CLAIMS

What is claimed is:

1. A method for application information risk management on a network device, the method comprising:

receiving target application information that a user selects and requests for validation by using a user device (S31), wherein the target application information comprises an SMS message;

validating the target application information to determine corresponding risk information (S32);

transmitting a rogue base station prompt information to the user device based on the corresponding risk information (S33);

wherein, if the corresponding risk information indicates that the SMS message comprises false information sent by a rogue based station, the method further comprises:

sending the rogue base station prompt information to other user devices near the user device, wherein a distance between each other user device and the user device is less than or equal to a predetermined device distance threshold.

2. The method of claim 1, wherein validating the target application information to obtain corresponding risk information comprises:

performing match querying in a corresponding validation database based on a related attribute information of the target application information; and

determining the corresponding risk information based on a record information that is in the validation database and that matches the related attribute information.

3. The method of claim 2, wherein the validation database comprises at least one of a library of message templates and a grade that enables successive validation of the target application information.

4. The method of claim 2, wherein the related attribute information comprises at least one of the following:

a sender information of the target application information;

a content of the target application information; or

a user guide information of the target application information.

5. The method of claim 4, wherein:

the related attribute information comprises the user guide information of the target application information, and

validating the target application information to obtain corresponding risk information further comprises, if no record information that matches the user guide information is identified in the validation database, simulating an execution of the target application information based on the user guide information to obtain the corresponding risk information.

6. The method of claim 5, wherein simulating the execution of the target application information based on the user guide information to obtain the corresponding risk information comprises:

simulating acquiring, based on the user guide information, target information that is in the target application information and that the user is guided to acquire; and

validating a correspondence between the target information and the target application information to obtain the corresponding risk information.

7. The method of claim 6, wherein validating the correspondence between the target information and the target application information comprises at least one of the following:

checking whether a sender information of the target information is consistent with the sender information of the target application information;

checking whether a content of the target information is associated with the content of the target application information; and

checking whether a sandbox operation information of the target information matches the target application information.

8. The method of claim 1, wherein the SMS message comprises a Smishing message.

9. An apparatus for application information risk management, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 8.