Verified, But Not Yours?
Risks in the Email Verification Process

Ayushi Mishra, Miuyin Yong Wong, Joseph A. Calandrino*, and Michelle L. Mazurek
*University of Maryland, *Carnegie Mellon University*

1 Introduction

Account creation for websites and online services routinely requires users to submit personal contact information, including an email address. This email address subsequently becomes a channel for account confirmation, promotional communications, credential recovery, and other sensitive transaction notifications [7]. While this communication channel brings clear utility to both service providers and users, it also introduces a key risk: the email address submitted during registration may not belong to the account creator, whether due to an inadvertent error or a deliberate act of impersonation. This creates the potential for problems ranging from abusive subscription (deliberately signing an individual up for services without their permission) to data leakage (sending communications to the wrong individual).

One obvious, and widely adopted, potential solution to this problem is *email verification*: ensuring that the account creator has control of the provided email address by sending some type of validation email and requiring evidence of receipt. However, poorly designed email verification systems may not effectively mitigate potential privacy and security risks that can occur when the *account creator* does not match the *email owner*. For example, verification emails may leak private information about the account creator to the email owner. On the other hand, some systems may allow the account creator to take too many actions before the verification step succeeds, enabling impersonation of the email owner. For example, the account creator may be able to post content, leave comments, or send replies under the email owner's identity prior to verification.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Leibniz University, Hannover, Germany.

Prior work has considered several related issues, including the weakness of email password recovery as a single point of failure [6], the effectiveness of notifying users during registration about previous compromises involving their email addresses [2], identity misbinding vulnerabilities in authentication systems caused by inconsistencies between identities and accounts [5], privacy risks arising from email tracking and information leakage [4], and the general problem of misdirected emails [8]. These works, however, do not directly address the risks posed by email verification itself when the account creator and email owner do not match.

More closely related, Sudhodanan and Paverd investigated *pre-hijacking* [10], in which an attacker creates an account on a platform using a victim's email address, hoping that the victim will later attempt to create an account using a single-sign-on service, allowing the attacker to retain access. Szurdi and Christin examined email typosquatting [11] and showed how mistyped email addresses can expose sensitive information to unintended recipients. These works expose failures and risks related to account registration, but both are significantly more narrowly focused than the broader problems of misconfigured email verification that we study.

- **RQ1**: What types of email verification mechanisms exist?
- **RQ2**: What potential risks arise from mismatches between account creators and email owners?
- **RQ3**: What are the best verification practices to prevent these risks?

Specifically, we systematically test each domain to evaluate what data can be leaked from the account creator to the email owner; what actions the email owner can take upon receiving an unexpected verification email that could harm the account creator (e.g., hijacking the account); and what actions the account creator can take that could potentially harm the email owner (e.g., using up a free trial of a service or posting something embarrassing in the email owner's name). In the process, we categorize the potential harms according to Citron and Solove's taxonomy of privacy harms [3].

Our preliminary results suggest that misconfigured or even missing verification is widespread, with consequences ranging from minor annoyance to serious and significant harms.

2 Methods

We designed a systematic methodology to study the risk associated with verification mechanisms.

Domain selection We sought to study domains in three major categories: popular, less popular, and sensitive. Using the Tranco popularity ranking (January 13 to Feburary 11, 2026) [1], we selected the 300 most *popular* domains and 300 *less popular* domains ranked between 200,000-200,299. In addition, we used keyword search to identify *sensitive* domains dealing with healthcare, dating/relationships, government/politics, religion, gambling, and sex[1] from the complete Tranco list. After filtering for accessibility, English-language support, and signups that do not require Social Security Numbers (SSNs), payment credentials, or government-issued IDs, we evaluated 96 popular and 42 less popular domains (138 total); evaluation of sensitive domains is ongoing.

Evaluation procedure Following domain selection, we systematically tested each platform's registration and email verification workflows to analyze interactions between the account creator and the email owner. The first author manually tested each domain,[2] playing two distinct roles in turn: the account creator who registered the account, and the email owner whose address was used during the signup. As the account creator, we registered the account and recorded any functionality available without confirming control of the associated email address. This included, for example, filling in (fictional) personal details or using any features of the platform when possible. When submitting credit card information was possible, we input a Visa gift card with a small dollar value purchased for the study.

As the email owner, we recorded all received emails, including any personal information, verification links, authentication codes, or account related details contained within the email. We also attempted to hijack the newly created account, by clicking any magic link included in the received email, attempting a password reset, or exploiting any exposed account information provided through the misdirected email. Additionally, we examined whether the email owner could access any sensitive information entered by the account creator, including payment details, saved addresses, subscriptions, and account-specific activities.

To ensure consistency and eliminate interference, each experimental session (one session consists of one domain and either the account creator or email owner role) was conducted in a fresh virtual machine. Unique, fresh email addresses and fictional user profiles were used for each domain. This setup ensured that, e.g., no cookies were shared between the account creator and the email owner, and that all emails received could be traced to one source domain.

All sessions were conducted manually one at a time, minimizing the impact on the tested domains. Sessions were screen-recorded using the cloud recording feature in Zoom [12]. We are currently in the process of notifying tested domains about any potential risks or harms we identified.

3 Results

We highlight our preliminary results on popular and less popular domains below.

Email verification mechanisms Domains we analyzed handle email verification in three main ways: verification required before using the account (79 domains); no verification required (44); and verification with restricted features, meaning some features are restricted until verification is complete (15).

Risks for account creators We identified a range of potential harms to account creators, including account hijacking, data leakage, and economic harm. Overall, 87 accounts (63%) were vulnerable to hijacking (e.g., via password reset). 32 accounts (23%) with potential economic harms largely resulted from saved payment methods, recurring premium subscriptions, and/or automatically renewing memberships that could accrue to the account creator once the account was hijacked. Data leakage (57 domains, 41%) commonly included items such as username or IP address. A few cases included more concerning data, including full home addresses, phone numbers, profile pictures, and login credentials set by the account creator.

Risks for email owners Potential harms to email owners included preventing legitimate registration with their own email address (85 domains, 62%), often requiring account recovery procedures to regain access, as well as loss of signup incentives like free trials or first-time-user discounts (21 domains, 15%). An additional 13 domains (9%) exposed email owners to impersonation-related risks, potentially damaging the email owner reputation or personal relationships through unauthorized interactions conducted in their name. We also observed a substantial number of unsolicited emails, including engagement, newsletter subscriptions, and promotional/marketing emails or general information updates unrelated to specific user actions.

4 Discussion and Ongoing Work

We continue to expand our analysis, including to sensitive domains that may amplify the risks of verification-related failures. We are also in the process of notifying affected domains of our findings. Based on our findings, we hope to identify and disseminate best practices for email verification in order to prevent harms to both email owners and account creators.

[1] Sensitive categories adapted from GDPR's definition [9].

[2] To verify consistency and correctness, 10% of domains were also tested by the second author.

References

[1] Tranco list, 2026.

[2] Yusuf Albayram and Jaden Walker. Investigating effectiveness of informing users about breach status of their email addresses during website registration. *International Journal of Human–Computer Interaction*, 41(13):8066–8085, 2025.

[3] Danielle Keats Citron and Daniel J Solove. Privacy harms. *BUL Rev.*, 102:793, 2022.

[4] Steven Englehardt, Jeffrey Han, and Arvind Narayanan. I never signed up for this! privacy implications of email tracking. *Proceedings on Privacy Enhancing Technologies*, 2018.

[5] Xi Gao, Lei Yu, Houhua He, Xiaoyu Wang, and Yiwen Wang. A research of security in website account binding. *Journal of Information Security and Applications*, 51:102444, 2020.

[6] Lei Jin, Hassan Takabi, and James B.D. Joshi. Security and privacy risks of using e-mail address as an identity. In *2010 IEEE Second International Conference on Social Computing*, pages 906–913, 2010.

[7] Naveen Kumar. 89 email marketing statistics of 2026 (roi & growth data), 2026. Accessed: 2026-01-09.

[8] Emilee Rader and Anjali Munasinghe. "wait, do i know this person?": Understanding misdirected email. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[9] Protection Regulation. Regulation (eu) 2016/679 of the european parliament and of the council. *Regulation (eu)*, 679(2016):10–3, 2016.

[10] Avinash Sudhodanan and Andrew Paverd. Pre-hijacked accounts: An empirical study of security failures in user account creation on the web. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1795–1812, 2022.

[11] Janos Szurdi and Nicolas Christin. Email typosquatting. In *Proceedings of the 2017 internet measurement conference*, pages 419–431, 2017.

[12] Zoom Video Communications. Zoom meetings. https://zoom.us/, 2026.