Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Passwordless and Phishing-Resistant Authentication: The Next Frontier

Deepak Pandey
Simeio Solutions LLC, USA
Corresponding author: Deepak Pandey. **Email:** pandey.reach@gmail.com

| ABSTRACT

This article examines the transition from traditional password-based authentication systems to passwordless and phishing-resistant methods. Despite widespread awareness of password vulnerabilities, many organizations have hesitated to adopt alternative solutions due to implementation challenges and user experience concerns. However, recent technological advancements, regulatory changes, and increasing security threats have accelerated the shift toward more secure authentication methods. The article explores the current landscape of passwordless authentication, analyzing its benefits and challenges through examination of cognitive limitations in password management, the proliferation of sophisticated attack vectors, and the operational burdens of maintaining password infrastructures. It evaluates emerging technologies including biometric authentication, hardware tokens, mobile-based solutions, and certificate-based approaches. The article further discusses how regulatory frameworks across Europe, the United States, and globally are driving adoption, and provides a structured implementation framework addressing technical, operational, and human factors. It suggest that passwordless authentication will become the predominant approach to digital identity verification by 2025, fundamentally transforming user access while enhancing security posture.

| KEYWORDS

Passwordless authentication, Phishing resistance, Biometric verification, Digital identity, Cybersecurity compliance

| ARTICLE INFORMATION

ACCEPTED: 12 July 2025 **PUBLISHED:** 04 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.63

1. Introduction

For decades, passwords have served as the primary gatekeepers of digital access despite their well-documented shortcomings. The fundamental paradox of password-based security lies in the inverse relationship between security and usability: complex passwords that resist attacks are difficult for users to remember, while memorable passwords often fail to provide adequate protection. Recent research published in ACM Transactions on Privacy and Security reveals that when organizations implement stringent password complexity requirements, they inadvertently create significant cognitive burden on users, leading to counterproductive security behaviors [1]. A comprehensive longitudinal study tracking over 25,000 users across multiple organizations found that as password complexity requirements increased, instances of password reuse rose dramatically, with users recycling variations of the same password across an average of 7.4 distinct services. This behavior effectively nullifies the security benefits of complex password policies, as a single compromised credential can cascade into multiple system breaches across an organization's digital ecosystem [1]. This dichotomy has created an untenable situation where security breaches due to compromised credentials have become commonplace, costing organizations substantial financial losses annually in remediation efforts and reputational damage.

The limitations of password-based authentication extend beyond mere inconvenience. Credential-based attacks—including phishing, credential stuffing, and brute force attempts—have grown increasingly sophisticated, rendering traditional password systems inadequate for protecting sensitive data and critical infrastructure. The IBM Security Cost of a Data Breach Report demonstrates that organizations heavily reliant on password-based authentication experience significantly longer breach detection times, with the mean time to identify (MTTI) exceeding 287 days for companies without advanced authentication protocols [2]. This extended exposure window dramatically increases the scope and severity of breaches, as malicious actors gain extended access to internal systems. Furthermore, the report highlights a concerning trend wherein threat actors increasingly leverage automated credential harvesting techniques, enabling them to process billions of username/password combinations against multiple targets simultaneously, overwhelming traditional defense mechanisms [2]. The expanding attack surface created by remote work environments has further exacerbated these vulnerabilities, with remote endpoints becoming prime targets for credential theft through sophisticated social engineering campaigns that exploit human psychology rather than technical vulnerabilities.

Passwordless authentication represents a paradigm shift in identity verification, replacing knowledge-based factors (what you know) with possession-based (what you have) and inherence-based (what you are) factors that are significantly more difficult to compromise. The ACM study examining authentication method effectiveness across diverse organizational environments found that enterprises implementing passwordless technologies experienced pronounced security improvements, with phishing attack success rates declining by significant margins compared to control groups maintaining traditional password infrastructures [1]. This substantial risk reduction stems from the fundamental architecture of passwordless systems, which eliminate the transferable secrets that credential-based attacks exploit. The cryptographic binding of authentication to specific devices or biometric characteristics creates verification mechanisms that cannot be easily replicated or transferred between systems, addressing the core vulnerability of knowledge-based authentication approaches [1]. From biometric verification to hardware security keys and cryptographic authentication protocols, these emerging technologies promise both enhanced security and improved user experience—a rare combination in the cybersecurity domain.

This article examines the current state of passwordless authentication technologies, explores their benefits and limitations, analyzes the regulatory landscape driving their adoption, and provides a framework for organizations transitioning from traditional password systems. The IBM Security report emphasizes that organizations must evaluate authentication modernization within their broader security transformation initiatives, as identity verification represents a critical control point affecting numerous downstream security processes [2]. Organizations that have successfully implemented passwordless authentication report significant operational benefits beyond security improvements, including substantial reductions in help desk volumes related to credential management. The report documents cases where authentication-related support tickets decreased by substantial percentages following passwordless adoption, freeing technical resources for higher-value security initiatives [2]. As we approach 2025, understanding these developments is crucial for security professionals, technology leaders, and policymakers seeking to address the growing inadequacy of password-based security in an increasingly complex threat environment.

2. The Limitations of Password-Based Authentication

Password-based authentication systems have persisted as the dominant security mechanism for digital access despite their numerous vulnerabilities and limitations. This section examines the fundamental weaknesses that have rendered passwords increasingly inadequate for modern security requirements.

2.1 Cognitive Burden and User Behavior

The human cognitive limitations regarding password management create an intractable security problem. Research in cognitive psychology has established that the average person can effectively manage between five to seven complex passwords. However, comprehensive studies conducted by Bonneau and Preibusch reveal that the average working professional now maintains access to approximately 191 password-protected services, with this number increasing by 14% annually as digital transformation initiatives expand the application landscape within enterprises. This cognitive overload creates an insurmountable memory challenge that manifests in measurable security degradation across organizations of all sizes and sectors [3]. The authors' examination of 150 websites' password practices uncovered a troubling market failure in authentication security, where even security-sensitive websites rarely implemented robust password security measures. Their research documented that when faced with complex password requirements, users developed systematic patterns for password creation that significantly reduced their effective entropy despite meeting formal complexity requirements. The study found that password policies across sites showed dramatic inconsistencies, creating additional cognitive burden as users attempted to track different requirements across services. This fragmented authentication landscape leads to what the researchers termed "password recycling," where users modify a small set of core passwords to meet varying requirements, creating predictable patterns that attackers can exploit systematically. Perhaps most concerning, the cognitive burden of password management drove a majority of professionals to store passwords insecurely, with many maintaining unencrypted digital records and utilizing physical documentation methods such as notebooks or adhesive notes in workplace environments. These behaviors collectively undermine the theoretical security benefits of complex password policies, creating a substantial gap between security theory and operational reality that sophisticated attackers systematically exploit [3].

2.2 Attack Vector Proliferation

The attack surface for password-based systems has expanded dramatically in recent years, with multiple exploitation techniques achieving unprecedented success rates against traditional defenses. The Microsoft Digital Defense Report 2023 documents the evolution of credential-based attacks, finding that phishing campaigns have progressed from generic, mass-distributed attempts to highly targeted, contextually-aware approaches that leverage organizational intelligence and social engineering principles. Their analysis of authentication attempts across enterprise environments revealed that targeted phishing campaigns now achieve significantly higher success rates when incorporating organizational context and personal information, compared to generic attempts [4]. The report highlights that threat actors are increasingly using AI to generate more convincing phishing content, with well-crafted spear-phishing messages achieving click rates of over 30% in some organizations. This effectiveness reflects the sophistication of modern attack methodologies, which frequently incorporate real-time intelligence gathering and dynamic content adaptation. Beyond phishing, the report identifies credential stuffing as a persistent threat, noting that in 2023, Microsoft detected and blocked over 15 billion brute force authentication attacks against Azure Active Directory accounts. The report further documents how sophisticated credential stuffing operations now employ distributed infrastructure capable of testing millions of credential pairs daily while evading traditional rate-limiting and IP-based protections. Additionally, advanced persistent threat (APT) groups increasingly target authentication systems as primary attack vectors, with a significant percentage of documented APT campaigns incorporating credential theft components. The fundamental vulnerability connecting these diverse attack methodologies remains constant: knowledge-based authentication fundamentally relies on transferable secrets that can be extracted through technical or social means, creating an inherent security limitation that cannot be mitigated through policy enhancements alone [4].

2.3 Organizational Cost and Complexity

The maintenance of password infrastructures imposes significant and often underestimated operational burdens on organizations across multiple dimensions. Research conducted by Bonneau and Preibusch analyzing authentication practices across diverse organizations found that password-related support issues constituted a substantial percentage of total IT help desk volume, with this percentage increasing in regulated industries with stringent password rotation requirements [3]. Their economic analysis established that the fully loaded cost per password reset incident represents a significant expense when accounting for all associated costs, including help desk labor, lost productivity, and authentication infrastructure maintenance. The researchers identify what they term a "security-usability trade-off," where stringent password requirements create substantial operational friction while delivering questionable security benefits. Beyond direct support costs, the maintenance of password infrastructure requires substantial specialized resources, with organizations allocating significant personnel to password-related security administration. These responsibilities include password policy configuration and enforcement, directory management, authentication integration for new applications, and credential compromise monitoring. The research further documented that security teams typically dedicate considerable time to monitoring for credential compromises across dark web repositories and breach notification services, with a majority of organizations reporting at least one significant credential compromise incident annually despite these monitoring efforts. Perhaps most concerning from a security resource allocation perspective, the study found that organizations dedicated a substantial portion of their total security budget to password-related infrastructure and operations, creating opportunity costs that limited investment in emerging security capabilities better aligned with contemporary threat landscapes [3].

These cumulative limitations have created an environment where password-based systems provide diminishing security returns while consuming disproportionate resources, creating an unsustainable security posture for modern organizations facing sophisticated threat actors.

Challenge Category	Key Finding	Security Impact	Organizational Impact
Cognitive Burden	Average professional manages ~191 password-protected services	Password recycling across services	Reduced effective security posture
	Annual increase of 14% in password-protected services per user	Increased pattern-based password creation	Greater attack surface
	Users can effectively manage only 5-7 complex passwords	Insecure password storage methods (notebooks, sticky notes)	Increased vulnerability to credential theft
	Inconsistent password policies across services	Development of predictable password modification patterns	Exploitable password creation behaviors
Attack Vectors	Evolution from generic to targeted phishing campaigns	Higher success rates for contextually-aware attacks	Increased breach likelihood
	AI-generated phishing content	Higher click-through rates on malicious messages	More successful credential theft
	Credential stuffing attacks against enterprise services	Automated testing of millions of credential pairs daily	Continuous threat to authentication systems
	APT groups targeting authentication systems	Credential theft as primary attack vector	Persistent advanced threats
Organizational Costs	Password resets constitute major IT help desk volume	Substantial labor allocated to credential management	Reduced IT efficiency
	Significant cost per password reset incident	Ongoing operational expenses	Resource diversion from strategic security initiatives
	Security teams monitoring dark web for credential leaks	Regular credential compromise incidents	Reactive rather than proactive security posture
	Budget allocation to password infrastructure	Limited investment in advanced security capabilities	Security technology opportunity costs

Table 1: Password Management Challenges and Security Implications [3, 4]

3. Emerging Passwordless Authentication Technologies

The evolution beyond password-based authentication has accelerated significantly, producing a diverse ecosystem of passwordless technologies. This section examines the most promising approaches and their underlying mechanisms.

3.1 Biometric Authentication

Biometric authentication leverages unique physical or behavioral characteristics to verify identity, eliminating the need for memorized credentials. Research from SecureAuth's State of Authentication Report has documented substantial improvements in biometric technology accuracy and security over recent years [5]. Physiological biometrics including fingerprint recognition have achieved widespread adoption in consumer devices, with dramatic reductions in error rates compared to earlier implementations. Modern facial recognition systems now incorporate sophisticated liveness detection and 3D mapping technologies that significantly reduce vulnerability to presentation attacks. Iris scanning provides substantially higher entropy compared to typical passwords, offering mathematically superior security characteristics. The evolution of behavioral biometrics has further expanded authentication options, with keystroke dynamics, gait analysis, and voice pattern recognition enabling continuous verification beyond traditional point-in-time authentication approaches [5].

3.2 Hardware Authentication Tokens

Physical authentication devices provide cryptographically secure validation without requiring password input. Microsoft's deployment guide for phishing-resistant authentication has demonstrated that FIDO2-compliant security keys implementing public key cryptography substantially reduce phishing vulnerabilities compared to traditional password systems [6]. The documentation outlines how major organizations have documented significant reductions in account compromise rates following enterprise-wide deployments of hardware token authentication. These security keys create authentication mechanisms where private keys never leave the physical device, rendering remote credential interception impractical through current attack methodologies. Smart cards with embedded secure elements provide similar security benefits, particularly in highly regulated environments with stringent authentication requirements [6].

3.3 Mobile-Based Authentication

Smartphones have emerged as powerful authentication platforms, offering multiple passwordless options. SecureAuth's industry research indicates that push notification authentication combined with local biometric verification can substantially reduce friction in authentication workflows while maintaining strong security posture [5]. QR code scanning enables cross-device authentication without direct credential transmission, addressing key vulnerability points in traditional authentication flows. Mobile digital identity wallets represent a particularly promising development, consolidating multiple authentication credentials in secured hardware enclaves with biometric access controls. The widespread availability of smartphones in global markets creates opportunities for passwordless adoption without requiring additional hardware procurement [5].

3.4 Certificate-Based Authentication

Modern public key infrastructure (PKI) implementations provide strong cryptographic identity verification through client certificates bound to devices and zero-knowledge proofs that authenticate without revealing underlying credentials. Microsoft's guidance on phishing-resistant authentication documents significant reductions in successful attack rates when organizations implement certificate-based authentication compared to traditional password systems [6]. Self-sovereign identity frameworks built on distributed ledger technologies enable user-controlled identity verification without requiring centralized credential storage. These cryptographic approaches offer mathematical rather than policy-based security assurances, fundamentally addressing the shared-secret vulnerabilities inherent in traditional authentication models.

Authentication Category	Key Technologies	Security Benefits	Implementation Considerations	Adoption Factors
Biometric Authentication	Fingerprint recognition	Eliminates memorized credentials	Requires compatible hardware	Widespread in consumer devices
	Facial recognition with liveness detection	Significantly reduces presentation attacks	Privacy considerations	Integrated in mobile devices
Hardware Authentication Tokens	FIDO2-compliant security keys	Private keys never leave device	Physical token management	Strong phishing resistance
	Smart cards with secure elements	Strong cryptographic protection	Card issuance and lifecycle management	Common in regulated environments
Mobile-Based Authentication	Push notifications with biometric verification	Reduces authentication friction	Mobile app deployment	Leverages existing devices
	QR code scanning	Avoids credential transmission	Cross-device integration	Simple implementation path
	Mobile digital identity wallets	Consolidates multiple credentials	Secured hardware enclaves	Growing ecosystem support
Certificate-Based Authentication	Client certificates	Transparent authentication	Certificate lifecycle management	Browser and device integration
	Self-sovereign identity	User-controlled verification	Distributed ledger integration	Emerging standards adoption

Table 2: Emerging Passwordless Authentication Technologies Comparison [5, 6]

4. Regulatory Landscape and Compliance Drivers

The regulatory environment has become an increasingly powerful catalyst for passwordless authentication adoption, with frameworks around the world establishing new standards and expectations for digital identity verification.

4.1 European Regulatory Framework

The European Union has positioned itself at the forefront of digital identity regulation, creating comprehensive frameworks that actively promote passwordless technologies. The eIDAS 2.0 (Electronic Identification, Authentication, and Trust Services) regulation represents a transformative development in the European digital identity landscape. According to the European Commission's digital strategy documentation, this updated framework explicitly prioritizes secure authentication methods for the interoperable digital identity wallets that will be mandatory across all member states [7]. The regulation introduces technical requirements for authentication mechanisms, establishing more resistant technologies as the preferred approach for European digital identity systems. Complementing eIDAS 2.0, the General Data Protection Regulation's emphasis on data minimization principles has driven organizations toward tokenized authentication approaches that reduce exposure of personally identifiable information during verification processes. The European Union's digital identity framework further reinforces this trajectory through implementation guidance that specifically addresses the persistent vulnerability of credential-based systems to phishing and other social engineering attacks [7].

4.2 United States Regulatory Developments

While the U.S. lacks a unified federal framework comparable to eIDAS, several significant regulatory developments are driving passwordless adoption. Executive Order 14028 on improving national cybersecurity has established requirements for multi-factor, phishing-resistant authentication across federal agencies. As detailed in the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model, this approach has created substantial momentum for advanced authentication technologies throughout the federal ecosystem and associated contractor networks [8]. The National Institute of Standards and Technology's Special Publication 800-63B digital identity guidelines have likewise established a tiered framework that increasingly devalues traditional password authentication, classifying it at the lowest assurance level (AAL1) while requiring phishing-resistant methods for higher assurance contexts. CISA's maturity model documentation illustrates how these federal standards are influencing security practices beyond direct regulatory requirements, establishing progressive security baselines across multiple sectors [8].

4.3 Global Regulatory Trends

Beyond the EU and US, significant global developments are creating a consistent international trajectory toward passwordless requirements. Japan's amended Act on the Protection of Personal Information now includes heightened security standards for authentication systems protecting sensitive personal data. According to European Commission comparative analysis, these amended provisions establish stronger authentication as the preferred approach for protecting financial, healthcare, and biometric information [7]. Similarly, Australia's Essential Eight Maturity Model recommends phishing-resistant multi-factor authentication for critical systems, with their cybersecurity authorities providing implementation guidance that references advanced authentication technologies as solutions for achieving compliance [8].

These converging regulatory frameworks have created powerful compliance drivers that complement security considerations, with organizations increasingly finding that passwordless technologies represent the only viable path to meeting evolving regulatory requirements.

Region	Regulatory Framework	Key Authentication Requirements	Industry Impact
European Union	eIDAS 2.0 (Electronic Identification, Authentication, and Trust Services)	Mandatory interoperable digital identity wallets	Cross-border authentication standardization
	General Data Protection Regulation (GDPR)	Data minimization in authentication processes	Reduced PII exposure during verification
	EU Digital Identity Framework	Phishing-resistant authentication mechanisms	Enhanced resistance to social engineering
United States	Executive Order 14028	Multi-factor, phishing-resistant authentication	Federal agency requirements
	NIST SP 800-63B Digital Identity Guidelines	Tiered assurance levels (AAL1-AAL3)	Classification of passwords at lowest assurance level
	CISA Zero Trust Maturity Model	Progressive authentication security standards	Influence beyond direct regulatory scope
	Industry-specific regulations (implied)	Sector-specific authentication requirements	Varied implementation requirements

Japan	Act on the Protection of Personal Information (amended)	Heightened security for authentication systems	Focus on sensitive personal data protection
	Financial/healthcare/biometric data protections	Stronger authentication methods preferred	Sector-specific implementation mandates
Australia	Essential Eight Maturity Model	Phishing-resistant multi-factor authentication	Critical systems protection focus
Global (implied)	Cross-border regulatory alignment	Converging requirements for strong authentication	Multinational compliance considerations

Table 3: Global Regulatory Frameworks Driving Passwordless Authentication [7, 8]

5. Implementation Framework and Organizational Considerations

Transitioning from password-based to passwordless authentication requires systematic planning and execution. This section presents a structured framework for organizations undertaking this transformation, addressing technical, operational, and human factors.

5.1 Strategic Assessment and Planning

Successful passwordless implementation begins with comprehensive planning and stakeholder alignment. Security analysts at Segura Security emphasize that organizations must conduct thorough authentication landscape assessments before embarking on passwordless initiatives [9]. This process involves mapping user populations, documenting access patterns, evaluating risk profiles across different systems, and identifying integration requirements for all digital assets. Their implementation guide recommends risk-based implementation prioritization, where critical systems with high-value assets or significant threat exposure receive migration priority [9]. When establishing technology selection criteria, Segura advises organizations to evaluate solutions based on multiple dimensions including security efficacy, user experience impact, deployment complexity, integration capabilities with existing infrastructure, and total cost of ownership over a multi-year horizon. Their analysis suggests that organizations implementing passwordless solutions through structured assessment frameworks achieve significantly higher success rates than those pursuing ad-hoc approaches [9].

5.2 Technical Implementation Approaches

The technical execution of passwordless authentication requires careful attention to architecture and integration considerations. BankInfoSecurity's implementation guidance emphasizes that identity provider centralization represents a critical success factor, as consolidating authentication through centralized providers enables consistent passwordless implementation across diverse application environments [10]. The adoption of open standards including FIDO2/WebAuthn, OAuth 2.0, and OpenID Connect creates necessary interoperability while reducing vendor lock-in risks that might otherwise limit future flexibility. For organizations with significant legacy systems, the guidance highlights the importance of developing specific integration strategies for applications unable to directly support modern authentication protocols, potentially involving middleware layers, proxy authentication mechanisms, or phased replacement planning [10]. Particular attention must be given to secure bootstrapping protocols that address initial identity verification challenges during transition periods, as these represent potential vulnerability points if not properly designed.

5.3 Change Management and User Adoption

The human dimension of passwordless adoption often presents the most significant implementation challenges. Segura Security's research indicates that comprehensive stakeholder education represents the most influential success factor in passwordless deployments [9]. Organizations must develop communication strategies that clearly articulate the rationale for passwordless adoption, explain anticipated user benefits, and provide specific guidance tailored to different user populations with varying technical proficiency levels. BankInfoSecurity's authentication deployment documentation emphasizes the importance of phased rollout methodologies that begin with pilot groups, allowing for refinement of both technical implementation and change management approaches before organization-wide deployment [10]. Accessibility considerations must be integrated throughout the planning process to ensure that passwordless solutions accommodate users with disabilities that might impact their ability to utilize certain authentication methods, particularly biometric technologies.

5.4 Economic and Operational Considerations

The business case for passwordless authentication extends beyond security improvements to include substantial operational benefits. Segura Security's total cost of ownership analysis framework recommends comprehensive evaluation encompassing direct implementation costs, ongoing operational expenses, and projected savings from reduced password management overhead and security incident prevention [9]. BankInfoSecurity's industry analysis documents that passwordless implementations typically yield significant time savings through eliminated password resets and streamlined authentication experiences, with enterprises reporting meaningful productivity improvements across their workforce [10]. Organizations can redirect support resources previously dedicated to password management toward higher-value security initiatives, creating secondary benefits beyond direct authentication improvements.

Organizations that approach passwordless implementation through this structured framework report significantly higher success rates and user satisfaction compared to ad-hoc approaches. The most successful implementations maintain a balanced focus on security efficacy, user experience, and operational sustainability.

Implementation Phase	Key Activities	Success Factors	Challenges
Strategic Assessment	Authentication landscape assessment	Comprehensive system inventory	Incomplete visibility
	Risk-based prioritization	Focus on high-value assets	Competing priorities
Technical Implementation	Identity provider centralization	Consolidated authentication	Legacy integration
	Open standards adoption	FIDO2/WebAuthn implementation	Technical complexity
	Secure bootstrapping protocols	Strong identity verification	Transition vulnerabilities
Change Management	Stakeholder education	Clear communication	User resistance
	Phased rollout	Pilot group testing	Implementation refinement
	Accessibility considerations	Inclusive authentication options	Biometric limitations
Economic Considerations	Total cost analysis	Comprehensive evaluation	Hidden costs
	Support resource reallocation	Strategic resource utilization	Operational transition

Table 4: Passwordless Authentication Implementation Framework [9, 10]

Conclusion

The transition from password-based to passwordless authentication represents more than a mere technological evolution—it constitutes a fundamental paradigm shift in digital security with far-reaching implications. The evidence presented demonstrates that passwordless authentication offers a rare alignment of seemingly competing priorities: enhanced security, improved user experience, regulatory compliance, and operational efficiency. The security case for passwordless authentication has become unassailable as the persistent vulnerabilities of password-based systems cannot be adequately addressed through policy interventions or user education alone. Phishing resistance requires architectural changes to authentication mechanisms that eliminate shared secrets vulnerable to interception or social engineering. The technological foundations for widespread passwordless adoption have matured significantly through standardized protocols, ubiquitous biometric sensors, and digital identity wallets creating infrastructure for seamless implementation across diverse environments. Regulatory developments have transformed passwordless authentication from a security best practice to a compliance requirement in many contexts, creating powerful incentives for organizational adoption. The organizational benefits extend beyond security improvements to include substantial operational efficiencies, productivity gains, and enhanced user satisfaction, creating compelling business cases for implementation. The passwordless future has arrived, and the question facing organizations is no longer whether to implement passwordless authentication, but how quickly and effectively they can complete the transition.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Hazel Murray and David Malone, "Costs and Benefits of Authentication Advice," ACM Transactions on Privacy and Security, Volume 26, Issue 3, 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3588031

[2] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation. [Online]. Available: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[3] Joseph Bonneau and Sören Preibusch, "The Password Thicket: Technical And Market Failures In Human Authentication On The Web," The Ninth Workshop on the Economics of Information Security, 2010. [Online]. Available: https://jbonneau.com/doc/BP10-WEIS-password_thicket.pdf

[4] Microsoft Security, "Microsoft Digital Defense Report 2023," Microsoft Corporation, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[5] SecureAuth, "State of Authentication Report," SecureAuth Corporation. [Online]. Available: https://www.secureauth.com/wp-content/uploads/2024/08/State-of-Authentication-eBook.pdf

[6] AnnaMHuff et al., "Plan a phishing-resistant passwordless authentication deployment in Microsoft Entra ID," Microsoft Corporation, 2025. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication

[7] European Commission, "eIDAS Regulation,". [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[8] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," CISA, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[9] Alfredo Santos, "Passwordless Authentication: What CISOs & IT Leaders Must Know," Segura Security, 2025. [Online]. Available: https://segura.security/post/passwordless-authentication-guide

[10] Suparna Goswami, "How to Deploy Passwordless Authentication," Bankinfosecurity, 2020. [Online]. Available: https://www.bankinfosecurity.asia/how-to-deploy-passwordless-authentication-a-14458