Hidden in Plain Bytes: Investigating Interpersonal Account Compromise with Data Exports

Julia Nonnenkamp, Naman Gupta, Abhimanyu Dev Gupta, Rahul Chatterjee
Department of Computer Science, University of Wisconsin–Madison

CCS 2025

Introduction

In intimate partner violence, abusers often exert control by compromising targets' **online accounts**. Account security interfaces (ASIs) like lists of "recent logins" are the main way users check for this. However, prior work shows ASIs often hide past logins or use vague device identifiers [1]. We evaluate whether **personal data exports** required under laws like the GDPR offer more complete indicators of compromise in this threat model.

Research Questions

1. What security information exists in data exports?
2. How does it compare with user interfaces (ASIs)?
3. How well can we reconstruct attacker actions?

Method

We created target and adversary personas with accounts on 6 common platforms: Apple, Google, Facebook, Instagram, Snapchat, and Discord. After 2 months of benign use on two iPhones, we staged 4 attacks: (A1) surveillance via covert logins and (A2) location monitoring; (A3) impersonation (sending & deletion of messages); and (A4) lockout via password reset. After, we requested data exports and repeated attacks 30 days later.

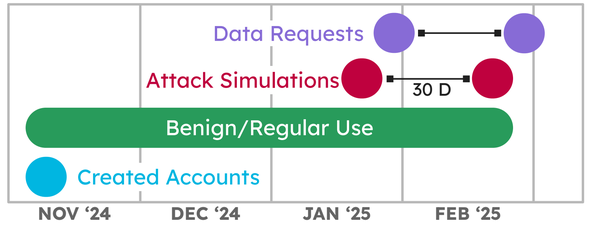


Fig 1. Timeline of simulation method. After 2 months of benign use, all 4 attacks were repeated in two sessions 30 days apart; exports were requested within 8 days of each.

Findings: RQ1 & 2

Coverage varied by platform, but every data export retained longer login history and more granular device identifiers than its ASI (Fig. 2-3).

Event	Src	Apple	Discord	Face-book	Google	Insta-gram	Snap-chat
Active Sessions	*DE*	✓	✓	✓	✓	✓	✓
	ASI	◑	✓	✓	✓	✓	✓
Historical Logins	*DE*	✓	✓	✓	✓	✓	✓
	ASI	×	×	✓	◑	◑	◑
Password Changes	*DE*	✓	×	✓	✓	✓	✓
	ASI	◑	×	◑	◑	✓	×

Fig 2. Security events available in each platform's data export (DE) vs account security interfaces (ASI). ✓ = full history, ◑ = partial, × = not recorded. Data exports contain longer and more complete authentication records.

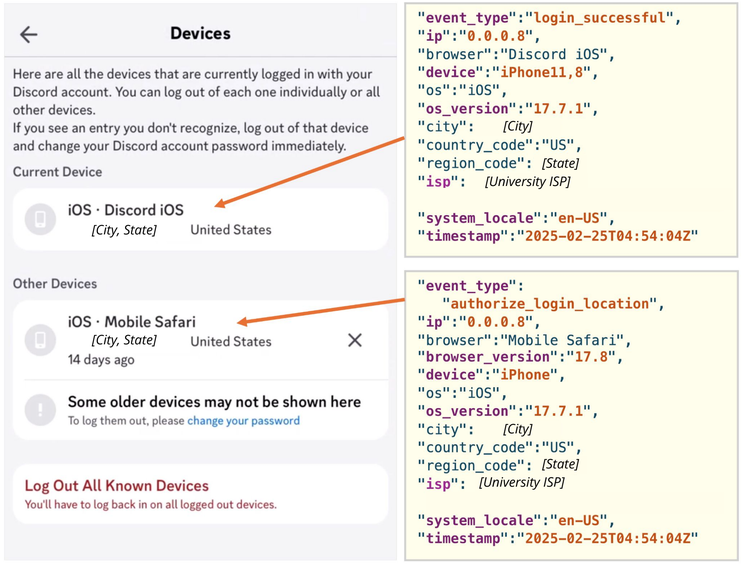


Fig 3. Discord's ASI lists logged-in devices only as "iOS." The matching export entries (right) includes device model, OS version, and IP address.

Findings: RQ3

All 6 platforms recorded authentication events with sufficient device identifiers (IP address, user agent) to distinguish between the two personas' devices. We also examined if exports recorded what the attacker did after authenticating. No platforms retained records of location sharing (e.g., Find My). Discord provided analytics of what pages and messages the attacker browsed. Deleted message contents were unavailable understandably, but only Snapchat and Discord recorded that a deleted message had ever existed (Fig. 4).

Attack	Auth event w/ device ID	Post-auth action w/ device ID
A1 - Surveillance	✓ all 6 platforms	Discord only
A2 - Location Monitoring	—	× not recorded
A3 - Impersonation	✓ all 6 platforms	Discord, Google
A4 - Lockout	✓ all 6 platforms	—

Fig 4. Extent to which various actions could be attributed to the attacker via record linkage on known IDs belonging to the attacker's device. A2 does not have corresponding auth events as it was carried out after A1.

Acknowledgements – Supported by NSF Award #2339679 and the Baldwin Wisconsin Idea Endowment. Archival publication at ACM CCS 2025.

Contact – nonnenkamp@wisc.edu

Paper

[1] A. Daffalla, M. Bohuk, N. Dell, R. Bellini, and T. Ristenpart. 2023. Account Security Interfaces: Important, Unintuitive, and Untrustworthy. *USENIX Security Symposium*.