Passkeys: The Journey to Prevent Phishing Attacks

Part 2. Partial 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.
- **Part 3: Full prevention** - Explains how to achieve comprehensive phishing resistance. [2]

A passkey-only strategy is fundamental to preventing phishing attacks. However, given passkey challenges, relying parties (RPs) can start by implementing the Partial Prevention strategy for their high-risk users and features. This paper outlines phishing attack patterns against RPs with passkeys deployed and proposes a targeted passkey-only strategy implementation to avoid security pitfalls and mitigate the adoption challenges.

Audience

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

Table of Contents

1 Introduction

RPs should implement the Partial Prevention stage security measures, or higher, if they are facing phishing threats. This is because the lower stages do not provide service-level phishing protection. While the Full Prevention stage offers complete phishing prevention by removing all phishable authentication methods, such a sudden transition could disrupt user access to critical applications. An abrupt change in authentication methods may frustrate users, damage trust, and lead to service abandonment. The Partial Prevention stage acts as a transition phase, balancing enhanced security by implementing passkey requirements while minimizing user disruption.

This document explains the transition method from the Optional Adoption stage to the Partial Prevention stage. Section 2 discusses phishing attacks at these stages, demonstrating how phishing attacks are possible with a hybrid solution. Section 3 introduces a passkey-only strategy, to protect our services from phishing attacks. Section 4 presents Partial Prevention stage patterns, including enforcing passkey use for specific users and features.

2 Phishing vulnerabilities on passkey-deployed RPs

This section describes four passkey deployment cases with phishing vulnerabilities. Each deployment implements passkeys on its application. However, the phishing resistance of passkeys is not utilized as there are methods to bypass passkey authentication. Note that the root cause of these attacks is not passkeys themselves but rather issues with RP deployments.

2.1 Passwords as vulnerabilities to bypass passkey authentication

When RPs implement both passkeys and passwords as authentication methods, the passwords can undermine the security benefits of passkeys. Support of password-based authentication as a fallback mechanism helps users access services on devices without passkey capabilities, but it also creates an opportunity for attackers. Attackers can use phishing attacks to obtain passwords and then use these credentials to gain unauthorized access to user accounts. Mitigation strategies for this security concern are detailed in section 3 of this document.

2.2 Unauthorized passkey registration in compromised accounts

When RPs implement passkeys but allow registration with phishable authentication methods, attackers can register passkeys on compromised accounts, enabling complete account takeover. For instance, consider an application that uses password authentication for general access but requires passkey authentication for high-risk operations such as external fund transfers. If the RP allows new passkey registration using only password authentication, attackers can exploit this vulnerability through a two-step process: first obtaining user credentials through phishing attacks to gain initial access, then registering their own passkeys to bypass the enhanced security measures for high-risk operations. Detailed mitigation strategies for this security risk are presented in section 4.2 of this document.

2.3 Exploit account recovery mechanisms to bypass passkey authentication

Account recovery processes based on weak authentication methods create potential security bypasses and undermine the strength of passkey authentication systems. Consider a security-conscious application that requires passkey authentication for account access, which addresses the vulnerabilities outlined in sections 2.1 and 2.2. The application must provide account recovery mechanisms for users who lose access to their passkeys, but implementing recovery through email or SMS one-time passwords (OTPs) alone introduces significant vulnerabilities. Attackers can exploit this by targeting the recovery pathway rather than the primary authentication flow. By obtaining email addresses through phishing attacks and initiating account recovery, attackers can intercept OTPs through phishing, bypassing the passkey requirement. Mitigation strategies for this security concern are detailed in section 3 of this document.

2.4 Social engineering attacks to downgrade account security level

One sophisticated phishing attack vector involves social engineering users deleting their registered passkeys, potentially leading to account compromise. Consider an application that has implemented robust security measures: required passkey authentication for login and phishing-resistant account recovery methods based on MNO's network authentication, which addresses vulnerabilities described in sections 2.1-2.3. This service is properly protected by passkeys. However, attackers can exploit user behavior through social engineering tactics to disable passkey-only strategy. These tactics typically involve presenting false technical error messages such as "Your environment doesn't support passkeys. Please enable password login before proceeding." Once users disable the option, accounts revert to a vulnerable state susceptible to traditional phishing attacks. The implementation of Full Prevention stage, as detailed in Part 3 [2], provides mitigation strategies for this vulnerability.

3 Fundamental to prevent phishing attacks

To prevent phishing attacks, RPs must employ a passkey-only strategy that enforces the use of passkeys and eliminates passwords. The passkey journey described in Part 1. Overview [1] explains that the Partial Prevention and Full Prevention stages are phishing-prevented stages, both satisfying passkey-only strategy requirements. As outlined in section 2.1, allowing password-based logins alongside passkeys causes a vulnerability that attackers can exploit through phishing sites, bypassing the passkey authentication. Therefore, to protect user accounts from phishing attacks, RPs should require phishing-resistant authentication methods like passkeys, while discontinuing support for less secure, phishable alternatives.

The prohibition of phishable methods applies to both login and account recovery processes. If account recovery mechanisms remain vulnerable to phishing attacks, attackers can potentially bypass robust authentication controls through these weaknesses as outlined in section 2.3. Therefore, RPs that employ phishing-resistant methods across all authentication scenarios (login, fallback, and account recovery) are considered more resilient against phishing attacks than RPs that employ phishable methods for account recovery.

4 Determining the area of a passkey-only strategy

A passkey-only strategy might restrict account access for some users. Since passkeys are relatively new, authentication failures can be particularly challenging for users to troubleshoot. To mitigate issues, RPs can start by adopting a passkey-only strategy for their high-risk users and features that really need protection from phishing. The details of the challenges are described in this document’s appendix; 6.1 Challenges of a passkey-only strategy.

4.1 Applying a passkey-only strategy to specific users

You can implement the Partial Prevention stage by enforcing passkeys for specific user groups. Applications can require a passkey-only strategy for specific users and other users can continue to access the service through traditional methods, like password authentication with SMS OTP.

The Partial Prevention stage has two approaches to choose from:

- **Enforce passkey use for all users who have registered passkeys**
  This approach disables password authentication when a user registers a passkey. While this approach is simple to implement and directly links passkey registration to phishing protection, it may impact users who face challenges with passkey use across their various devices and platforms.

- **Provide an option to enforce passkey usage (an option to disable passwords)**
  For this approach, passkey registration is a separate process from password disablement, allowing users to choose when to switch to passkey-only authentication. While this enables flexible passkey registration methods like conditional registration, RPs must promote both passkey registration and the passkey-only strategy to protect users from phishing attacks.

This strategy enables RPs to prioritize passkey adoption for appropriate user segments, such as users familiar with passkey technology or high-value accounts that face significant risks from phishing attacks. This approach achieves enhanced security while maintaining practical usability.

4.2 Applying a passkey-only strategy to specific features

You can implement the Partial Prevention stage by requiring passkeys for specific high-risk features. For example, an application can require passkey authentication when users access sensitive operations, such as transferring money outside of the RP. The application can continue to support traditional authentication methods for other features. This means users can access standard features using password authentication with SMS OTPs, but passkey authentication is required for high-risk operations.

There are two key points about passkey registration to protect important features and their resources:

- **RPs should implement passkey registration at the point where the features' resources are created.** For example, in a payment service that handles account deposits and withdrawals, the RP should check if a user has passkeys during the deposit process. If no passkey is registered, the account will be vulnerable against phishing attacks even if withdrawals require passkey authentication, as detailed in section 2.2. If it is difficult to require users to register passkeys at these points, it is crucial to ensure they register before potential attackers do.

- **RPs should treat passkey registration as a high-risk operation that requires proper authentication.** Consider the payment service example: without proper authentication during passkey registration, an attacker who gains initial access through phishing could register their own passkey (as detailed in section 2.2). This would give them persistent access to sensitive features that are meant to be protected by passkey authentication. By requiring strong authentication during passkey registration, RPs can maintain the security boundary between phishing-vulnerable authentication methods and passkey-protected high-risk operations.

4.3 Addressing challenges of a passkey-only strategy

While the strategies outlined in sections 4.1 and 4.2 help avoid challenges with a passkey-only strategy, they do not resolve these challenges. Although individual RPs cannot completely eliminate these challenges, they can take several measures to minimize user burden:

- **User choice and control are essential:**
  RPs should let users choose whether they want to use a passkey-only strategy. While passkeys are straightforward for users with a single smartphone, those managing multiple devices or cross-platform environments may face practical challenges with passkey use. Therefore, users should be able to try using a passkey-only strategy, and if they find it too difficult to continue, they should have

the option to switch back to traditional methods. This approach allows users to make informed decisions: they can either enhance their account security and use high-risk features by adopting passkeys or continue using traditional authentication methods with an understanding of the associated security trade-offs and give up using high-risk features.

- **Prepare alternative authentication methods:**
  Most customers are not familiar with passkeys yet. They may find it hard to understand error messages like passkeys not found. This causes a lot of frustration as it is described in this appendix. When passkeys prevent users from accessing services, they become frustrated with the technology, which might make them less likely to use passkeys.

  To solve this problem, RPs need to prepare alternative methods, such as email magic links or device flow or Client Initiated Backchannel Authentication (CIBA) with user code. While the Partial Prevention and Full Prevention stages do not allow phishable methods, they do allow methods that have not been classified yet. In the future, digital identity wallets show promise because they allow sharing of identity information safely without risk of phishing. Moreover, because passkey errors can be frustrating, it helps to only use passkey authentication when it is likely to work, like with conditional UI (autofill), to prevent users from seeing error messages.

  RPs can suggest that users set up backup options like federation or multiple passkeys. But this has limits because not everyone can use federation or set up passkeys with different providers, especially if they don't have multiple devices. Therefore, we might need to restart the identity checking or user setup process such as customer support. You can read more about these topics in the white paper Multiple Authenticators for Reducing Account Recovery Needs for FIDO-Enabled Consumer Accounts [4].

- **Clear communication and education is crucial:**
  Since many users are still unfamiliar with passkeys, RPs must provide clear, accessible explanations about passkey use. Following **Passkey Central Design Guidelines** [3] is particularly important to ensure consistent and user-friendly implementations.

By implementing these measures, RPs can help ensure that passkey adoption progresses smoothly while maintaining a positive user experience, even though the fundamental challenges of passkey-only strategy may persist.

5 Conclusion

Preventing phishing requires enforcing passkeys or other phishing-resistant authentication methods. The Partial Prevention stage serves as a critical transition phase in the overall passkey journey, enabling RPs to enhance security while managing UX impact through targeted implementation. Whether focusing on specific users or features, RPs should view Partial Prevention Stage 3 implementation strategies, as preparation for eventual full passkey adoption, while carefully considering their risk profile and user base's readiness for authentication changes.

6 Appendix

6.1 Challenges of a passkey-only strategy

Implementing a passkey-only strategy presents challenges. While the Partial Prevention stage mitigates these challenges by applying the strategy selectively to specific users and features, RPs must overcome them to reach the Full Prevention stage. This section outlines four key challenges that may impede progress toward the Full Prevention stage.

6.1.1 Additional user experience complexities with passkeys

While passkeys generally offer a good user experience, passkeys have yet to reach a state where all users can easily adopt them. In standard authentication scenarios, users only need to input a PIN or use biometric authentication. However, when a passkey is not present on the device being used for login, users must perform cross-device authentication by scanning a QR code and not all users are familiar with this experience.

Moreover, the failure scenarios for passkeys differ from those for passwords. Password-related failures, such as forgetting credentials, while annoying, are situations that users can comprehend. In contrast, passkey failures often manifest as "passkey not found" errors. Since typical users do not fully understand the mechanisms of passkeys, they may struggle to identify what went wrong or know how to prevent such issues proactively.

6.1.2 Business impact of passkey-only strategy

The remaining challenges with passkeys can negatively impact business metrics when implementing a passkey-only strategy. For example, if RPs remove password authentication from the login process, the login success rate inevitably decreases due to the reduced number of authentication options. Additionally, requiring passkey registration during account creation can reduce sign-up rates due to user experience challenges and vague concerns about passkey reliability. These potential impacts on business metrics represent a major concern in transitioning to the Full Prevention stage.

6.1.3 Limited choices for phishing-resistant authentication

For consumer applications, phishing-resistant authentication options remain limited. As discussed in section 3 of Part 1. Overview [1], passkeys are currently the only widely available phishing-resistant authentication method for consumer applications. Without phishing-resistant account recovery options, RPs must rely on methods like email magic links when users lose passkey access. This constraint means that even if the RP reaches the Full Prevention stage, it may not be able to meet the RP's requirement for adequate security.

6.1.4 Psychological resistance to losing perceived choices

A final challenge in moving to a passkey-only strategy involves reactance, a concept from psychology where people resist changes that take away their sense of freedom or choice. Many users see passwords as a familiar option, even if they are less secure. Especially if a service already supports passwords, users assume it is an available choice. When passwords disappear, some users may feel they have lost control, which can lead to frustration or rejection of the new system. Moreover, if there are no easy alternatives for users who cannot use passkeys—due to technical limitations, device compatibility, or other barriers—their resistance can grow even stronger.

7 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.

8 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 3. Full prevention
https://fidoalliance.org/white-paper-passkeys-the-journey-to-prevent-phishing-attacks/

[3] Passkey Central Design Guidelines
https://www.passkeycentral.org/design-guidelines/

[4] FIDO Alliance White Paper: Multiple Authenticators for Reducing Account Recovery Needs for FIDO-Enabled Consumer Accounts
https://fidoalliance.org/wp-content/uploads/2020/06/FIDO_White_Paper_Multiple_Authenticators_CDWG.pdf

9 Document history

Change	Description	Date
Publication	White paper first published.	March 2025