting access to a user account, and for receiving an access interface to input said security identifier, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier, and for accessing said user account if comparison between said security identifier entered to a predetermined security identifier stored in a database is successful.

In a fourth exemplary technique, there is provided a system for providing access to a user account, including; communication means for receiving a request to access said user account; and for sending an access interface in response to said request, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising a security identifier having one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character; and a processor for receiving and comparing

said security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

There is further provided a software product operatively adapted to implement the method of the first exemplary technique.

In one form, the predetermined character set is unique to a subset of users. This enhances the security of the system since the set of characters is different for different user or subsets of users, increasing the possible number of characters to be guessed in a password guessing program for examples.

In another form, the predetermined character set is proprietary to the user account administrator. Again, a password guessing program for example would have difficulty determining the character set for a user since each administrator, for example each institution, can design their own character set. Combined with different character sets for subsets of users provides even more security.

Preferably, the user is required to progressively input more than one security identifier, ideally with each of these on a separate login screen with separate customised graphical display character set to enhance security. For example, the user may need to enter a username, followed by a password, and followed by a PIN. In other forms, the same character set may be used for each login screen, or there may be only a login screen.

The predetermined character set for each issued security identifier may be different, again assisting with enhancing security of the access systems.

It is preferred that the user inputs the security identifier by selecting the characters on the graphical display character set via a pointer driven device or a touch screen. In this way, key loggers are inhibited from recording keystrokes on a traditional keyboard and thereby causing unauthorised access to a user's details. However, in another form a selection of keyboard keys could be used to select the characters displayed, for example the tab and arrow keys.

Alternatively, the user may input a part of the security identifier by selecting at least one character on the graphical display character set, and part of the security identifier by selecting keys on a traditional keyboard.

Advantageously, the graphical display character set may be displayed in different orders or orientations for each attempted access, to further inhibit key loggers from accessing user details.

To inhibit password guessing programs, it is preferred that access to the user account is rejected if an incorrect security identifier is inputted a predetermined number of times. Furthermore, it is also preferred that access to the user account is rejected if an excluded character is selected, ie a character that is outside the allowed graphical display character set.

In another form, the predetermined character set and security identifier may be variable for each user to increase the numbers of possible options and increase the difficulty in guessing a user's identifier.

For some administrators or institutions, the access interface may further include an advertising display to allow an administrator to obtain additional financial benefits from use of its system.

Implementation of the techniques disclosed herein may improve security to a user when entering identification details to access a user account by inhibiting the threats of keyboard logging, skimming devices, password guessers and/or phishing. For example, phishing scams will be defeated by the use of a customized graphical key character set unique for each user that is linked to their fixed account name and will only be presented to them at logon. In this way if the customer is tricked in to going to an invalid site it will not have the necessary custom character set to enable the client to input their security ID. This is compounded if multiple login screens with different character sets are deployed. Key logging will also be defeated by failing to use known keyboard layouts, and in particular standard keyboards, to enter security IDs. Furthermore, even if key strokes are captured the value of the selected character will be unknown to a third party, and if the character layout is varied for each login, will be very difficult for a third party to log or guess. Password guessers will also be defeated by failing to include standard alphabet and numerical characters in a security ID, and furthermore by using characters proprietary to an administrator/institution will make the guessing a password very difficult. Randomising the order and location of the characters during login inhibits the ability for skimming device access to a security ID.

It is envisaged that implementation of the techniques disclosed herein may also help to protect against domain address spoofing, hijacking and redirection techniques that divert legitimate internet traffic to a false site to harvest user login credentials intermittently, as it will not be possible for the user to enter their codes as the required character sets will not exist.

BRIEF DESCRIPTION OF THE DRAWINGS

An illustrative embodiment of the present invention will now be described with reference to the accompanying figures. Further features and advantages of the invention will also become apparent from the accompanying description.

Figure 1 is a contextual diagram providing an overview of the system in one embodiment of the present invention;

Figures 2a to 2j (hereinafter "Figure 2") show a flowchart of an exemplary method for implementing the present invention;

Figure 3 is a summary overview of a set up process for implementing the method of Figure 2;

Figure 4 is an exemplary Level 1 entry access interface and graphical display character set using the field name "username";

Figure 5 is an exemplary Level 2 entry access interface and graphical display character set using the field name "password";

Figure 6 is an exemplary Level 3 entry access interface and graphical display character set using the field name "PIN";

Figure 7 is an exemplary security ID creation access interface and graphical display character set;

Figure 8 is an exemplary administrator database table for security ID settings of a particular user;

Figure 9 is an exemplary administrator database table for logon settings for a particular user;

Figure 10 is an exemplary master character set table;

Figure 11 is another exemplary master character set table; and

Figure 12 is an exemplary security ID access interface in another embodiment where traditional keyboard characters are used.

CLAIMS:

1. A method for providing access to a user account via an electronic device having a visual display screen, the method including the steps of:

issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character, said predetermined character set being unique to a subset of users;

providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier;

allowing said user to input said security identifier by selecting characters on the graphical display character set; and

comparing said entered security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

2. A method according to claim 1, wherein the predetermined character set is proprietary to the user's account administrator.

3. A method according to claim 1, wherein the user is required to progressively input more than one security identifier to enhance security.

4. A method according to claim 3 wherein the predetermined character set for each security identifier is different.

5. A method according to any one of claims 3 or 4, wherein each security identifier is entered on a separate interface.

6. A method according to claim 1, wherein the user inputs said security identifier by selecting the characters on the graphical display character set via a pointer driven device or a touch screen.

7. A method according to claim 1, wherein the graphical display character set is displayed in different orders or orientations for each attempted access.
8. A method according to claim 1, further including the step of rejecting access to the user account if an excluded character is selected from the graphical display character set.
9. A method according to claim 1, further including the step of rejecting access to the user account if an incorrect security identifier is inputted a predetermined number of times.
10. A method according to claim 1, wherein the user inputs a part of said security identifier by selecting at least one character on the graphical display character set, and part of said security identifier by selecting keys on a traditional keyboard.
11. A method according to claim 1, wherein the predetermined character set and security identifier is variable for each user.
12. A method according to claim 1, wherein the access interface further includes an advertising display.
13. A method according to claim 1, wherein the characters in the predetermined character set include one or more of character types selected from the group consisting of: alpha-numeric, punctuation marks, images/pictures and colours.
14. A system for providing secure access to a user account via an electronic device having a visual display screen, including:
communication means for issuing at least one security identifier to the user, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character, said predetermined character set being unique to a subset of users;

a database for storing said at least one security identifier and said predetermined character set;

a processor for providing an access interface on said visual display screen for said user to input said security identifier, wherein said access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier; and for comparing said security identifier entered by said user on the graphical display character set to the security identifier stored in said database, and for comparing said security identifier entered to a predetermined security identifier stored in said database, and if comparison is successful, providing access to said user account.

15. A system for providing secure access to a user account via an electronic device having a visual display screen, including:

communication means for receiving at least one security identifier, said security identifier including one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-numeric character, said predetermined character set being unique to a subset of users;

an electronic device having a visual display screen adapted for requesting access to a user account, and for receiving an access interface to input said security identifier, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising the security identifier, and for accessing said user account if comparison between said security identifier entered to a predetermined security identifier stored in a database is successful.

16. A system for providing secure access to a user account, including:

communication means for receiving a request to access said user account, and for sending an access interface in response to said request, wherein the access interface includes a graphical display character set which includes a graphical representation of at least the characters comprising a security identifier having one or more characters chosen from a predetermined character set, wherein at least one of the characters in the predetermined character set is a non alpha-

numeric character, said predetermined character set being unique to a subset of users; and

a processor for receiving and comparing said security identifier to a predetermined security identifier stored in a database, and if comparison is successful, providing access to said user account.

17. A system according to any one of claims 14 to 16, wherein the predetermined character set is proprietary to the user's account administrator.

18. A system according to any one of claims 14 to 16, wherein the security identifier is inputted by selecting the characters on the graphical display character set via a pointer driven device or a touch screen.

19. A system according to any one of claims 14 to 16 wherein the graphical display character set is displayed in different orders or orientations for each attempted access.

20. A system according to any one of claims 14 to 16, the processor being further configured for rejecting access to the user account if an excluded character is selected from the graphical display character set.

21. A system according to any one of claims 14 to 16, the processor being further configured for rejecting access to the user account if an incorrect security identifier is inputted a predetermined number of times.

22. A system according to any one of claims 14 to 16, wherein the security identifier is partially inputted by selecting at least one character on the graphical display character set, and partially inputted by selecting keys on a traditional keyboard.

23. A system according to any one of claims 14 to 16, wherein the predetermined character set and security identifier is variable for each user.

24. A system according to any one of claims 14 to 16, wherein the access interface further includes an advertising display.

25. A system according to any one of claims 14 to 16, wherein the characters in the predetermined character set include one or more of character types selected from the group consisting of: alpha-numeric, punctuation marks, images/pictures and colours.

26. A software product operatively adapted to implement the method according to any one of claims 1 to 13.