

# “I cannot do anything”: User’s Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account

Mahdi Nasrullah Al-Ameen, *Utah State University*  
mahdi.al-ameen@usu.edu

Huzeyfe Kocabas, *Utah State University*  
huzeyfe.kocabas@aggiemail.usu.edu

## Background

- 620 million accounts are stolen from 16 different websites
- **Prior studies focused on:**
  - The security and usability of authentication schemes
  - Users’ password management strategies
  - Automated techniques to detect unauthorized access to user accounts
  - Educational tools to prevent social engineering attacks.
- **There is a gap in understanding:**
  - Users’ behavior upon losing access or identifying an unauthorized access to their online accounts
  - Users’ strategies to protect their accounts in the future

## Methods

- ❑ Semi-structured interview (audio-recorded) with 22 participants in the USA
- ❑ Diverse backgrounds of participants: Mathematics, Learning Science, Architecture, and Engineering
- ❑ Study session: Between 20 and 30 minutes
- ❑ Compensation: \$10 Amazon.com gift card
- ❑ Thematic analysis on transcription

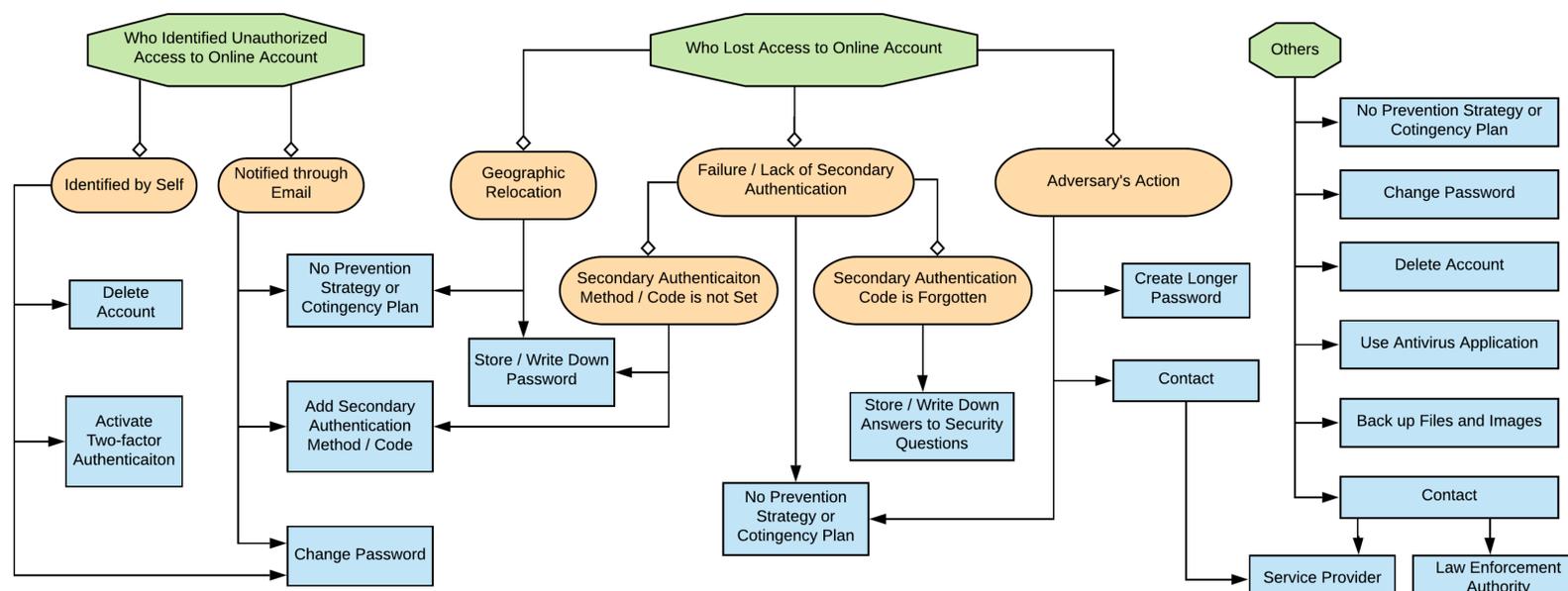


Figure 1: Prevention Strategies and Contingency Plans of Participants to Protect their Online Accounts

## Research Questions

- How do users respond to a situation when they lose access, or identify an unauthorized access to their online account?
- What are the strategies and contingency plans of users to protect their online accounts in the future?

## Future Works

- ❑ A large-scale survey to attain quantitative and more generalizable results
- ❑ Investigating users’ strategies to protect the medium used to write down passwords
- ❑ Exploring the relation between users’ strategies to protect their online accounts and the underlying susceptibility to social engineering attacks

## Findings

- 17 of 22 participants either lost access or identified unauthorized access to their financial or identity accounts.
- **Reasons behind Losing Access to Online Accounts:**
  - Geographic relocation
 

“There was one email account that I lost completely because I had not connect my phone number with it and I tried using it from a different country using a wrong password and it blocked me out.” (P15)
  - Lack or failure of secondary authentication
  - Adversary’s actions
    - User’s prevention strategies could increase security risks
    - Accessibility issues constrain secure behavior
- **Security Misconceptions**
  - Email will notify whenever there is an unauthorized access !
  - Security software, like an antivirus application protects online accounts !
  - “They [adversaries] cannot get my password.” (P06)