

Claims

1. An account theft risk identification method, comprising:
 - collecting device information of a device that bears an operation behavior according to information about the current operation behavior (S210);
 - acquiring all user identity information of historical operation behaviors on the device within a preset time period prior to the current operation behavior (S220);
 - analyzing a user identity analysis location represented in each piece of user identity information, and counting the number of user identity analysis locations on the device in the time period (S230); and
 - determining whether the current operation behavior has an account theft risk according to the number of user identity analysis locations on the device in the time period (S240).
2. The risk identification method of claim 1, wherein the user identity information comprises credential information in user registration information; and
 - the step of analyzing a user identity analysis location represented in each piece of user identity information, and counting the number of user identity analysis locations on the device in the time period specifically comprises:
 - acquiring the user identity analysis location according to a credential type and a credential number in each piece of user registration information, and
 - counting the number of user identity analysis locations on the device.
3. The risk identification method of claim 2, wherein the step of acquiring the user identity analysis location according to a credential type and a credential number in each piece of user registration information, and counting the number of user identity analysis locations on the device comprises:
 - determining an analysis mode for the user identity analysis location according to a class of the credential type; and
 - analyzing the first six digits of each credential number to acquire the user identity analysis location when the credential type is a Chinese domestic resident ID card, and counting the number of user identity analysis locations on the device accordingly; or

presuming that each credential type or each credential number corresponds to one user identity analysis location when the credential type is a Chinese domestic non-resident ID card or a foreign credential, and counting the number of user identity analysis locations on the device accordingly.

4. The risk identification method of claim 1, wherein the step of collecting device information of a device that bears an operation behavior according to information about the current operation behavior comprises:

acquiring corresponding device information of the device by collecting a device identification code of the device.

5. The risk identification method of claim 4, wherein the step of acquiring corresponding device information of the device by collecting a device identification code of the device comprises:

determining content of the collected device information according to a type of the device; wherein the collected device information comprises a MAC, an IP and/or a UMID when the device is a PC; and

the collected device information comprises a MAC, an IMEI, a TID and/or a mobile phone number when the device is a mobile terminal.

6. The risk identification method of claim 4, wherein the step of acquiring corresponding device information of the device by collecting a device identification code of the device comprises:

determining a mode of counting the number of user identity analysis locations on the device according to a device quantity identified from the device identification code;

analyzing and counting, when a unique device is identified, the number of user identity analysis locations on the device; or

analyzing and counting, when multiple devices are identified, the number of user identity analysis locations on each device; or

setting the number of user identity analysis locations on the device as 0 when no device is identified; and

using the obtained number of user identity analysis locations on the device as an input variable of a preset scoring model, to evaluate an account theft risk level of the device.

7. The risk identification method of any of claims 1 to 6, wherein the step of determining whether the current operation behavior has an account theft risk according to the number of user identity analysis locations on the device in the time period comprises:

evaluating an account theft risk level of a user of the current operation behavior in combination with the total number of users on the device, the number of mobile phone numbers bound to the user of the current operation behavior, the number of devices for historical operation behaviors of the current user, the number of IP addresses of the historical operation behaviors of the current user, a difference between the information about the current operation behavior and information about the historical operation behaviors of the current user, and/or whether routing characteristic information of the current operation behavior is the same as routing characteristic information of the historical operation behaviors, and optionally wherein the step of determining whether the current operation behavior has an account theft risk according to the number of user identity analysis locations on the device in the time period further comprises calculating an account theft risk value in combination with the account theft risk level of the device and the account theft risk level of the user of the current operation behavior, and identifying an account theft when the risk value is greater than a preset threshold.

8. An account theft risk identification apparatus (300), comprising:

a device information collection module (310) configured to collect device information of a device that bears an operation behavior according to information about the current operation behavior;

a user information acquisition module (320) configured to acquire all user identity information of historical operation behaviors on the device within a preset time period prior to the current operation behavior;

a user identity analysis module (330) configured to analyze a user identity analysis location represented in each piece of user identity information, and count the number of user identity analysis locations on the device in the time period; and

an account theft risk evaluation module (340) configured to determine whether the current operation behavior has an account theft risk according to the number of user identity analysis locations on the device in the time period.

9. The risk identification apparatus (300) of claim 8, wherein the user identity information comprises credential information in user registration information; and

the user identity analysis module (330) acquires the user identity analysis location according to a credential type and a credential number in each piece of user registration information, and counts the number of user identity analysis locations on the device.

10. The risk identification apparatus of claim 9, wherein the user identity analysis module (330) determines an analysis mode for the user identity analysis location according to a class of the credential type; and

analyzes the first six digits of each credential number to acquire the user identity analysis location when the credential type is a Chinese domestic resident ID card, and counts the number of user identity analysis locations on the device accordingly; or

presumes that each credential type or each credential number corresponds to one user identity analysis location when the credential type is a Chinese domestic non-resident ID card or a foreign credential, and counts the number of user identity analysis locations on the device accordingly.

11. The risk identification apparatus of claim 8, wherein the device information collection module (310)

acquires corresponding device information of the device by collecting a device identification code of the device, and optionally wherein the device information collection module determines content of the collected device information according to a type of the device, wherein the collected device information comprises a MAC, an IP and/or a UMID when the device is a PC and the collected device information comprises a MAC, an IMEI, a TID and/or a mobile phone number when the device is a mobile terminal.

12. The risk identification apparatus of claim 8, wherein the user identity analysis module (330) determines a mode of counting the number of user identity analysis locations on the device according to a device quantity identified by the device information collection module from the device identification code;

analyzes and counts, when a unique device is identified, the number of user identity analysis locations on the device; or analyzes and counts, when multiple devices are identified, the number of user identity analysis locations on each device; or sets the number of user identity analysis locations on the device as 0 when no device is identified; and

uses the obtained number of user identity analysis locations on the device as an input variable of a preset scoring model of the account theft risk evaluation module, to evaluate an account theft risk level of the device.

13. The risk identification apparatus of any of claims 8 to 12, wherein the account theft risk evaluation module (340) evaluates an account theft risk level of a user of the current operation behavior in combination with the total number of users on the device, the number of mobile phone numbers bound to the user of the current operation behavior, the number of devices for historical operation behaviors of the current user, the number of IP addresses of the historical operation behaviors of the current user, a difference between the information about the current operation behavior and information about the historical operation behaviors of the current user, and/or whether routing characteristic information of the current operation behavior is the same as routing characteristic information of the historical operation behaviors, and optionally wherein the account theft risk evaluation module calculates an account theft risk value in combination with the account theft risk level of the device and the account theft risk level of the user of the current operation behavior, and identifies an account theft when the risk value is greater than a preset threshold.

14. An account theft risk prevention and control system, comprising the risk identification apparatus (300) of any of claims 8 to 13, an account theft reporting apparatus (200), and a risk processing apparatus (100), wherein

the risk identification apparatus (300) is configured to calculate an account theft risk value in an operation behavior platform, and identify an account theft when the risk value is greater than a preset threshold;

the account theft reporting apparatus (200) is configured to report an account theft message to the risk processing apparatus and a user receiving device when the risk identification apparatus (300) identifies an account theft; and

the risk processing apparatus (300) is configured to block a stolen account of a user and intercept risk data associated with the stolen account when receiving the account theft message.

15. The risk prevention and control system of claim 14, wherein the system comprises a case database configured to store the risk data intercepted by the risk processing apparatus (100), such that the risk processing apparatus (100) examines the risk data and the risk identification apparatus (300) verifies the scoring model.