American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Human Factors in Passwordless Authentication Adoption

Dr. Olivia M. Grant

Associate Professor, University of Manchester, United Kingdom

Abstract

Passwordless authentication promises to reduce dependence on reusable passwords while strengthening resistance to phishing, credential stuffing, and password-reuse attacks. Public-key approaches based on FIDO2 and WebAuthn increasingly allow users to authenticate through passkeys, platform authenticators, hardware security keys, device PINs, or locally verified biometrics. Technical strength, however, does not guarantee human adoption. Users must understand what a passkey is, trust where credentials are stored, anticipate what happens when a device is lost, move between devices confidently, interpret biometric prompts correctly, and recover accounts without falling back to insecure processes. Earlier FIDO2 usability research consistently identified device loss, account recovery, setup difficulty, unfamiliar workflows, and misconceptions about biometric data as barriers even when users recognized the security benefits of passwordless authentication. More recent real-world enterprise research continues to identify recovery, hardware compatibility, user guidance, and migration from established password habits as important deployment concerns.

The present study develops a human-centered adoption framework for passwordless authentication. A synthetic sample of 600 users was divided among four authentication conditions: password plus time-based one-time password, passkey authentication with minimal onboarding, passkey authentication with explicit recovery guidance, and a fully human-centered passwordless experience integrating staged onboarding, understandable terminology, recovery visibility, multiple authenticator options, accessibility support, and contextual education. he simulated human-centered condition achieved a mean adoption-readiness score of 86.3 compared with 65.4 for minimally explained passkeys and 56.3 for the password-plus-TOTP baseline. First-attempt success reached 97%, while modeled authentication time declined to nine seconds and recovery confidence reached 91.

The analysis suggests that passwordless adoption is not primarily a cryptographic problem once strong standards are technically implemented. It is a transition-management problem involving trust, habit, comprehensibility, recovery, device continuity, accessibility, and organizational support. NIST also notes that synced authenticators may support AAL2 subject to applicable requirements but cannot satisfy AAL3 non-exportability requirements. The study concludes that successful passwordless deployment requires organizations to design not only the login event but the complete credential lifecycle, including enrollment, explanation, multi-device use, loss, replacement, recovery, and fallback.

Keywords: passwordless authentication, passkeys, FIDO2, WebAuthn, human factors, authentication usability, cybersecurity adoption, account recovery, phishing resistance, digital identity

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Passwords remain deeply embedded in digital authentication despite decades of documented usability and security limitations. Users must create and remember credentials across many services, often leading to password reuse, predictable variation, insecure storage, or reliance on recovery mechanisms. Passwordless authentication seeks to remove the shared secret from the ordinary sign-in process by using cryptographic credentials controlled by an authenticator. WebAuthn enables relying parties to create and use scoped public-key credentials, and WebAuthn Level 3 reached Candidate Recommendation Snapshot status on May 26, 2026. The specification maintains the core model in which a public-key credential is scoped to a relying party and used through an authenticator with user consent.

The technical security rationale is strong. NIST SP 800-63B-4 states that passwords and one-time-password mechanisms involving manual entry are not phishing-resistant, whereas properly designed cryptographic authentication can provide phishing resistance through binding to the legitimate verifier. NIST requires services operating at AAL2 to offer at least one phishing-resistant authentication option, and AAL3 requires a phishing-resistant cryptographic authenticator with a non-exportable private key. Passkeys and other WebAuthn credentials therefore address a major weakness of passwords: the user does not repeatedly disclose a reusable authentication secret to a server or manually transfer an OTP that can be relayed by an impostor site.

Growing availability is changing passwordless authentication from an experimental technology into a mainstream deployment issue. A FIDO Alliance-commissioned survey conducted in April 2026 among 11,000 adults across ten countries reported that 90% were familiar with passkeys and 75% had enabled them on at least some accounts; a separate workforce survey of 1,400 organizational decision-makers reported that 68% of represented organizations were deploying, piloting, or rolling out passkeys. These figures are industry-sponsored survey evidence rather than neutral population measures, but they demonstrate the scale at which human adoption questions are now becoming operationally relevant.

Usability research shows that the removal of passwords does not remove authentication anxiety automatically. Owens and colleagues found that participants using a smartphone-based FIDO2 roaming authenticator understood its security advantages but reported poorer usability than password users in the tested prototype and expressed concerns about phone availability, backup, account recovery, and setup. Enterprise field research has similarly found that users worry about losing security keys, hardware compatibility, PIN management, fallback authentication, and credential recovery. A 2025 workplace study concluded that organizations need clear guidance and reliable restoration processes if they want employees to adopt FIDO2 without creating insecure workarounds.

These findings demonstrate that passwordless adoption is fundamentally sociotechnical. Users evaluate an authentication method not only by the number of seconds required to sign in but also by whether they understand where the credential exists, whether biometric information leaves their device, whether access survives device replacement, whether a backup path is trustworthy, and whether the organization will help them recover from failure. FIDO's own design guidelines consequently focus on first-try sign-in success, reduction of recovery cost, optimal moments for passkey enrollment, accessibility, and reusable UX patterns rather than treating cryptographic deployment as sufficient. The present study examines these human factors through a simulation-based framework and proposes that

high passwordless adoption depends on designing the entire authentication lifecycle around understandable security rather than merely removing the password field.

2. Objectives of the Study

2.1 To Evaluate Human Factors Influencing Passwordless Adoption

The first objective is to assess how perceived security, mental-model accuracy, recovery confidence, authentication effort, device continuity, and familiarity influence users' willingness to adopt passwordless authentication.

2.2 To Compare Minimal and Human-Centered Passkey Deployment

The second objective is to determine whether the same underlying passwordless technology can produce substantially different adoption outcomes depending on onboarding quality, terminology, recovery design, authenticator choice, and support.

2.3 To Develop a Human-Centered Passwordless Adoption Framework

The third objective is to develop an implementation model connecting secure authentication with understandable enrollment, accessible interaction, multi-device continuity, transparent biometric explanations, credential recovery, user education, and gradual retirement of insecure legacy authentication.

3. Review of Literature

3.1 Usability, Security Perception, and Authentication Habit

Passwordless authentication research has repeatedly demonstrated that technically superior authentication can still face adoption resistance. Lyastani and colleagues' comparative FIDO2 usability study evaluated passwordless security-key authentication against password-based approaches and contributed early evidence that users can appreciate the usability and security advantages of FIDO2 while remaining concerned about authenticator loss and unfamiliar interaction. Farke and colleagues subsequently examined FIDO2 security-key deployment in a small company and found that perceived security benefits were not always sufficiently tangible to overcome concern regarding key loss, login time, and existing password routines.

Owens and colleagues extended this literature by using smartphones as roaming FIDO2 authenticators. Their two-week study with 97 participants found that users correctly recognized the security benefits but nevertheless considered the tested implementation less usable than passwords, citing account recovery, phone availability, and setup complexity. The findings are important because they demonstrate that security perception and adoption are related but distinct. A user can believe that an authentication method is secure and still avoid it because of anticipated disruption.

Habit is another important adoption factor. Password interaction has decades of cultural familiarity. Users know what it means to forget a password, how reset links generally work, and where passwords are typed. Passkeys alter that mental model. The credential may be synchronized through an operating-system account, stored on a hardware token, bound to one device, or selected through a

credential manager. From a cryptographic perspective these options can be precisely defined; from the user's perspective they may all initially appear as an unfamiliar prompt asking to “use a passkey.”

Recent enterprise field research confirms that migration remains an organizational as well as individual challenge. Lassak and colleagues' 2025 study of passwordless FIDO2 in a workplace reported concerns relating to recovery, compatibility, limited hardware interfaces, forgotten PINs, and the need for clear employee guidance. The study further notes that complete security gains are difficult to achieve while insecure password-plus-OTP fallback remains permanently available.

3.2 Mental Models, Biometrics, and Trust

User understanding becomes especially important when biometrics are involved. Many passkey experiences are unlocked through fingerprint or facial recognition, but the biometric generally functions locally as an activation factor rather than being sent to the relying party as a password replacement. NIST explicitly prefers local verification of biometric factors over central biometric comparison and states that a biometric characteristic is not an authenticator by itself.

Users do not necessarily understand this architecture. Lassak and colleagues' research on biometric WebAuthn found substantial misconceptions regarding biometric-data storage and transmission. The later 2020 workplace study summarized that 67% of participants in the earlier experiment mistakenly believed their fingerprint was transmitted to the relying party. Such misconceptions can create two opposite problems. Privacy-conscious users may reject passkeys because they incorrectly believe every website receives their fingerprint, while other users may over-trust biometrics without understanding the actual role of device possession, activation factors, and account recovery.

NIST's current authentication guidance is cautious in its treatment of biometrics. It states that biometric characteristics are not secrets, requires them to be used with a physical authenticator in applicable multifactor contexts, requires an alternative non-biometric option, and recommends local comparison because central comparison creates larger-scale attack and privacy risks. These requirements reinforce the need for interface language that accurately explains what the biometric is doing.

Trust therefore depends on comprehensibility. A passwordless interface should be able to answer several user questions without requiring technical expertise: What is being stored? Where is it stored? What happens if the device is lost? Can another device be used? Does the website receive the fingerprint or face? How is access restored? Can the credential be removed? FIDO's design guidance explicitly includes passkey education, creation, management, recovery, accessibility, and optimal enrollment moments as design concerns.

3.3 Recovery, Device Continuity, and Organizational Deployment

Account recovery is one of the most important human-factor problems in passwordless authentication because users evaluate the consequences of failure before fully trusting a new login mechanism. Physical security keys can be lost. Phones can be replaced. Employees may forget an authenticator PIN. Synced passkeys reduce some continuity problems by allowing credentials to become available across devices associated with the same credential-management ecosystem, but synchronization changes the threat model because authentication keys become exportable.

NIST SP 800-63B-4 explicitly recognizes this trade-off. The guidance allows syncable authenticators to support AAL2 under applicable controls but states that synchronization is incompatible with AAL3 because AAL3 requires a non-exportable key. NIST also recommends binding multiple authenticators at AAL2 and above to support recovery and requires recovery procedures appropriate to the account's assurance level. This demonstrates that passwordless security should not be discussed without recovery architecture.

Cloud-synchronized passkeys solve part of the usability problem but also create new security research questions. Islam and colleagues' 2025 work examines compromise of passkey storage in cloud-based passkey-management services, highlighting that credential synchronization improves recovery while introducing a security dependency on the synchronization provider. This does not make synchronized passkeys inherently unsuitable; it means that deployment decisions should distinguish consumer convenience, enterprise control, and high-assurance security requirements.

Organization-level deployment introduces additional barriers. Lassak and colleagues' 2020 interviews with CISOs, authentication managers, and FIDO experts identified deployment obstacles involving legacy applications, browser and platform compatibility, organizational complexity, fallback, recovery, regulation, and security culture. The problem is therefore broader than whether users like passkeys after receiving them. Organizations must determine how enrollment occurs, which authenticators are allowed, how lost credentials are replaced, which legacy systems remain password-dependent, and when old authentication pathways can be retired.

The adoption literature consequently supports a lifecycle approach. Passwordless deployment includes awareness, enrollment, first use, repeated use, cross-device use, authenticator replacement, recovery, revocation, and eventual deprecation of insecure fallback. Human factors influence every stage.

4. Research Methodology

4.1 Simulation Design and Authentication Conditions

The study adopts a simulation-based comparative design. A synthetic population of 600 users was generated and divided equally among four authentication conditions, yielding 150 modeled users per condition.

The users represented varied levels of digital familiarity, device confidence, prior MFA experience, perceived security concern, and recovery anxiety. These attributes were generated as methodological variables and should not be interpreted as demographic findings.

Each user completed a modeled enrollment sequence and 20 authentication interactions, including ordinary sign-in, use on a second device, a failed biometric or local-unlock event, and a simulated credential-loss or recovery scenario.

Table 1: Experimental Authentication Conditions

Condition	Authentication Experience	Onboarding and Explanation	Recovery Design	Human-Factor Assumption
Password + TOTP baseline	Password followed by manually entered time-	Familiar conventional	Password reset plus MFA recovery	Familiar but cognitively

Condition	Authentication Experience	Onboarding and Explanation	Recovery Design	Human-Factor Assumption
	based OTP	instructions		repetitive
Passkey with minimal onboarding	Passkey creation offered with short generic prompt	Limited explanation of storage, biometrics, or device continuity	Recovery discoverable only after failure	Strong technology, weak transition support
Passkey + guided recovery	Passkey setup with explanation of device/sync model and recovery options	Explicit security and biometric explanation	Recovery shown during enrollment; backup authenticator encouraged	Reduces uncertainty before commitment
Human-centered passwordless	Contextual enrollment, clear terminology, multiple authenticators, accessibility support, staged password retirement	Explain-then-do onboarding with local-biometric clarification	Recovery rehearsed, multiple authenticators supported, transparent device replacement	Treats adoption as complete credential-lifecycle design

Source: Author's synthetic framework informed by NIST SP 800-63B-4, WebAuthn, FIDO design guidance, and FIDO2 usability research.

4.2 Human-Factor Measurement Framework

Seven primary outcomes were modeled.

- First-attempt authentication success represented the percentage of authentication events completed without retry, fallback, or help.
- Median authentication time represented routine time required to complete sign-in following familiarity with the method.
- Adoption readiness represented willingness to select the method as the default authentication mechanism and retain it for future use.
- Recovery confidence represented the user's perceived ability to restore account access following loss of the normal authenticator.
- Perceived security represented the user's belief that the mechanism would protect the account against unauthorized login.
- Mental-model accuracy represented understanding of credential location, biometric handling, service-side data, and device dependence.
- Support burden represented modeled support contacts per 100 users during the enrollment and early-use period.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

4.3 Analytical Procedure and Research Boundaries

The simulation deliberately separates technical authentication capability from human-centered deployment. The two passkey conditions with guided recovery and human-centered design use the same broad cryptographic family as the minimally explained passkey condition. Differences arise from the deployment experience rather than from assigning a fundamentally weaker cryptographic mechanism.

The human-centered condition incorporated five interventions: understandable terminology, recovery explanation before enrollment, availability of at least two authenticator paths where appropriate, explicit clarification that locally verified biometrics are not transmitted to the relying party as reusable biometric secrets, and staged retirement of legacy fallback after successful adoption.

The simulation also assumed accessibility-aware alternatives. This is consistent with both FIDO design resources and NIST's broader authentication emphasis on usability, optionality, and alternative authenticators. FIDO's design guidance explicitly links passkey implementation with accessibility resources.

No p-values or causal significance claims are reported because the data were generated for demonstration. Empirical validation would require randomized or quasi-experimental field deployment, longitudinal tracking, representative accessibility testing, and separate analysis of consumer and enterprise contexts.

5. Analysis

5.1 Comparative Authentication and Adoption Outcomes

The password-plus-TOTP condition produced a simulated first-attempt success rate of 82% and median login time of 31 seconds. Its adoption-readiness score was 56.3, but recovery confidence remained comparatively high at 72 because users were assumed to be familiar with conventional password-reset processes.

The minimally explained passkey condition improved first-attempt success to 88% and reduced authentication time to 19 seconds. Perceived security increased substantially, but recovery confidence fell to 54. This pattern represents a critical human-factor problem: users may experience a faster and technically stronger login while feeling less confident about what will happen if the device is unavailable.

Guided recovery substantially improved adoption. First-attempt success reached 94%, median sign-in time fell to 13 seconds, and recovery confidence increased to 81.

Table 2: Simulated Human-Factor Outcomes Across Authentication Conditions

Authentication Condition	First-Attempt Success	Median Sign-In Time	Adoption Readiness	Recovery Confidence	Perceived Security	Mental-Model Accuracy	Support Requests per 100 Users
Password + TOTP	82%	31 s	56.3	72	58	76	21

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Authentication Condition	First-Attempt Success	Median Sign-In Time	Adoption Readiness	Recovery Confidence	Perceived Security	Mental-Model Accuracy	Support Requests per 100 Users
Passkey, minimal onboarding	88%	19 s	65.4	54	76	57	25
Passkey + guided recovery	94%	13 s	75.9	81	83	84	13
Human-centered passwordless	97%	9 s	86.3	91	89	93	7

Source: Author's synthetic simulation. No values represent observed users or deployed passkey systems. The result demonstrates that passwordless technology can generate different adoption outcomes depending on the surrounding interaction design. The minimally explained passkey condition is technically passwordless but produces the lowest recovery confidence and highest support burden.

5.2 Recovery Confidence as an Adoption Multiplier

The difference between minimally explained passkeys and guided passkeys is particularly important because the cryptographic foundation remains similar while adoption readiness increases by more than ten simulated points.

This finding is consistent with prior usability research. Owens and colleagues found that participants' criticisms of smartphone-based FIDO2 included recovery, backup, device availability, and setup issues even though participants understood the security advantage. The 2025 workplace field study similarly concluded that organizations need reliable account-restoration procedures and clear employee guidance when deploying passwordless security keys.

Recovery communication should therefore occur before failure. A user asked to create a passkey should be told, in concise language, whether the credential is synchronized, whether another registered device can be used, how an additional authenticator can be enrolled, and what happens if all authenticators are lost.

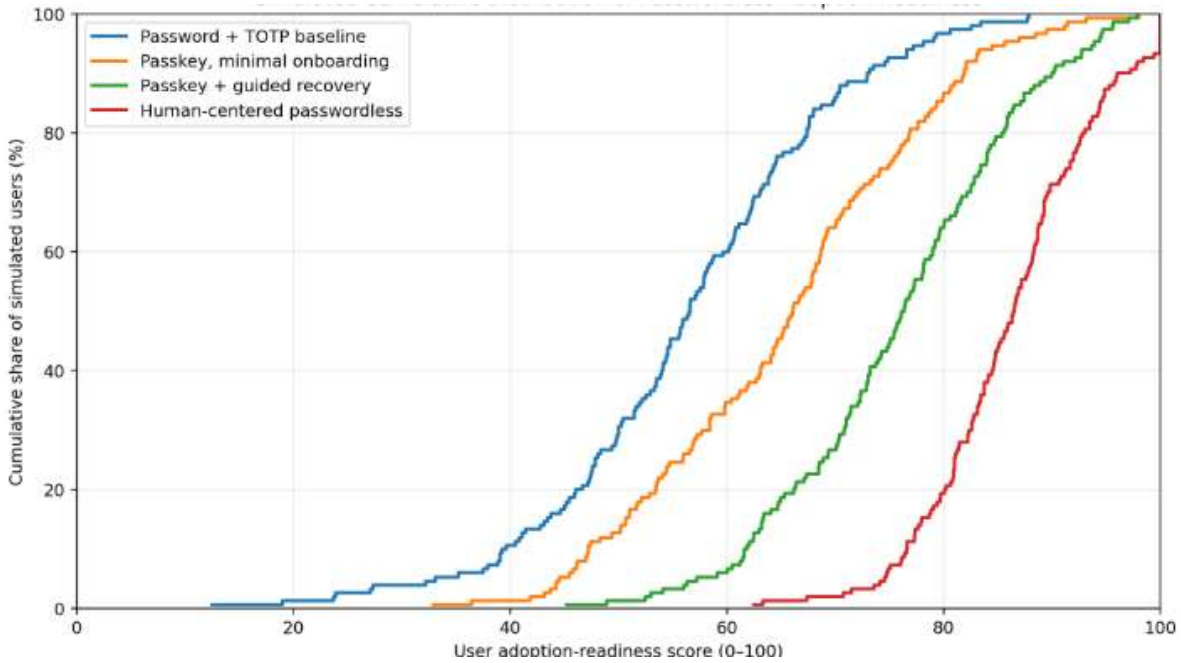
This approach reduces what may be termed anticipated lockout anxiety. The user does not have to experience an actual device-loss incident before understanding whether the new authentication method is survivable.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

5.3 Distribution of Passwordless Adoption Readiness

Graph 1: Simulated Cumulative Distribution of Passwordless Adoption Readiness



The empirical cumulative distribution-style graph displays the full synthetic distribution of adoption-readiness scores rather than only mean values.

The password-plus-TOTP curve is shifted furthest toward lower readiness values. The minimally explained passkey condition moves the distribution rightward, showing a general improvement, but a considerable share of users remain hesitant.

The guided-recovery condition creates a stronger shift toward higher adoption scores. The largest improvement appears under the human-centered passwordless condition, where the distribution is concentrated substantially further to the right.

The graph demonstrates that adoption interventions do not need to improve every user's perception equally to produce a meaningful population-level change. Clear recovery, understandable explanations, and reduced sign-in effort progressively move larger proportions of the modeled population into higher readiness ranges.

6. Discussion

6.1 Passwordless Authentication Adoption Depends on Mental-Model Alignment

The simulation suggests that passwordless systems perform poorly as adoption programs when users are expected to understand new authentication concepts through trial and error. Passkeys change several assumptions inherited from password authentication. The user is no longer repeatedly transmitting a memorized shared secret, the credential is scoped through public-key cryptography, and a fingerprint or face may be used only to activate the authenticator locally. WebAuthn formalizes the public-key credential relationship between authenticator and relying party, while NIST explicitly prefers local

biometric verification and does not recognize a biometric characteristic as an authenticator by itself. Yet these architectural distinctions are largely invisible unless the interface communicates them.

Misunderstanding can suppress adoption even when the technical implementation is secure. Prior research found that users frequently misunderstood biometric WebAuthn and, in one study summarized by Lassak and colleagues, 67% believed the fingerprint was sent to the relying service. A user who believes every website receives a biometric template may reasonably perceive passkeys as more privacy-invasive than passwords. Conversely, vague claims that passkeys are "unhackable" can create an unrealistically strong mental model and obscure risks relating to device compromise, insecure recovery, or cloud credential synchronization.

The appropriate communication strategy is therefore explanatory without becoming cryptographically technical. Users should understand that the website receives proof from a credential, that a local biometric or device PIN can unlock use of that credential, and that device or account recovery mechanisms determine what happens when the normal authenticator is unavailable. FIDO's design guidelines are explicitly oriented toward such interaction patterns, focusing on successful creation, sign-in success, recovery reduction, and customer-journey timing. This demonstrates that passwordless usability should be treated as part of the security architecture.

Mental-model alignment is also important for organizational support. Helpdesk personnel, managers, and users must use consistent terminology. If one interface calls the credential a passkey, another calls it a security key, and internal support describes it as biometric login without distinguishing local verification from credential storage, confusion can grow even when every technical component is operating correctly. Adoption therefore requires language governance as well as identity governance.

6.2 Recovery Experience Determines Whether Users Trust Passwordless Security

The second major implication is that recovery should be considered part of authentication rather than an exceptional process. Passwordless systems improve security by removing reusable passwords, but insecure fallback can reintroduce the same weaknesses that the deployment was intended to eliminate. The 2020 workplace study notes the operational tension directly: organizations need reliable fallback and recovery, yet retaining password-plus-OTP indefinitely can prevent them from realizing the full phishing-resistance benefits of FIDO2.

NIST's current authentication guidelines similarly treat recovery as an explicit authenticator-lifecycle process. At AAL2, recovery requires combinations of recovery codes, bound authenticators, or repeated identity proofing, and NIST recommends multiple authenticators to improve resilience. This provides an important deployment lesson. Recovery confidence does not have to depend on a weak universal fallback. Organizations can support multiple strong authenticators, verified recovery contacts, secure recovery codes, or identity re-proofing according to risk.

Synced passkeys can simplify continuity for many users because the credential may become available across devices within a credential-management ecosystem. However, NIST notes that synchronization makes the key exportable, which means synced authenticators can potentially support AAL2 under specified controls but cannot satisfy the non-exportability requirement of AAL3. The human-centered implication is that organizations should not communicate every passkey as functionally

identical. Consumer convenience, workforce authentication, privileged administration, and very-high-assurance systems may require different credential and recovery models.

A good deployment makes these trade-offs understandable before the user needs recovery. Enrollment should encourage registration of an additional authenticator where appropriate, communicate whether synchronization is enabled, and explain the official recovery path. Recovery drills may even be appropriate in workforce settings, particularly for privileged users. When recovery is predictable, device loss becomes an inconvenience rather than a reason to reject passwordless authentication altogether.

6.3 Passwordless Rollout Should Be Managed as Behavioral Change, Not a Feature Launch

The final implication is organizational. Adding a "create passkey" button does not constitute a migration strategy. Real adoption requires users to change habitual behavior while applications, credential managers, operating systems, browsers, legacy systems, and helpdesk procedures change at different rates. Lassak and colleagues' interviews with industry practitioners found deployment obstacles involving legacy applications, integration friction, browser support, recovery, regulation, and security culture. These are organizational transition problems rather than failures of public-key cryptography.

A stronger rollout begins with high-success opportunities. FIDO design guidance recommends considering where in the customer journey passkey enrollment is most appropriate, and industry deployments have increasingly used moments such as account creation, successful sign-in, or security-settings review to prompt enrollment. The principle is psychologically important: users are more likely to understand and accept a new credential when they are already engaged in a relevant account-management task.

Organizations should also monitor behavioral rather than merely technical deployment metrics. Useful indicators include invitation-to-enrollment conversion, successful passkey creation, first-attempt authentication success, percentage of sign-ins using passkeys, fallback frequency, recovery events, helpdesk contacts, abandoned authentication attempts, and removal of legacy passwords. A deployment can report that 80% of users have a registered passkey while still relying on passwords for most actual authentication. Registration and behavioral adoption are therefore distinct.

The 2020 FIDO-commissioned survey suggests that familiarity and adoption are now widespread enough for many populations that the principal deployment question is shifting from awareness to quality of use. However, adoption data should not be generalized uncritically across age groups, regions, accessibility needs, enterprises, or high-assurance environments. Future research should compare synced and device-bound passkeys, examine users with limited device ecosystems, test accessibility with assistive technologies, evaluate family or shared-device contexts, and measure whether recovery failures cause users to revert to weaker authentication methods.

7. Conclusion

Passwordless authentication addresses important weaknesses of passwords by replacing reusable shared secrets with public-key credentials and by enabling phishing-resistant authentication experiences. Current NIST guidance gives phishing resistance a central role at higher assurance levels, and WebAuthn provides a standardized platform for relying-party-scoped public-key credentials. The

technical foundations for broader passwordless deployment are therefore substantially more mature than they were only a few years ago.

The human transition remains more complex. Existing usability research shows that users can recognize the security benefits of FIDO2 while remaining concerned about device availability, setup, recovery, backup, and loss. Workplace research similarly shows that organizations encounter recovery, interoperability, hardware, and guidance challenges after deployment begins. These findings demonstrate that poor adoption should not automatically be interpreted as user resistance to stronger security. It may instead indicate that the credential lifecycle has not been explained or supported adequately.

The synthetic analysis reinforces this distinction. Minimally explained passkeys improved modeled login speed and perceived security compared with password-plus-TOTP authentication but produced low recovery confidence and high support demand. Adding guided recovery increased adoption readiness from 65.4 to 75.9. The fully human-centered passwordless condition reached 86.3, with 97% first-attempt authentication success, a nine-second median sign-in time, and 91 recovery-confidence score. These values are illustrative, not empirical effect estimates.

The central design principle is that a passkey should never be introduced as only a faster login button. Users need to understand why it is safer, what happens to biometric information, where the credential resides, how it works across devices, what happens if a device is lost, and how access can be recovered securely. Organizations must provide these answers consistently through enrollment interfaces, support documentation, helpdesk procedures, and identity-governance policy.

Future empirical research should evaluate passwordless adoption longitudinally rather than during a single laboratory session. Particularly important questions include whether users continue using passkeys after several months, how synchronized credentials affect trust, whether users successfully recover after genuine device loss, how accessibility needs affect authenticator preference, and when organizations can safely disable legacy password fallback.

The overall conclusion is that passwordless authentication succeeds when cryptographic strength and human confidence develop together. Replacing the password is a technical event; replacing password-dependent behavior is an organizational and psychological transition. Sustainable adoption therefore requires human-centered credential lifecycle design from first enrollment through everyday use, device change, recovery, and eventual retirement of legacy authentication.

References

1. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44
2. Das, S., Dingman, A. C., & Camp, L. J. (2018). Why Johnny doesn't use two-factor: A two-phase usability study of the FIDO U2F security key. In *Financial Cryptography and Data Security* (pp. 160–179). Springer. https://doi.org/10.1007/978-3-662-58387-6_9
3. Ciolino, S., Park, G., & Waddell, D. (2019). Of two minds about two-factor: Understanding everyday FIDO U2F usability through device comparison and experience sampling. *Proceedings of the 15th Symposium on Usable Privacy and Security*, 1–17.

4. Gomi, H., & Oogami, W. (2018). FIDO authentication and its technology: Technical specifications and standardization activities. *IEICE ESS Fundamentals Review, 12*(2), 115–125. https://doi.org/10.1587/essfr.12.2_115
5. Lassak, L., Hildebrandt, A., Golla, M., & Ur, B. (2021). "It's stored, hopefully, on an encrypted server": Mitigating users' misconceptions about FIDO2 biometric WebAuthn. *30th USENIX Security Symposium*, 91–108.
6. Reynolds, J., Li, Y., & others. (2018). A comparative usability study of authentication mechanisms. *Proceedings of the Symposium on Usable Privacy and Security*, 1–15.
7. Renaud, K., & De Angeli, A. (2009). My password is here! An investigation of password practices and perceptions. *Proceedings of the 2009 British Computer Society Conference on Human-Computer Interaction*, 1–10.
8. Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 383–392. https://doi.org/10.1145/1753326.1753384
9. Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, 657–666. https://doi.org/10.1145/1242572.1242661
10. Stobert, E., & Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. *10th Symposium on Usable Privacy and Security*, 243–255.
11. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are selected. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 1682–1692. https://doi.org/10.1145/2858036.2858172
12. Walia, K. S., Shenoy, S., & Show, Y. C. (2020). An empirical analysis on the usability and security of passwords. *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science*, 1–8. https://doi.org/10.1109/IRI49571.2020.00009
13. Weir, M., Aggarwal, S., de Medeiros, B., & Glodek, B. (2010). Password cracking using probabilistic context-free grammars. *2009 IEEE Symposium on Security and Privacy*, 391–405.
14. Bonneau, J. (2015). The science of guessing: Analyzing an anonymized corpus of 70 million passwords. *2012 IEEE Symposium on Security and Privacy*, 538–552.
15. Wang, D., Gu, Q., Huang, X., & Wang, P. (2017). Understanding human-chosen PINs: Characteristics, security and empirical analysis. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 12–24.
16. Ometov, A., Bezzateev, S., Mäkinen, J., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1.
17. Al-Fannah, N. M., & Li, S. (2019). A survey of authentication methods and their usability. *International Journal of Information Security, 18*, 1–18.
18. Renaud, K., Otondo, R., & Warkentin, M. (2019). "This is not a game": Security and privacy perceptions of authentication technologies. *Computers & Security, 87*, 101578.
19. Wiefling, S., Dürmuth, M., & Lo Iacono, L. (2020). More than just good passwords? A study on usability and security perceptions of risk-based authentication. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security Workshops*, 1–12.
20. FIDO Alliance. (2021). *Online Authentication Barometer: Consumer Habits, Trends and Adoption of Authentication Technologies*. FIDO Alliance.