Passkeys: The Journey to Prevent Phishing Attacks

Part 3. Full Prevention

March 2025

Editors:

Tatsuya Karino, Mercari, inc.

Abstract

This whitepaper is part of a three-part series on preventing phishing attacks through passkey deployment:

- **Part 1: Overview** - Introduces the concepts of a passkey journey toward phishing prevention. [1]
- **Part 2: Partial prevention** - Details strategies for enforcing passkeys in specific scenarios. [2]
- **Part 3: Full prevention** - Explains how to achieve comprehensive phishing resistance.

The Full Prevention stage can be achieved by gradually expanding a limited passkey-only strategy from the Partial Prevention stage until passkeys are required in all areas and for all users. This transition will likely become easier as the industry matures: more services adopt passkeys, users become familiar with them, and the technology continues to improve. While few RPs can currently reach this level, the number is expected to increase over time. This paper outlines approaches to eventually achieve comprehensive phishing resistance.

Audience

RPs and developers who want to protect their applications from phishing attacks by adopting passkeys.

Table of Contents

1 Introduction

The approach to phishing resistance found in the Partial Prevention stage is valuable, however it leaves certain vulnerabilities unaddressed. By protecting only specific features or user segments with passkey authentication, other parts of the service remain exposed to phishing attacks. Remedying these remaining security concerns requires progression to the Full Prevention stage, where comprehensive phishing resistance is achieved through universal passkey enforcement.

This document explains how to move from Partial Prevention to Full Prevention. Section 2 explores ways for RPs to overcome challenges and reach the Full Prevention stage. Section 3 describes factors that simplify this transition. The appendix analyzes remaining security risks after Full Prevention is achieved.

2 The path to Full Prevention

High-assurance RPs should gradually expand their passkey-only strategy during the Partial Prevention stage. This stage serves as a critical preparation phase for achieving complete phishing resistance in the Full Prevention stage. While Full Prevention represents the ultimate goal of using phishing-resistant authentication across all features and users, direct implementation often proves impractical due to technical and business challenges. Only after sufficient preparation can RPs confidently transition to the comprehensive phishing resistance of the Full Prevention stage.

2.1 Increasing passkey-protected users

The Partial Prevention stage introduced a passkey-only strategy for specific user segments as a controlled approach to phishing resistance. **One key approach to the Full Prevention stage involves expanding the number of users protected by passkeys**. For example, when an RP requires passkey usage for users with registered passkeys, increased passkey registration reduces the number of potential phishing victims. Similarly, an RP that requires passkeys for users with assets above a certain threshold, lowers this threshold and expands phishing protection.

While there are various methods to increase passkey adoption during this transition, **users should consciously opt in to passkey-only strategy.** Enabling the passkey-only strategy forces users to confront the challenges of a passkey-only strategy described in the "Challenges of a passkey-only strategy," of Part 2: Partial prevention

[2]. Therefore, aggressive approaches to enforcing a passkey-only strategy, such as automatic passkey registration prompts or conditional registration, may not be suitable during this transitional phase.

2.2 Adopting passkey-only strategy in new and existing services

RPs can expand the passkey-only strategy to services, though the path differs for new versus existing services.

For existing services, transitioning to passkeys can be more challenging. First, there must be a strong justification to offset potential negative impacts on business metrics. For instance, if ongoing phishing attacks are causing tangible financial losses, the reduction in risk may outweigh any decrease in user satisfaction or conversion rates tied to the introduction of passkeys. However, from a psychological perspective, users who are accustomed to using passwords may exhibit reactance if that familiar choice is taken away. This sense of lost freedom can trigger frustration or resistance, making it harder to fully implement and maintain a passkey-only strategy.

By contrast, **implementing a passkey-only strategy for new services tends to face less resistance than existing services.** Since there is no established user base expecting to use passwords, reactance is minimized. Users will simply learn the service's login requirements without feeling that an existing option has been removed. Additionally, new services must carefully consider phishing prevention and incident response in advance, as they do not know how much damage can be caused by a phishing attack. Since passkeys can prevent phishing damage, they are more likely to be accepted in new services.

2.3 Eliminate phishable methods from all RP features

The final step is to require passkey use across all features and for all users. This means removing all phishable methods from account creation, prohibiting password-based logins, and eliminating weak recovery methods.

Most RPs cannot avoid maintaining alternative authentication methods such as email magic links or device flow/CIBA with user codes, since passkeys often represent their only phishing-resistant authentication option, especially in consumer applications. These alternative methods should be implemented with additional security controls like strict rate limiting, threat detection, and enhanced monitoring to minimize potential abuse vectors.

3 Enablers for Full Prevention transition

Several industry-wide factors are expected to serve as enablers in resolving the challenges of a passkey-only strategy. Individual RPs need to communicate intentionally with users to mitigate challenges of passkey-only authentication as completely resolving the challenges remains difficult.

Several industry-wide factors could help address the challenges:

- **Increases in passkey adoption across RPs**: As passkey adoption grows and more RPs implement passkey-only strategy, users will become increasingly familiar with this authentication method. While login challenges may occur when passkeys are unavailable, users will naturally learn to navigate recovery procedures and prevent such situations. Alongside user adaptation, broader adoption across RPs will help establish and refine best practices for passkey implementation.

- **Advances in passkey provider capabilities**: Passkey providers are evolving towards expanding the range of passkey synchronization capabilities. As this technology progresses, users will be less likely to encounter situations where they cannot find available passkeys, which is currently one of the main difficulties with passkey implementation.

- **More accessible high-assurance identity verification methods:** One of the challenges in reaching and maintaining Full Prevention is limited choices for phishing-resistant authentication, particularly in consumer applications. Currently, the lack of available phishing-resistant authentication methods makes it difficult to implement secure account recovery processes. The emergence of more accessible high-assurance identity verification methods based on digital identity wallets could enable secure and user-friendly transmission of personal information for account recovery purposes.

These developments could reduce the barriers to implementing passkey-only strategy, creating more opportunities for wider adoption among RPs.

4 Conclusion

Preventing phishing attacks requires a strategic journey from traditional authentication through multiple stages: beginning with introducing passkeys alongside existing

methods (Optional Adoption stage), progressing to enforcing passkeys for specific users or features (Partial Prevention stage), and ultimately achieving comprehensive phishing resistance through exclusive use of passkeys or other phishing-resistant methods (Full Prevention stage). While this transition presents significant challenges, particularly for user experience and business impact, a systematic approach enables RPs to progress through these stages successfully. This gradual approach includes introducing passkeys gradually, validating their effectiveness in controlled environments, and expanding their area based on both user readiness and industry developments. The adoption challenges regarding a passkey-only strategy currently limit the number of RPs that can achieve the Full Prevention stage, but as passkey technology evolves and proper preparation is executed, from initial deployment through selective enforcement to complete adoption, more RPs will be able to implement this stringent security measure.

5 Appendix

5.1 Residual security considerations

While the Full Prevention stage provides robust authentication security by not supporting phishable authentication methods, potential attack vectors still exist. Although these attack methods are not yet widespread, they may become more prominent as passkey adoption increases and services reduce their dependence on phishable authentication factors. This section summarizes potential attack scenarios that could emerge under these circumstances.

5.1.1 Phishing risks: alternative authentication

Attackers could exploit alternative authentication methods to bypass passkey authentication. Alternative authentication methods, such as email magic links and device flow / CIBA with user code, are not classified as phishable methods because they make it difficult for attackers to create practical phishing sites. However, these methods are not phishing-resistant either. If attackers find ways to exploit these login methods in the future, we should reclassify them as phishable.

To prevent these threats, RPs must conduct periodic threat modeling and security analysis. Analysis should encompass emerging attack patterns, changes in authentication technology landscapes, and evolving security practices within the industry. Regular assessment enables RPs to identify potential vulnerabilities before they can be exploited and to adapt their authentication mechanisms accordingly.

5.1.2 Phishing risks: external providers

Attackers could exploit external providers to bypass passkey authentication. External providers are services that RPs rely on for authentication, such as identity providers (providers of federation), email providers, and passkey providers. For example, if an RP supports federation as one of its login methods and if the identity provider's authentication is weak, such as using only a password, attackers can take over the RP account by compromising the identity provider's account.

There are several ways to mitigate risk. For example:

- **Evaluate the security properties and user authentication methods of external providers.** RPs can only rely on the external provider to a degree commensurate with the risk associated with the RP's features. However, this is only feasible when providers offer the necessary features. For example, when RPs support federation and the identity providers support Authentication Context Class Reference (ACR) (described on OpenID Connect Core 1.0 [3]), RPs can assess the strength of user authentication performed by the identity providers. Regarding passkeys, there is currently no direct method to verify the security properties of passkey providers, and the only option is to identify the provider using an Authenticator Attestation Global Unique Identifier (AAGUID) and assess the provider beforehand. However, this approach is not recommended because it may lead to a situation where users are unable to use their desired passkey provider, as managing an allowlist of passkey providers can be cumbersome for RPs and requires frequent updates to stay current.

- **RPs do not have to rely solely on external providers to mitigate phishing attacks, they can use a combination of authentication methods provided by external providers and their own internally managed authentication methods.** For example, when a user logs in, the RP can require both the authentication method provided by the external provider (for example, passkey providers) and an additional authentication method managed by the RP (for example, SMS OTP or Time-based One-Time Password (TOTP)). This approach can mitigate the risk of phishing attacks because attackers would need to steal credentials from both the external provider and the RP. However, this is a huge downside in terms of usability.

5.1.3 Unattested passkey registration

Passkey registration with no attestation is relatively weaker than that with attestation but offers strong protection post-registration. Synced passkeys lack attestation capabilities because it would not be very meaningful, especially in situations where the security environment might change through export/import. The white paper: FIDO Attestation [4] states, "The AAGUID without attestation is 'informational' only and does not provide any assurance of its authenticity." This lack of attestation creates a potential for security gaps during passkey registration such as malicious passkey providers: attackers might create fake passkey providers and trick users into using them. RPs cannot verify if these registrations are genuine because there is no attestation to prove authenticity.

While the passkey registration process may have potential vulnerabilities, passkey authentication remains secure once properly registered. Passkey authentication continues to offer stronger security compared to traditional passwords. To protect existing users, the best approach is to encourage them to register passkeys as soon as possible.

5.1.4 Session hijacking

Session hijacking remains a potential threat even in the Full Prevention stage. Attackers can intercept or steal active session tokens to gain unauthorized access. While passkeys prevent direct account compromise through phishing, compromised sessions can still allow attackers to perform actions on behalf of legitimate users. This risk becomes more significant as services transition to passkey-only authentication, potentially making session hijacking a more attractive target for attackers.

To mitigate this risk, implementing sender-constrained tokens or sessions is essential. These mechanisms ensure that session credentials can only be used from the device that originally obtained them. Several implementations are available for this approach, such as Device-Bound Session Credentials (DBSC), which use device-specific cryptographic binding or Demonstrating Proof of Possession (DPoP) [5], which proves token ownership through cryptographic signatures. By implementing sender-constrained sessions alongside passkey authentication in the Full Prevention stage, RPs can establish comprehensive protection against both authentication and session-level attacks.

6 Acknowledgments

The authors acknowledge the following people (in alphabetic order) for their valuable feedback and comments:

- Tim Cappalli, Okta
- Joseph Choi, Royal Bank of Canada - Solutions Acceleration & Innovation
- Norman Field, Strongkey
- Bill Fish, Prove
- Hideaki Furukawa, NRI SecureTechnologies, Ltd.
- Max Hata, NTT Docomo
- Steve Johnson, Microsoft
- Sue Koomen, American Express Company
- Rolf Lindemann, Nok Nok
- Christine Owen, 1Kosmos
- Megan Shamas, FIDO Alliance
- Tom Sheffield, Target Corporation
- Mitch Tseng, Egis Technology Inc.
- Shane Weeden, IBM
- Diego Zavala, Google Inc.

7 References

[1] Passkey's journey to prevent phishing attacks Part 1. overview
https://fidoalliance.org/white-paper-passkeys-the-journey-to-prevent-phishing-attacks/

[2] Passkey's journey to prevent phishing attacks - Part 2. Partial prevention
https://fidoalliance.org/white-paper-passkeys-the-journey-to-prevent-phishing-attacks/

[3] OpenID Connect Core 1.0
https://openid.net/specs/openid-connect-core-1_0.html

[4] White Paper: FIDO Attestation: Enhancing Trust, Privacy, and Interoperability in Passwordless Authentication
https://fidoalliance.org/fido-attestation-enhancing-trust-privacy-and-interoperability-in-passwordless-authentication/

[5] RFC 9449 OAuth 2.0 Demonstrating Proof of Possession (DPoP)
https://www.rfc-editor.org/rfc/rfc9449.html

8 Document history

Change	Description	Date
Publication	White paper first published.	March 2025