TOKEN

CISO WHITEPAPER

Passkeys Are Not Completely Secure After All

Unless They Are Tied to Dedicated Biometric Hardware

How attackers exploit passkey enrollment, how trusted employees are deceived, and why Token stops the attack cold.

> **THE CENTRAL FLAW**
>
> The attacker does not break the passkey. The attacker deceives the employee, takes control of the real account, and registers a new passkey on hardware the attacker owns.

August 2026

EXECUTIVE SUMMARY

Passkeys are an important improvement over passwords because they replace reusable secrets with public key cryptography. A passkey registered for one service cannot simply be copied from a fake login page and replayed against the legitimate service.

A new campaign targeting Microsoft Entra users exposes a different weakness. Attackers are not breaking existing passkeys. They are deceiving employees, taking control of the real account, and then registering a new passkey on an authenticator controlled by the attacker. Microsoft recognizes that new credential as legitimate because it was created through the account's genuine enrollment process.

The lesson for CISOs is precise. Phishing resistant authentication does not automatically create phishing resistant enrollment. Passkeys are only fully secure when the enterprise can prove who is enrolling the credential, which physical device will contain it, whether the legitimate user is physically present, and whether the enrollment is occurring at an authorized endpoint.

THE CRITICAL DISTINCTION

The attacker does not compromise passkey cryptography. The attacker exploits a weaker enrollment process to create a new valid credential inside the victim's real account.

Why This Matters Now

The campaign is especially effective because many organizations are actively asking employees to adopt passkeys. A caller claiming to support a company security rollout is not inventing an implausible story. The attacker is inserting a fraudulent process into a real enterprise initiative, using familiar Microsoft screens and legitimate security notifications to make the deception feel authentic.

ANATOMY OF THE CAMPAIGN

How the Microsoft Entra Passkey Enrollment Attack Works

1 The Attacker Prepares a Convincing Enrollment Portal

The criminal registers a domain containing credible terms such as passkey, register, deploy, assign, security, or Microsoft. The site is customized with the target organization's branding, Microsoft styling, and language that resembles an internal authentication rollout.

2 The Employee Receives a Call From Supposed IT Support

The attacker claims to represent the company help desk, Microsoft support, or the identity security team. The employee is told that passkey enrollment is required and is directed to the fraudulent portal.

3 The Employee Enters Microsoft Credentials

Believing the site is legitimate, the employee enters a Microsoft 365 username and password. The phishing platform immediately transfers those credentials to the attacker.

4 The Attacker Signs In to the Real Microsoft Account

From a separate computer, the attacker enters the stolen credentials into the legitimate Microsoft login page. The employee remains on the fraudulent site while the attacker advances through the real authentication flow.

5 The Fraudulent Portal Adapts in Real Time

The phishing platform can change what appears on the employee's screen as Microsoft presents authentication challenges. The caller keeps the employee engaged while the attacker satisfies the requirements of the legitimate account.

The Attacker Turns Account Access Into a Permanent Credential

6 The Attacker Begins Genuine Passkey Registration

Once inside the real Microsoft account, the attacker starts the legitimate passkey enrollment process. The new credential is created on hardware controlled by the attacker, not on the employee's computer, phone, or enterprise issued device.

7 The Employee Is Kept Occupied by Enrollment Theater

The fake portal may display progress messages, confirmation screens, or a fabricated recovery phrase. These elements are designed to make the employee believe the enrollment is continuing locally while the real registration is completed elsewhere.

8 Microsoft Sends a Legitimate Registration Notice

The employee may receive a genuine message stating that a new passkey was registered. Because the employee believes that registration was the purpose of the call, the legitimate warning appears to confirm success rather than expose the attack.

9 The Attacker Now Has Persistent Access

The phone call can end and the phishing site can disappear. The attacker possesses a valid passkey associated with the victim's real account and can continue using it until the credential is discovered and removed.

The Passkey Itself Was Not Compromised

The attacker did not extract the victim's existing passkey, defeat FIDO2, or cause a credential registered for a fraudulent domain to work against Microsoft. The attacker gained enough control of the real account to create a completely new passkey through Microsoft's legitimate enrollment process.

This distinction matters because the strength of the credential does not repair weakness in the process that creates, replaces, recovers, or approves it. If a weaker identity path can authorize a stronger credential, the weaker path determines the actual security of the system.

THE TOKEN MODEL

Why Dedicated Biometric Hardware Changes the Trust Model

A passkey stored on a general purpose computer or mobile device ultimately depends on the security, enrollment controls, and identity assurance of that device. The enterprise may have limited visibility into who was physically present, whether the device is personally owned, and whether the credential can be synchronized or recovered through another account.

Token binds the credential to dedicated biometric hardware. The private key remains inside the secure device, the authorized fingerprint is required to activate it, and physical proximity confirms that the authenticator is beside the endpoint requesting access. The system therefore establishes more than possession of a credential. It establishes the presence of the verified person at the legitimate endpoint.

Dedicated Secure Hardware

The credential is created and retained inside a purpose built authenticator. It cannot be exported, copied, or silently moved to an attacker controlled device.

Live Fingerprint Verification

Every sensitive authentication or enrollment action requires the authorized fingerprint directly on the Token device. Account possession alone is not sufficient.

Physical Proximity

The authenticator must be near the endpoint performing the action. A caller operating from another location cannot turn an employee into a remote approval mechanism.

Cryptographic Origin Binding

The credential responds only to the legitimate relying party. A fraudulent enrollment site cannot obtain a valid Token assertion for Microsoft.

No Cloud Credential Sync

The private key remains in dedicated hardware rather than being synchronized through a consumer cloud account or copied across general purpose devices.

Enterprise Lifecycle Control

The organization can require the existing Token device before another authenticator, recovery method, or endpoint is added to the account.

How Token Stops This Attack Cold

The Fake Portal Cannot Collect a Reusable Credential

The Token private key never leaves the hardware and is never entered into a web page. A fake portal can imitate the appearance of Microsoft, but it cannot collect, copy, or relay the cryptographic credential. The device will not create a valid assertion for the fraudulent relying party.

The Attacker Cannot Register a Replacement Credential Remotely

The enterprise can require the employee's existing Token device before any new passkey, authenticator, recovery method, or endpoint is added to the account. The registration action would therefore require the authorized hardware, the registered fingerprint, the legitimate service, and physical proximity to the endpoint conducting the enrollment.

An attacker working from another computer cannot satisfy that chain of trust. Control of the Microsoft account is not enough. A persuasive call is not enough. A copied screen is not enough. The new passkey cannot be registered because the attacker cannot produce the existing Token device, the fingerprint, and proximity at the attacker controlled endpoint.

The Employee Can Still Be Deceived, but the Deception Cannot Create Access

The attack may still convince an employee that a fake enrollment site is legitimate. Token does not depend on every employee recognizing every sophisticated deception. It makes the deception operationally useless. The attacker cannot transfer the hardware, copy the private key, manufacture physical proximity, or reproduce the authorized fingerprint.

> THE HARD STOP
>
> No Token device, no biometric approval, no authorized enrollment. The attacker may control the conversation, but cannot create the credential.

The Entire Identity Lifecycle Must Use the Same Standard

This campaign exposes a broader architectural issue. Strong authentication at login is not enough when a weaker process can create or replace the credential. The same assured identity standard must govern initial enrollment, authenticator replacement, account recovery, device registration, credential removal, privilege elevation, and help desk assisted restoration.

A company cannot require dedicated biometric hardware for normal access while allowing support personnel to bypass it through a phone conversation. It cannot protect routine login with a hardware bound passkey while permitting a new passkey to be added through a weaker recovery route. Every process that creates or transfers trust must require the same verified person, registered device, legitimate service, and authorized endpoint.

PASSKEY SECURITY WITH AND WITHOUT DEDICATED BIOMETRIC HARDWARE

SECURITY QUESTION	PASSKEY WITHOUT DEDICATED BIOMETRIC HARDWARE	PASSKEY BOUND TO TOKEN
Who can authorize enrollment	May depend on account access and the controls of a general purpose device	Requires the registered Token device and the authorized fingerprint
Where the private key lives	May be stored or synchronized within a broader device ecosystem	Remains inside dedicated secure hardware
Can the credential be copied or synced	Depends on platform and account recovery design	No. The private key is not exported or cloud synchronized
Is physical presence proven	Not necessarily at the endpoint where the new credential is created	Yes. Proximity is enforced at the endpoint
Can a remote attacker enroll a new credential	Possible when the attacker first gains sufficient account control	Blocked when the existing Token device is required for enrollment

A New Standard for Enterprise Passkey Security

Passkeys remain an important improvement over passwords, but they should not be treated as the final answer for high value enterprise identity. The cryptography can be secure while enrollment remains vulnerable to human deception and account takeover.

For sensitive systems, a passkey should be bound to dedicated biometric hardware. The organization should know exactly which device contains the credential, which individual can activate it, which endpoint is requesting the action, and whether that person is physically present during enrollment and use.

That is the difference between passwordless authentication and Biometric Assured Identity. Token makes the creation and use of a credential dependent on the legitimate person, the registered physical authenticator, the authorized endpoint, and the real service. Without those elements, no new credential should be enrolled and no access should be granted.

THE STANDARD

No Token device, no enrollment.
No Token device, no entry.

PRIMARY REPORTING

- The Hacker News, Hackers Use Fake Microsoft Entra Passkey Enrollment Sites
- BleepingComputer, Entra Passkey Enrollment Vishing Targets Microsoft 365 Users
- Okta Threat Intelligence, Vishing Actors Target Microsoft Entra Passkey Enrollment
- Token, Biometric Authentication for Enterprise Security