Quantifying Internet Privacy and Security Risks in Authentication Recovery Channels

Motunrayo Adebayo

Indiana Wesleyan University

DOI: https://dx.doi.org/10.47772/IJRISS.2025.908000647

Received: 22 August 2025; Accepted: 28 August 2025; Published: 25 September 2025

ABSTRACT

Authentication recovery is an important step, yet it has often been overlooked in digital identity systems. In the event where users forget credentials, lose devices, or get locked out of accounts, a recovery mechanism such as SMS codes, email reset, magic links, or backup codes reinstates access. These days, recovery protection sacrifices their strength and becomes the points of vulnerabilities adversaries come to exploit. Why would a cybercriminal resort to brute-forcing a strong password when a recovery system may be weaker through SIM swap fraud, phishing, or fallback processes poorly executed? This paper studies the privacy and security threats that hide under recovery workflows presented in scholarly literature, industry standards, and technical advisories. It maintains that for account recovery being most commonly done using SMS and email, there are vulnerabilities always present with such recovery methods. Recovery by passkeys and WebAuthn offers more resilient protections yet remains less popular in the practical aspect. In the presence of maybe only some partial direction from standards like NIST SP 800-63B, ISO/IEC 27001, PCI DSS, OWASP guidelines, ENISA advisories, and in line with the FIDO2 specification, there is still no complete global framework issued for governing recovery. This research, by framing recovery as a security and privacy concern, takes a step toward demanding the need for recovery-by-design principles that include consideration of resilience, minimization of identifiers, and transparency to end-users. Without a change to recovery, it will keep eroding digital trust, leaving accounts and personal data exposed.

INTRODUCTION

With the growth of digital ecosystems, authentication has assumed the role of trust in online interactions. Users presently rely on digital identity systems not only for accessing social media or entertainment platforms but for performing key operations, such as financial transactions, healthcare management, or enterprise operations. The vulnerability of an authentication system is, however, decided by the weakest link in the lifecycle. Recovery steps that are supposed to act as lifelines for legitimate users weakening or undermining authentication in the first place often yield the pathway for attackers. The paradox thus declares how vulnerable we are between usability and resilience.

While password cracking requires an immense amount of computation, a recovery hacker uses a variety of human errors, organizational weaknesses, and infrastructural vulnerabilities. High-profile compromise incidents show that attackers often circumvent front-end security to target back ends. SIM swap fraud has been perpetrated on such a scale worldwide that accounts have been misappropriated and great monetary loss accounted for (Traynor, 2019). Likewise, phishing campaigns with fake password reset warnings have tricked users into divulging their credentials, after which attackers gain downstream access to services (Verizon, 2023).

Adding to it the excessive organizational inertia, is the fact that even with warnings from standards bodies for a long time, many service providers continue to offer SMS and email recovery as the default option. The more secure alternatives: hardware tokens, WebAuthn, and passkeys are considered exotic simply because of the usability issues around them and the cost imposed (FIDO Alliance, 2024). This disconnect flags a systemic problem, where recovery mechanisms haven't kept pace alongside the threats.

This paper intends to analyze recovery channels as critical points of vulnerability in the authentication ecosystem. It examines insecure practices, reviews regulatory and standards-based frameworks, and discusses security and privacy issues; all of this is based on academic studies, international standards, and reports from industry. It concludes with recommendations for ensuring that recovery is embraced within security-by-design approaches so that adversaries can no longer exploit the continuance of an account as a back door.

Authentication Recovery Mechanisms

The mechanisms are put in place to recover an account when credentials are forgotten, authentication tokens lost, or users locked out. Such processes must establish a proper balance between level of accessibility and resilience. However, if history shows anything, it tests a repeated bias toward convenience at the expense of security.

SMS-based recovery codes remain widely deployed by financial services, telecommunications providers, and consumer platforms. They are preferred because virtually every user possesses a form of caller ID specification in a form of number. Yet, the SMS-based recovery remains vulnerable due to the mobile infrastructure's shortcomings. Telecom protocols such as SS7 and Diameter, still in widespread use, allow interception of calls and messages (ENISA, 2021). Furthermore, in case of SIM-swap fraud, attackers socially engineer carriers into wrongly assigning a victim's number to themselves. Intercepting thus all SMS-based recovery codes becomes the secondary objective with priority for such attackers.

Another popular channel is email-based recovery, as practically all online services require an email address for account reset. This widespread use, however, establishes a single point of failure: compromise of an inbox may cascade into multiple account compromises (Microsoft, 2020). Phishing campaigns exploit such user expectations by launching fake recovery prompts that mimic legitimate ones so that the attacker takes control.

Magic links were implemented by some cloud and productivity platforms for convenience. They allow the user to log in directly through an email, searching for a password. Yet their poor implementation kills security for most situations. When the link is not bound to device or session context, replay attacks can be performed by malicious actors that intercept the email link (OWASP, 2023).

A traditional fallback of backup codes and security questions. Backup codes, if stored offline, are secure; however, most users either never generate them or store them insecurely. Security questions, once common, have proven useless because their answers can often be easily guessed, found out online, or reused from multiple platforms (Bonneau et al., 2015).

Passkeys and WebAuthn authenticators are the next step in the nascent playground of server-side mobile security mechanisms that offer more resilience. The cryptographic credentials are immune to theft and phishing attacks. Passkeys, which are FIDO2-based standards, could be filtered through SMS or e-mail resets by users. Through WebAuthn, they can be recovered by biometrics or hardware token pairing with strong guarantees of authenticity (W3C, 2021). However, practically no implementations verifiably exist due to the interoperability barriers, infrastructural requirements, and user unfamiliarity.

Threat Landscape in Recovery Exploitation

The exploitation of recovery channels is no mere hypothetic occurrence; it has been a cybercrime term of art since the beginning of time.

SIM swap fraud is a classic case of how attackers take advantage of human and organizational weaknesses. By impersonating a victim and convincing a telecom operator to reassign the service, the criminals gained swift control of SMS-based recovery methods. With the stolen number, they intercepted codes, reset accounts, and withdrew funds. It has been said that even very well-resourced carriers had difficulty erecting effective defenses against insider fraud or social engineering (Traynor, 2019).

Phishing and email compromises continue to rank among the most prevalent threats. Password reset emails are expected communications and, as such, serve as perfect vehicles for deception. The term "means of deception"

refers to the various pathways used by attackers to dupe users into either creating credentials or approving fraudulent password resets.

An email compromise can put an attacker in a more privileged position, wherein the recovery hubs for different accounts that are tied via that email id get compromised, thus exacerbating the damage that has been wrought through the breach (Verizon, 2023).

`Magic-link abuse occurs when services fail to tie the validity of such links to the context of a user's use of the application. Hence, intercepted links can be re-played from unauthorized devices, with a bypass of password checks and multi-factor authentication.'

Recovery token brute-force and enumeration attacks remain possible if not rate-limited enough, either by the systems themselves, networks, or both. If trying countless reset codes can pay off, so go the attackers, especially on poorly implemented ones.

These threats exist with recovery practices remaining nascent. If it is not reformed, perpetrators will keep on abusing recovery avenues as their least resistant path to infiltrate what ought to stand as secure systems.

Standards and Governance Frameworks

International standards bodies have recognized recovery as a key issue; however, advice remains somewhat scattered.

According to the NIST Digital Identity Guidelines SP 800-63B, SMS recovery is forbidden because the channel could be intercepted, and the mobile number could be hijacked by means of SIM swap fraud (NIST, 2017). Instead, phishing-resistant authenticators and multiple methods of recovery are recommended.

ISO/IEC 27001 and 27002 lay down requirements for a secure management of an identity life cycle forming part of the information security management system. These standards, however, are essentially guidelines, leaving the finer implementation details to be decided by the implementing organization (ISO/IEC, 2013).

PCI DSS v4.0 calls for strong authentication for systems accessing cardholder data and discourages the use of SMS-based one-time passwords, although in some quarters, it is not really enforced.

The OWASP Authentication Guidelines offer very detailed technical suggestions able to deal with password reset processes such as distrusting recovery attempts, notifications to the user of such attacks, and context verification (OWASP, 2023).

ENISA threat advisories powerfully imply that vulnerabilities in telecom infrastructure continue to be exploited and warn organizations to expedite the death of SMS-based recovery (ENISA, 2021).

Last but certainly not least, the FIDO2 and WebAuthn specifications define phishing-resistant methods of authentication and recovery. Being the strongest technical standard that exists, however, it is only as good as the ability of an organization to implement it and the readiness of users to adopt it (FIDO Alliance, 2024; W3C, 2021).

But even with such efforts, there is no single, worldwide unified recovery framework. The issue remains that various organizations interpret the requirements differently, hence maintaining the status quo of insecure defaults.

Privacy Implications of Recovery

Recovery identifiers such as phone numbers and email addresses serve the purpose of being persistent digital identifiers. Being useful for account resets, they begin to serve as anchors from one service to another. Hence this introduces a perfection of privacy.

Standards such as ISO/IEC 29100 advocate minimal data collection and restrict other use, yet use for other purposes including marketing and analytics are a common end to the recovery identifiers (ISO/IEC, 2011). For

example, the phone numbers used for SMS recovery might be used for targeted advertising. Likewise, recovery email addresses may be cross-matched across platforms to create extended profiles that go far beyond mere recovery.

Another source of harm comes from a compromise of recovery identifiers. That is, a compromised recovery email inbox may give way to resetting accounts but also to intrusions into personal communications, financial transactions, and professional correspondences. A recovery phone number compromise may be exploited for misrepresenting the involved subscriber, unwanted Spam text messages, or unlawful financial acquisitions. Thus, recovery must be performed not only as a security metric but as a privacy measure.

Case Studies Across Sectors

Recovery insecurity matters across industries.

On the money side, account takers have gone through it a gazillion times when SMS, recovery password or PIN system is relied upon. Thus, bank accounts are drained, crypto-wallets are emptied, and unauthorized transactions are carried out through SIM-swap attacks. Though never really endorsed to ever do things this way, most of them continued with such a system just because customers were so used to it (PCI SSC, 2022).

The patient portals in healthcare were provisionally linked to recovery identifiers that led to the unauthorized disclosures of highly sensitive medical information. When these identifiers are recycled or reassigned, messages put through for the original users might be diverted to others, thus violating confidentiality obligations (ENISA, 2021).

If sad, that says it all for cloud services; magic link implementations have been outright abused-as in, links got intercepted and re-used on a different client device. These are exactly instances of why it is dangerous to prioritize ease of use without proper safeguards (OWASP, 2023).

In contrast, those enterprise identity providers who implement WebAuthn and hardware tokens speak to a greater resilience. Here are examples that show it is clearly feasible to have phishing-resistant recovery technically, and the availability of such methods practically reduces phishing incidents (FIDO Alliance, 2024).

RECOMMENDATIONS

This calls for a layered approach toward risk mitigation.

For organizations, SMS and security questions should go into decline as default recovery channels. Phishing-resistant methods such as passkeys and WebAuthn should be favored above all. Whenever an escape to fallback methods must exist-they should be backed up by layered verification, contextual checking, and real-time notifications. Recovery flows should be tested during penetration testing and audits.

Standardization requires the common recovery framework. Existing standards mention recovery only in passing and never provide prescriptive baselines. A harmonized set of guidelines merging NIST, ISO/IEC, PCI DSS, OWASP, and FIDO2 should explicitly mention what is expected. Mandates for specific sectors, especially finance and health, should also impose phishing-resistant recovery.

Users must be taught to move away from SMS and toward authenticator apps or hardware tokens, frequently checking their recovery settings and decommissioning any identifiers that are no longer considered trustworthy. Above anything else, recovery should be treated as first-class security. As it stands, without very deliberate reform, recovery is the weakest link in authentication.

CONCLUSION

Unique identity systems are in fact broken due to compromised recovery mechanisms that were exploited. For their convenience, SMS, email, and magic links dominate recovery methods, yet they are also among the

easiest for attackers to exploit. More resilient options, such as passkeys and WebAuthn, do exist but face adoption barriers.

The absence of a unified recovery framework causes persistence in the inconsistencies. Certain standards do give faint direction but stop short of enforceable mandates. Recovery now needs a reversal: recovery-by-design, which puts privacy, resilience, and transparency in place right then and there.

Only by setting recovery to be scrutinized just like primary authentication can organizations close the systemic gaps, hold onto user data, and restore digital identity trust.

REFERENCES

1. Bonneau, J., Herley, C., van Oorschot, P., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), 78–87. https://doi.org/10.1145/2699390
2. ENISA. (2021). ENISA threat landscape 2021. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape
3. FIDO Alliance. (2024). FIDO2 and passkeys technical overview. https://fidoalliance.org/fido2/
4. ISO/IEC. (2011). ISO/IEC 29100: Privacy framework. International Organization for Standardization. https://www.iso.org/standard/45123.html
5. ISO/IEC. (2013). ISO/IEC 27001: Information security management systems. International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html
6. Microsoft. (2020). Evolving account recovery. Microsoft Security Blog. https://www.microsoft.com/security/blog
7. NIST. (2017). SP 800-63B: Digital identity guidelines. National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63b.html
8. OWASP. (2023). Authentication cheat sheet. Open Web Application Security Project. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
9. PCI Security Standards Council. (2022). PCI DSS v4.0. https://www.pcisecuritystandards.org/document_library
10. Traynor, P. (2019). Cellular carrier fraud: Implications for account recovery. IEEE Security & Privacy, 17(2), 9–15. [https://doi.org/10.1109/MSEC.2019.2893745] (https://doi.org/10.1109/ MSEC.2019. 2893745)
11. Verizon. (2023). Data breach investigations report. Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir/
12. W3C. (2021). Web Authentication API (WebAuthn). World Wide Web Consortium. https://www.w3.org/TR/webauthn-2/