Team name: EmpowerG Team

Team member 1

Name: Vưu Ngọc Mỹ Linh
Email: togepi.linh.vuu@gmail.com
Phone: 0767181233

Team member 2

Name: Lê Thu Thảo
Email: lethuthao1368@gmail.com
Phone: 0345887096

Team member 3

Name: Trần Thị Li Li
Email: lilitran208@gmail.com
Phone: 0935390208

Team member 4

Name: Nguyễn Thị Thanh Ngân
Email: nganntt99@gmail.com
Phone: 0812768202

Proposal Title

Banking Account Takeover Detection Module

Short description

Account takeover happens quite regularly these days. Safruti (2022) mentioned on Forbes that billions of credentials from social media networks, e-commerce sites and financial applications were stolen and sold on the internet. In banking, the threat is even more severe as the loss would be a significant amount of money. To prevent fraud in banking, especially in cases where scammers log into a bank account and spend money illegally, the Account Takeover Detection

System is proposed to automatically identify the suspicious login and block the account immediately, so that further fraud activities would not occur.

Solution

To auto-detect suspicious login, IP, devices' MAC Addresses, locations and face comparison are used in the system. They are stored in a database to compare with the historical login times.

Specifically, there are three stages for tracking the user's behaviours. When creating an account, the user is asked to provide their photo as a profile picture. In their first login, their IP, device and location are stored as default information. Following times, whenever the account is accessed, those details are tracked and compared with the historical data. If all of those are different from the history, the system asks the user to capture their face and compares it with the profile picture. If it is matched, the user will successfully log in. Otherwise, an alert will be sent to the account owner via SMS and email, and the account will be blocked temporarily until the real user asks to unblock it.

Some challenges should be considered. Users are asked to share their location every time they use the service. It can be annoying when they are on holiday and use new devices as they would be detected as strangers and need to verify their faces.

To conclude, the proposed system helps protect the user from account takeover, outweighing small complex steps that they need to take when they are not in their daily lives. If those steps were not checked, the user would lose their money and need to spend time recovering their account.

Innovation, Impact, Integrity, Applicability

Innovation:

- In Vietnam, there is no active prevention of this kind of fraud. Both banks and authorisations provide only suggested action to avoid ATO and then focus on dealing with the result after the crime happened.
- This is a new layer to protect the user's account instead of the incomplete system before (running by human, OTP), which can spot the genuine user.

Impact:

- Although there are some protections like 2FA, and OTP, the ATO still happened (2,500 cases per year - VN government). A more proper solution is that we could authorise the actual user whenever the transaction occurs. This could save millions of dollars (VTV24)
- It will help to improve the brand reputation and could be considered a unique selling point as there are no banks in VN that offer an active solution except for some recommendations. It helps to gain customer trust and loyalty without interfering with the customer experience by taking easy steps to verify.

Integrity:

- Not ask for private permissions that could harm the user, only track user behavior when using the banking app.
- All the information of customers will be encrypted.

Applicability:

- We collect data from the banking app (location, device fingerprinting, internet connection), which can get from proper permissions. Then, we will build a reliable profile for each customer. For face distinguishing, we will train a model to compare the two pictures, the profile picture and the latest one.

Motivation

We would like to join this competition for many reasons. The first one is because of its urgent and exciting topic. This year, we are asked to solve the real problem in banking and financial institution with the help of geolocation technology. Many beloved family members and friends were victims. They lose their accounts with all their savings, which is terrible and unacceptable. We want to do something to prevent this shamed situation.

Besides, we could see the organiser and partners' enthusiasm and the professionalism of judges and mentors. It can be sure that we can learn a lot of new things and experiences from them.

Last but not least, this is “Code like a girl.” We love how our competition tries to empower women in the STEM industry. We believe that, like men, and women, our selves can also do amazing things with our unique characteristics. Let us prove it through this challenge!