# Passkeys: The Journey to Prevent Phishing Attacks

## Part 1. Overview

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.
- **Part 2: Partial prevention** - Details strategies for enforcing passkeys in specific scenarios. [1]
- **Part 3: Full prevention** - Explains how to achieve comprehensive phishing resistance. [2]

**Making your services phishing-resistant takes more than one day because you are not just adopting a new phishing-resistant authentication method. It is a journey with multiple stages where you improve security by strengthening account login and recovery processes.** This paper outlines the passkey journey and defines the authentication and recovery requirements for each stage.

## Audience

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

## Table of Contents

# 1 Introduction

**Passkeys are beginning to be adopted to prevent phishing attacks.** Passkeys are currently the only practical phishing-resistant option for consumers and exclusively using passkeys for RP account logins would provide the strongest security. However, an immediate switch can create significant user friction and potentially lead to service abandonment. Therefore, the recommendation within this paper is a staged approach to passkey adoption that balances security improvements with user experience.

**This white paper outlines specifications for the multi-stage passkey journey.** Each stage requires distinct authentication and account recovery requirements, with varying levels of phishing resistance. This document categorizes authentication methods and account recovery methods into two classes based on their level of phishing resistance. It then outlines the stages of the passkey journey, detailing the phishing resistance characteristics, as well as authentication and account recovery method requirements for each stage.

# 2 Classification of authentication methods

This section explains phishable and phishing-resistant authentication, and how other authentication methods are addressed in this document. Phishing refers to a method cybercriminals use to attempt to obtain sensitive data by pretending to be a trusted colleague, acquaintance, or organization to trick victims into providing sensitive information or network access.

- **Phishable authentication methods** can be stolen or compromised through phishing.
- **Phishing-resistant authentication methods** have a nature that prevents them from being stolen or compromised through phishing.

**This classification includes account recovery methods, which are fundamentally forms of authentication.** While account recovery methods are not typically used for regular authentication, they should be considered when evaluating the required authentication strength for service access. Therefore, this white paper includes account recovery methods.

**Phishable methods**

- Passwords
- One-time password (OTP) sent through Short Message Service (SMS), email, messaging apps, authentication app, Rich Communication Services (RCS)[1]
- Time-based OTP
- WebOTP[2]
- Push notification authentication[3]
- Device flow / Client Initiated Backchannel Authentication (CIBA) without user code
- Recovery codes

**Phishing-resistant methods**

- Passkeys (synced, device-bound)[4]
- Mobile Network Operator's (MNO's) network authentication [5]
- Transport Layer Security (TLS) client certificate authentication

**This paper does not categorize other methods, such as email-based magic links, as either phishable or phishing-resistant.** While they are harder to hack than phishable methods, they don't have any theoretical protection against phishing. The safety level of these methods depends on how each company sets up their login and account recovery process, and what kind of phishing attacks are currently common.

---

[1] Regardless of the delivery method, there is no phishing resistance in any case, as users can still input the codes into phishing sites.

[2] WebOTP automatically fills in OTP codes when the sender's domain matches the expected domain. However, this mechanism does not prevent users from manually entering OTP codes into phishing sites.

[3] Push notifications have no phishing resistance as users may approve malicious push notifications believing them to be from legitimate applications.

[4] Passkeys are classified as phishing-resistant due to their verifier name-binding mechanisms. The details are described in the Appendix.

[5] MNO's network authentication is classified as phishing-resistant due to their verifier channel-binding mechanisms.

- Email magic links[6]
- Federation protocols
- Device flow / CIBA with user code
- Identity verification through customer support[7]
- In-person account recovery at physical store locations

# 3 Passkey journey stages

**To protect against phishing attacks, relying parties (RPs) need to implement phishing-resistant methods.** This paper outlines the passkey journey, a progressive implementation framework for adopting passkeys to achieve phishing prevention. The passkey journey consists of four stages. While passkeys are introduced from the second stage onward, services can only be truly protected from phishing attacks when you reach the Partial Prevention and Full Prevention stages.

The minimum requirement for the Partial Prevention and Full Prevention stages is to eliminate phishable authentication methods, with uncategorized methods like email magic links being permissible. While the Full Prevention stage ideally requires the exclusive use of phishing-resistant methods, most RPs lack viable alternatives to passkeys. Consequently, dependence on alternative methods such as email magic links or device flow/CIBA with user code for account recovery becomes necessary. It is important to note that these methods may be reclassified as phishable as attack vectors evolve. RPs must maintain ongoing analysis of potential attack scenarios and regularly evaluate their security posture.

[6] Since few legitimate sites require URL entry for login, users are less likely to fall victim to phishing sites requesting URL input. Additionally, when URLs are embedded in HTML emails as clickable buttons, obtaining these URLs becomes more unnatural.

[7] Identity verification through customer support is resource-intensive, making it impractical for scalable attacks.

The following table summarizes acceptable methods for each stage.

*Table 1: Acceptable authentication methods*

| | Phishable methods | Phishing-resistant methods | Example |
|---|---|---|---|
| Legacy Authentication | ✅ | - | Login: password + OTP<br>Recovery: recovery codes |
| Optional Adoption | ✅ | ✅ | Login: password + OTP, or passkey<br>Recovery: recovery codes |
| | ✅ or ❌<br>Depends on conditions | ✅ | Login: password + OTP, or passkey<br>Recovery: network authentication<br><br>**Note:** In certain conditions, phishable methods are prohibited. |
| | ❌ | ✅ | Login: passkey<br>Recovery: network authentication<br><br>Note: at the least, non-phishable methods are required in all cases. |

**1. Legacy Authentication stage**

**In the Legacy Authentication stage, services provide no phishing resistance**, as RPs at this stage only support phishable authentication methods such as passwords and SMS OTPs. Consequently, accounts with these RPs are vulnerable to compromise through phishing.

**2. Optional Adoption stage**

**The Optional Adoption stage services support phishing-resistant methods (passkeys) alongside phishable authentication.** RPs at this stage lack phishing resistance as they do not enforce phishing-resistant methods. These services consistently allow fallback to phishable authentication methods, leaving accounts vulnerable to compromise through phishing.

**Services should reach this stage even if they do not currently need strong phishing resistance.** Both services and attack methods continuously evolve, so it is difficult to predict when a service might be a target of phishing attacks. If passkeys are already implemented, upgrading to the Partial Prevention becomes a viable option for countering the attacks.

**3. Partial Prevention stage**

**The Partial Prevention stage services implement partial phishing resistance.** RPs support both phishable authentication and phishing-resistant methods (passkeys), while enforcing the use of phishing-resistant methods under specific conditions. This enforcement strategy protects against phishing attacks for designated accounts and functionalities. The details of the Partial Prevention stage are described in Part 2: Partial prevention [1].

RPs that have suffered from phishing attacks or face potentially severe phishing risks should reach this level at a minimum. This is because the first two stages do not provide phishing resistance for the service.

**4. Full Prevention stage**

**The Full Prevention stage services achieve full phishing resistance. In this stage, RPs must not rely on phishable methods for login or account recovery under any conditions.** RPs exclusively support phishing-resistant methods (passkeys), eliminating support for phishable methods. Fallback to phishable methods is not permitted. This strict enforcement ensures comprehensive protection against phishing attacks for all accounts. The details of Full Prevention are described in Part 3: Full prevention [2].

Currently, only a limited number of RPs can achieve this stage due to the inherent usability and business challenges in reaching this stage. These challenges are detailed in "Challenges of a passkey-only strategy," of Part 2: Partial prevention [1]. However, RPs that have experienced phishing attacks or face potentially severe phishing risks should eventually reach this level. This is necessary because phishing risks persist even in stage 3, and these risks will eventually become actual threats.

# 4 Conclusion

This document explains how to build phishing-resistant services using passkeys, step by step. It covers the requirements and security features needed at each stage and recommends which stages different RPs should aim for. You can find the detailed steps

 

to move Partial Prevention and Full prevention stages in separate documents; Part 2: Partial prevention [1] and Part 3: Full prevention [2].

# 5 Appendix

## 5.1 Understanding phishing attacks

Phishing attack refers to a method cybercriminals use to attempt to obtain sensitive data by pretending to be a trusted colleague, acquaintance, or organization to trick victims into providing sensitive information or network access. According to "6.1. Authenticator Threats" of NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management [3], a phishing attack is when "the authenticator output is captured by fooling the subscriber into thinking the attacker is a verifier or RP".

In practice, phishing attacks occur through multiple channels:

1. Email-based phishing: An attacker sends a message to the victim's email address, directing them to a phishing site. The phishing site then requests that the victim enter their credentials, which are subsequently sent to the attacker.

2. Phone-based phishing/vishing: Attackers call victims directly, impersonating technical support, bank representatives, or government officials. They create a sense of urgency or fear to manipulate victims into revealing credentials, making payments, or granting remote access to devices.

3. SMS phishing (smishing): Attackers send text messages containing malicious links or requesting sensitive information, often posing as delivery services, banks, or government agencies.

4. Social media phishing: Attackers use fake profiles or compromised accounts to send malicious links through direct messages or posts.

Regardless of the method, once credentials are obtained, the attacker can authenticate on the genuine site or application effectively gaining unauthorized access to the victim's account.

## 5.2 Why are passkeys phishing-resistant?

Phishing attack refers to a method cybercriminals use to attempt to obtain sensitive data by pretending to be a trusted colleague, acquaintance, or organization to trick victims into providing sensitive information or network access. According to “6.1. Authenticator Threats” of NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management [3], a phishing attack is when "the authenticator output is captured by fooling the subscriber into thinking the attacker is a verifier or RP". In practice, this typically involves an attacker sending a message to the victim's email address, directing them to a phishing site. The phishing site then requests that the victim enter their credentials, which are subsequently sent to the attacker. The attacker can then use the credentials to authenticate on the genuine site or application, effectively gaining unauthorized access to the victim's account.

**FIDO Authentication offers phishing-resistant authentication with verifier name binding through origin-bound authentication.** NIST SP 800-63B-4 [3] elaborates on the concept of Phishing Resistance in section 3.2.5, stating that "phishing resistance is the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber". Two methods of phishing resistance are recognized: channel binding and verifier name binding.

- **Channel binding** is a method that cryptographically binds the authenticator outputs with a unique identifier of the established communication channel. This ensures that the credentials are only valid on the same channel, thus preventing man-in-the-middle attacks.
- **Verifier name binding** is a method that cryptographically binds the authenticator outputs with a pre-registered identifier of the verifier (usually the server's hostname). This ensures that the credentials are only valid for the legitimate verifier and thus prevents their use on phishing sites.

Passkey authentication achieves phishing resistance through verifier name binding by verifying the Relying Party ID (RPID) and origin. An RPID is a valid domain string identifying the RP on whose behalf a given registration or authentication ceremony is being performed. A passkey can be used for authentication only on the domain (or its subdomains) specified by RPID. Additionally, the assertion includes both the RPID and origin. This allows the RP to verify that these values match its expected values.

**Cross-device authentication with passkeys is resistant to phishing attacks due to proximity checks and secure transport.** The importance of proximity limitation and short-lived/one-time use of authentication codes is emphasized in section 6, "Mitigating Against Cross-Device Flow Attacks," of the "Cross-Device Flows: Security Best Current Practice" [4] document. The hybrid authentication (cross-device authentication), introduced in CTAP 2.2, significantly reduces the susceptibility to phishing attacks by providing local proximity through Bluetooth Low Energy (BLE) communication between the client and the authenticator in addition to leveraging the phishing-resistant properties of passkeys.

## 5.3 Authentication Methods Glossary

This section provides definitions for the various authentication methods mentioned throughout this document:

- **Time-based OTP (TOTP)**: A temporary password generated by an authentication app that changes every 30-60 seconds based on the current time and a shared secret key.

- **WebOTP**: A web standard that allows websites to programmatically request and verify one-time passwords received via SMS, streamlining the authentication process on mobile devices.

- **Push Notification Authentication**: A method where users receive a notification on a trusted device asking them to approve or deny an authentication attempt, typically by tapping a button in the notification.

- **Recovery Codes**: Pre-generated backup codes provided to users when they create an account, allowing them to regain access to their accounts if they lose access to their primary authentication method.

- **Device Flow / CIBA (Client Initiated Backchannel Authentication)**: Authentication method where users authorize access on a separate trusted device rather than the requesting device. A code is displayed on the requesting device that the user must enter on their trusted device, adding an additional verification step.

- **Email Magic Links**: An authentication method where a unique, time-limited link is sent to the user's email. When clicked, the link automatically authenticates the

 

user without requiring a password, using the email account access as a verification factor.

- **Federation Protocols**: Authentication methods where a trusted third party (identity provider) handles the authentication process and then confirms the user's identity to the service they're trying to access. Examples include OpenID Connect, and SAML.

- **Mobile Network Operator's (MNO's) Network Authentication**: A method that leverages the cellular network infrastructure to authenticate users based on their SIM card and device identification. This approach provides strong protection against phishing attacks because it relies on physical possession of the device and the secure communication channel established directly between the mobile device and the operator's network.

# 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 2. Partial prevention 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] NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management https://csrc.nist.gov/pubs/sp/800/63/b/4/2pd

[4] Cross-Device Flows: Security Best Current Practice https://www.ietf.org/archive/id/draft-ietf-oauth-cross-device-security-07.html#name-mitigating-against-cross-de

 

# 8 Document history

| Change | Description | Date |
|---|---|---|
| Publication | White paper first published. | March 2025 |
| | | |
| | | |
| | | |
| | | |