CLAIMS

1. A computer-implemented method, comprising:

determining that no password is required for connecting to a wireless network;

in response to determining that no password is required for connecting to the wireless network, retrieving data from at least two predefined network addresses through the wireless network, wherein the at least two predefined network addresses comprise a first network address to access first web page data and a second network address to access second web page data, wherein the first network address is associated with a first web page and the second network address is associated with a second web page that is different from the first web page; and

determining that a secondary login verification is required for connecting to the wireless network based on, at least, determining, by comparing the first web page data and the second web page data, that accessing the first web page and accessing the second web page both jump to a secondary login verification page, wherein determining that accessing the first web page and accessing the second web page both jump to the secondary login verification page comprises:

updating the first web page data and the second web page data, wherein the updating comprises:

deleting the first network address comprised in the first web page data and deleting the second network address comprised in the second web page data; or

replacing the first network address comprised in the first web page data and the second network address comprised in the second web page data with unified identification data;

comparing the updated first web page data and the updated second web page data to determine whether the updated first web page data and the updated second web page data are the same; and

determining, based on a comparison result, that accessing the first web page and accessing the second web page both jump to the secondary login verification page.

2. The method according to claim 1, comprising:

in response to determining that the wireless network is unsecure, blocking access by an electronic device to the wireless network.

3. The method according to claim 2, comprising providing a security risk warning to a user of the electronic device.

4. The method according to any one of claims 1 to 3, wherein determining that no password is required for connecting to the wireless network comprises:

calling a wireless network password management interface provided by an operating system;

obtaining a call result; and

determining, based on the call result, that no password is required for connecting to the wireless network.

5. The method according to any one of claims 1 to 4, comprising:

determining, based on accessing a specified network address, that a secondary login verification is required for connecting to the wireless network, wherein the specified network address comprises a network address of a user-defined API for an enterprise, and wherein the user-defined API is used to return specified identification information when the user-defined API is accessed.

6. The method according to claim 5, wherein determining, based on accessing a specified network address, that a secondary login verification is required for connecting to the wireless network comprises:

obtaining an access result of accessing the network address of the user-defined API;

determining that the access result does not comprise the specified identification information; and

in response to determining that the access result does not comprise the specified identification information, determining that a secondary login verification is required for connecting to the wireless network.

7. The method according to claim 1, wherein the first web page data comprises the first network address, wherein the second web page data comprises the second network address.

8. An electronic device, comprising:

a processor; and

a memory, configured to store an instruction that can be executed by the processor, wherein the processor is configured to:

determine that no password is required for connecting to a wireless network;

in response to determining that no password is required for connecting to the wireless network, retrieve data from at least two predefined network addresses through the wireless network, wherein the at least two predefined network addresses comprise a first network address to access first web page data and a second network address to access second web page data, wherein the first network address is associated with a first web page and the second network address is associated with a second web page that is different from the first web page; and

determine that a secondary login verification is required for connecting to the wireless network based on, at least, determining, by comparing the first web page data and the second web page data, that accessing the first web page and accessing the second web page both jump to a secondary login verification page, wherein determining that accessing the first web page and accessing the second web page both jump to the secondary login verification page comprises:

updating the first web page data and the second web page data, wherein the updating comprises:

deleting the first network address comprised in the first web page data and deleting the second network address comprised in the second web page data; or

replacing the first network address comprised in the first web page data and the second network address comprised in the second web page data with unified identification data;

comparing the updated first web page data and the updated second web page data to determine whether the updated first web page data and the updated second web page data are the same; and

determining, based on a comparison result, that accessing the first web page and accessing the second web page both jump to the secondary login verification page.

9. The device according to claim 8, wherein the memory comprises a wireless network type detection apparatus that is configured to perform the method according to any one of claims 1 to 7.