INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume10 Issue10, October-2025, pg. 45-55

Published Date: - 31-10-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Bridging Modern Authentication: A Unified Framework for Phishing-Resistant, Usable, and Scalable Enterprise Identity

Dr. Arvind S. Mehta

Global Institute of Cybersecurity Studies, University of Lisbon

Abstract: This article presents a comprehensive, theory-driven, and practice-oriented analysis of contemporary web authentication schemes with the explicit aim of proposing an integrated framework that reconciles competing goals of security, phishing resistance, organisational usability, and enterprise scalability. Drawing strictly from the provided literature — spanning foundational cryptography, comparative evaluations of authentication schemes, empirical analyses of credential-related incidents, standards for authorization, modern second-factor mechanisms, and practical incident-cost estimations — the study synthesises prior work to form an explanatory architecture and evidence-based recommendations. The abstracted framework emphasises layered defenses combining public-key cryptography, phishing-resistant multi-factor approaches, behavioural and organisational controls that address compliance costs, and pragmatic deployment patterns guided by standards such as OAuth 2.0 and FIDO2-inspired paradigms. The core contributions are (1) a conceptual model that maps attack surfaces to mitigation families grounded in canonical cryptographic principles (Diffie & Hellman, 1976) and subsequent protocol work; (2) an expanded taxonomy of usability-security tradeoffs informed by empirical usability studies and compliance-budget literature (Brooke, 1995; Beautement et al., 2008; Ciolino et al., 2019); and (3) a decision framework for enterprises to prioritise interventions based on breach cost data and incident vectors (IBM, 2024; Verizon, 2024; Thomas et al., 2017). The article concludes with detailed operational recommendations, limitations of current approaches, and directions for future research that balance rigorous security with real-world constraints on adoption and human behaviour. The paper is intended to serve researchers, security architects, and policy makers seeking a consolidated, evidence-based route to transition modern enterprises toward phishing-resistant and scalable identity assurance. (Maximum 400 words). (Bonneau, 2012; Diffie & Hellman, 1976; IBM, 2024; Lang et al., 2016).

Keywords: Authentication, Phishing-Resistance, FIDO2, OAuth 2.0, Usability, Enterprise Security, Identity Assurance

INTRODUCTION

The last five decades of cryptographic and authentication research have produced a complex landscape of mechanisms, protocols, and real-world practices. Fundamental cryptographic breakthroughs laid the mathematical groundwork for secure key exchange and public-key systems (Diffie & Hellman, 1976), which in turn enabled the construction of protocols and mechanisms that shape current authentication strategies. Overlaid on these technical foundations are human and organisational realities: users frequently reuse passwords across sites, organisations incur compliance costs for security behaviour interventions, and adversaries increasingly succeed through social engineering, phishing, and credential theft (Das et al., 2014; Beautement et al., 2008; Thomas et al., 2017). Major industry studies also reveal the continued financial impact of breaches, underscoring the urgency of effective identity controls (IBM, 2024; Verizon, 2024). Together, these strands motivate an integrated framework that both preserves strong cryptographic guarantees and addresses real-world usability and organisational constraints.

The dominant paradigm for web authentication historically has relied on memorised secrets — passwords — combined with optional second factors. However, passwords exhibit intrinsic weaknesses in security and usability. Bonneau et al. (2012) provided a seminal framework for comparative evaluation of web authentication schemes, highlighting metrics across deployability, security, and usability that remain vital today (Bonneau et al., 2012). More recent developments, particularly the rise of phishing-resistant mechanisms such as hardware-backed security keys and FIDO2-like approaches, show promise but also surface practical concerns about enterprise-scale rollout, device management, and user experience (Lang et al., 2016; Ciolino et al., 2019).

Concurrent with advances in authentication mechanisms, standards for delegated access and authorization (for example, OAuth 2.0) have become central components of modern web architectures, enabling third-party applications and single sign-on experiences but also introducing new complexities in secure token handling and federated identity (Hardt, 2012). Taken together, the literature suggests a fragmented ecosystem: no single solution is universally optimal across security, usability, and deployability axes; instead a layered, pragmatic approach is essential (Bonneau et al., 2012; Hardt, 2012).

This article addresses three core problems exposed by the literature. First, how can enterprises move beyond password-centric models to authentication schemes that are demonstrably phishing-resistant while remaining practical to deploy across large, heterogenous workforces? Second, how can such transitions be achieved without imposing prohibitive compliance costs or degrading user productivity? Third, how should organisations prioritise investments in identity controls when breach impacts and incident vectors vary widely across industries and organisational sizes (IBM, 2024; Verizon, 2024; Chidukwani et al., 2022)? By synthesising cryptographic foundations, empirical breach analyses, usability research, and deployment studies, this article develops a coherent, evidence-backed framework that provides prescriptive guidance for practitioners and identifies research gaps for academics.

The literature gap this work targets is integrative: prior studies frequently focus on one axis — cryptographic soundness, breach economics, or usability — but rarely produce a holistic, operationally oriented synthesis that directly maps technical mechanisms to organisational decision criteria (Bonneau et al., 2012; Beautement et al., 2008; IBM, 2024). This article fills that gap by translating cross-disciplinary findings into a unified model and by elaborating the tradeoffs and contextual considerations necessary for successful enterprise adoption of phishing-resistant identity solutions.

METHODOLOGY

The research methodology deployed in this conceptual and synthesis-driven article is textual, analytical, and comparative. The approach is designed to remain strictly based on the provided references while producing a structured, evidence-driven architecture and prescriptive guidance. The methodology comprises four interlocking components: (1) theoretical grounding; (2) comparative taxonomy mapping; (3) cross-evidence synthesis; and (4) prescriptive decision heuristics.

Theoretical grounding. The analysis begins with foundational cryptographic principles, particularly those introduced by Diffie and Hellman (1976), which provide the indispensable context for understanding public-key cryptography, key exchange, and the conceptual shift away from shared secrets. This theoretical grounding informs the security properties that modern authentication schemes aim to guarantee, including confidentiality, integrity, and non-repudiation, as well as resistance to active man-in-the-middle and credential-theft attacks.

Comparative taxonomy mapping. Building upon Bonneau et al. (2012), this study constructs a detailed taxonomy that organises authentication mechanisms along axes of security (with special attention to phishing resistance), deployability (including enterprise device management and federated identity standards), and usability (measured via constructs drawn from SUS and usability literature) (Bonneau et al., 2012; Brooke, 1995). The taxonomy maps classical approaches (passwords, knowledge-based tokens), second-factor mechanisms (TOTP, SMS-based OTPs), hardware-backed cryptographic factors (security keys, FIDO U2F/FIDO2-like approaches), and federated/authorization flows (OAuth 2.0) into a coherent framework for comparative evaluation (Hardt, 2012; Lang et al., 2016).

Cross-evidence synthesis. Each element in the taxonomy is evaluated by synthesising empirical findings from breach reports and studies of credential theft (IBM, 2024; Verizon, 2024; Thomas et al., 2017), usability studies and experience sampling with second-factor devices (Ciolino et al., 2019), and organizational behavioural research that characterises compliance budgets and managerial constraints (Beautement et al., 2008). This synthesis explicitly links attack vectors to mitigation families, enabling risk-prioritised recommendations. For instance, phishing as a primary vector for credential compromise is cross-referenced against studies that tease apart the role of password reuse and social engineering, leading to concrete mitigation strategies that prioritise phishing-resistant multi-factor approaches (Thomas et al., 2017; Das et al., 2014).

Prescriptive decision heuristics. Finally, the methodology produces actionable heuristics and deployment patterns by combining breach-cost metrics (IBM, 2024) with technical and usability tradeoffs. Enterprises

Published Date: - 31-10-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

can apply these heuristics to determine which authentication investments yield the highest expected reduction in breach costs per unit of implementation burden. These heuristics are constructed as narrative decision trees and prioritisation guides rather than mathematical optimisations to respect the constraint against including equations; all reasoning about cost-benefit is presented in descriptive textual form grounded in the referenced empirical evidence.

Throughout the methodology, every major claim and inference is tied directly to one or more of the provided references, ensuring that the synthesis remains within the strict constraint of using only the supplied literature. The narrative places special emphasis on real-world deployment nuances such as device portability, loss-recovery, and the compliance budget that shapes end-user behaviour (Lang et al., 2016; Ciolino et al., 2019; Beautement et al., 2008).

RESULTS

The analytical synthesis yields several substantive results: (A) a refined taxonomy of authentication mechanisms with phishing-resistance and deployability gradations; (B) a mapping between attack vectors and mitigation families; (C) an evidence-based prioritisation matrix for enterprise investments; and (D) an integrated, operational framework that aligns cryptographic mechanisms with organisational constraints. Each result is elaborated below.

A. Refined taxonomy of authentication mechanisms. Extending the framework of Bonneau et al. (2012), the taxonomy organises authentication schemes into four macro-classes: knowledge-based secrets (passwords and passphrases), possession-based ephemeral tokens (SMS OTP, TOTP apps), cryptographic possession-based tokens (hardware security keys, device-resident keys such as those used in FIDO U2F/FIDO2), and federated/delegated credential flows (OAuth 2.0 tokens and SSO). For each macro-class, the following properties are articulated:

● Security posture with respect to phishing: Knowledge-based secrets are highly susceptible to phishing because adversaries can directly collect the secret. Possession-based ephemeral tokens provide incremental defenses but are vulnerable to interception and targeted phishing attacks that coerce real-time token entry. Cryptographic possession-based tokens, especially those that perform origin-bound authentication (as in U2F/FIDO2-like designs), show robust phishing resistance by cryptographically binding authentication to the legitimate origin. Federated flows can be secure if implemented correctly, but misconfigurations and token-handling errors can introduce risks (Bonneau et al., 2012; Lang et al., 2016; Hardt, 2012).

● Deployability constraints in enterprise contexts: Knowledge-based secrets require minimal device inventory but impose heavy support burdens due to resets and reuse, often translating to substantial helpdesk costs. Ephemeral token systems require some client provisioning and time-synchronisation management. Cryptographic tokens with hardware backing require device distribution, loss/recovery planning, and lifecycle management. Federated flows necessitate identity provider configuration and application-side integration work (Bonneau et al., 2012; Lang et al., 2016).

● Usability implications: Knowledge-based secrets are familiar but cognitively burdensome (memory demands, reuse tendencies). OTP-based approaches introduce usability friction associated with token entry and can interrupt workflows. Hardware-backed keys, while highly secure, create first-time pairing and loss scenarios that need careful UX design. Empirical usability studies highlight that device comparisons and experience sampling reveal mixed user preferences and the critical role of contextual prompts and error-handling in shaping perceived usability (Ciolino et al., 2019; Brooke, 1995).

B. Mapping attack vectors to mitigation families. By synthesising breach and incident analyses (Thomas et al., 2017; Verizon, 2024; IBM, 2024), the study develops a nuanced mapping between typical attack vectors — phishing, credential stuffing driven by password reuse, malware-based exfiltration, token interception, and insider misuse — to mitigation families:

● Phishing: Most effectively mitigated by origin-bound cryptographic authentication (hardware-backed keys that validate origin) combined with user training and protected authentication flows. Phishing-resistant MFA guidance from authoritative bodies (such as CISA guidance) supports prioritising cryptographic second factors for combating phishing (Ciolino et al., 2019; CISA, 2023).

● Credential stuffing and reuse: Countered by eliminating reusable passwords through primary reliance on cryptographic authenticators or strong federated identity, together with monitoring for credential stuffing attempts and enforcing unique credentials per principal (Das et al., 2014; Bonneau et al., 2012).

● Malware and token exfiltration: Requires device hygiene controls, attestation of device integrity when possible, and cryptographic tokens that are non-exportable or rely on user presence checks, thus reducing automated exfiltration risk (Lang et al., 2016).

● Insider misuse: Managed by combining least-privilege models, robust authorization controls (where OAuth 2.0 and correct scope-limitation play roles), and organisational monitoring that correlates behaviour against role-based expectations (Hardt, 2012; Beautement et al., 2008).

C. Evidence-based prioritisation matrix for enterprise investments. Integrating cost-of-breach metrics (IBM, 2024) with the taxonomy and attack-mitigation mapping yields a narrative prioritisation scheme. The core insight is that investments should be triaged by expected reduction in breach likelihood for the most common and costly vectors. Because phishing and credential compromise repeatedly appear as top root causes in breach analyses (IBM, 2024; Verizon, 2024; Thomas et al., 2017), the highest priority for a broad class of enterprises is moving to phishing-resistant second factors and removing passwords where feasible.

Operationally, the prioritisation matrix suggests the following high-level path:

Published Date: - 31-10-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

1. For organisations with high external exposure and sensitive data, adopt cryptographic second factors for all privileged accounts first, combined with mandatory phishing-resistant MFA for remote access. This yields high marginal benefit per deployment cost given the high prevalence and cost of phishing-related breaches (IBM, 2024; Verizon, 2024).

2. For mid-tier organisations, deploy federated identity with strong assurance at the identity provider (leveraging robust authentication at login) and apply hardware-backed authentication for high-risk roles. This balances deployability and cost.

3. Small and resource-constrained organisations should prioritise layered defences: enforce unique passwords via organisational password management tools, enable MFA that is as phishing-resistant as feasible, and monitor for credential stuffing patterns. Although such organisations face deployment hurdles, small steps guided by risk-profile still confer material protection (Chidukwani et al., 2022; IBM, 2024).

D. Integrated operational framework. The final result is an architected framework that prescribes configuration patterns and organisational controls mapped to the taxonomy and prioritisation scheme. The framework's primary features include:

● Primary reliance on origin-bound cryptographic authenticators for authentication flows where feasible (this minimises phishing surface). The rationale is grounded in the demonstrated cryptographic defence such authenticators provide against credential capture and server impostor scenarios (Lang et al., 2016; Bonneau et al., 2012).

● Use of OAuth 2.0 for delegated authorisation while enforcing minimal scopes, short token lifetimes, and strong client authentication where confidentiality and integrity of delegated tokens matter (Hardt, 2012).

● Organizational policies that recognise compliance budgets and seek to minimise user friction: deploying security keys with well-defined loss-recovery processes, staged rollouts coupled with user training, and measurement using established usability scales such as SUS to track user experience and acceptance (Brooke, 1995; Beautement et al., 2008; Ciolino et al., 2019).

● Cost-aware prioritisation: focus initial rollouts on high-impact user groups (privileged administrators, remote-access users, and roles handling sensitive datasets), then broaden coverage based on observed gains in risk reduction and usability metrics (IBM, 2024; Verizon, 2024).

DISCUSSION

The integrated framework synthesised above is informed directly by the provided literature and yields several interpretive insights, practical caveats, and a mapping of limitations and future directions.

Interpretive insights. First, the long-term replacement of passwords is not purely a technical exercise but a socio-technical transformation. While cryptographic primitives and protocols supply the technical foundation (Diffie & Hellman, 1976; Lang et al., 2016), adoption hinges on resolving manageability and user-facing friction (Bonneau et al., 2012; Ciolino et al., 2019). The compliance budget concept highlights that security mechanisms will be adopted only when administrative overhead and cognitive burdens are seen as acceptable inside daily workflows (Beautement et al., 2008). Thus, deployment strategies must simultaneously reduce helpdesk load, provide seamless recovery options, and educate users without overwhelming them — a balance that prior usability research confirms as necessary (Brooke, 1995; Ciolino et al., 2019).

Second, breach cost data from large-scale industry studies alters prioritisation calculus. High average breach costs observed across sectors mean that investments in phishing-resistant authentication can be justifiable not merely on security grounds but also as financial risk reduction measures (IBM, 2024; Verizon, 2024). For example, the marginal cost of distributing hardware-backed security keys to a subset of high-risk users may be outweighed by reductions in breach probability, particularly when those users control high-impact assets. This is consistent with the study of common incident vectors: phishing and compromised credentials frequently underpin high-cost breaches (Thomas et al., 2017; IBM, 2024).

Third, federated identity and OAuth 2.0 present both an opportunity and a risk. Delegated authorisation simplifies user experience via single sign-on but requires disciplined application integration and the enforcement of narrow scopes and robust client authentication to prevent token misuse or over-privilege (Hardt, 2012). The role of authorization hygiene — limiting token scopes and enforcing periodic re-authentication for sensitive operations — is therefore central to preserving the security benefits of identity consolidation.

Practical caveats and limitations. While the framework emphasises phishing-resistant cryptographic authenticators, real-world constraints complicate a universal pivot. Device distribution logistics, replace-and-recovery policies for lost tokens, and heterogeneity in endpoint ecosystems (mobile, desktop, BYOD) pose non-trivial operational burdens (Lang et al., 2016). Moreover, user diversity in technical fluency and cultural factors can shape acceptance, necessitating staged rollouts and iterative UX improvements (Ciolino et al., 2019; Beautement et al., 2008). Organisations must be careful to avoid naïve “rip and replace” approaches that do not account for the full lifecycle of authenticators.

Another limitation stems from the fact that phishing-resistant physical authenticators can introduce new avenues for denial-of-service and social-engineering attacks around device loss. Attackers may try to exploit recovery mechanisms, social engineering helpdesks, or weak identity verification in recovery flows. The organisation must design recovery paths that preserve security while enabling legitimate access restoration — a classic tradeoff between availability and security (Beautement et al., 2008).

Finally, the evidence base informing prioritisation — while robust — is not exhaustive of every organisational context. Industry breach reports (IBM, 2024; Verizon, 2024) and attack-cause studies provide strong guidance but must be interpreted in light of sector-specific threat models and regulatory landscapes. For example, small businesses may face differing threat mixes and resource constraints compared to large enterprises, rendering some prioritisation recommendations less applicable without adaptation (Chidukwani et al., 2022).

Future research directions. The synthesis highlights several avenues for future inquiry that build on the provided literature:

1. Longitudinal studies of large-scale deployments of phishing-resistant hardware authenticators within enterprises. While device-level security promises are well-articulated (Lang et al., 2016), long-term studies that quantify the impact on breach frequency, helpdesk volumes, and workforce productivity over multi-year horizons would be invaluable.

2. Better understanding of human factors surrounding recovery workflows. Research should examine how different recovery designs (out-of-band verification, delegated recovery via trusted devices, identity re-verification) affect security outcomes and user satisfaction, drawing from compliance budget theory (Beautement et al., 2008) and usability evaluation frameworks (Brooke, 1995).

3. Sector-specific cost-benefit analyses. Leveraging breach-cost datasets and richer telemetry about incident vectors can enable more granular prioritisation heuristics tailored to industry characteristics, regulatory pressures, and organisational scale (IBM, 2024).

4. Enhanced federated authorization patterns. Work is needed to refine OAuth 2.0 deployments and scope-limitation strategies that can be more easily validated and automated, reducing the risk of over-privileged tokens and misconfigurations (Hardt, 2012).

5. Integration of device attestation and endpoint posture signals with authentication flows. While cryptographic authenticators provide strong origin-binding, combining them with attested endpoint integrity checks could reduce the risk from compromised endpoints, an area ripe for empirical investigation (Lang et al., 2016).

Recommendations for practitioners. Based on the synthesis, the article offers several pragmatic recommendations for enterprises seeking to improve identity assurance:

- Prioritise phishing-resistant multi-factor authentication for high-risk and privileged accounts first. The combination of high breach impact for these accounts and the strong defensive properties of hardware-backed authenticators make this a high-value early investment (IBM, 2024; Lang et al., 2016).

- Use federated identity cautiously: centralise identity at a trusted provider but enforce minimal token scopes, short lifetimes, and robust client authentication to prevent token misuse (Hardt, 2012).

Published Date: - 31-10-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

● Design recovery procedures that balance security and availability: require multi-step verification, limit high-risk recovery flows, and instrument helpdesks to detect anomalous recovery requests (Beautement et al., 2008).

● Track usability and acceptance quantitatively using established instruments (e.g., SUS) and experience sampling to iteratively refine rollout strategies and training materials (Brooke, 1995; Ciolino et al., 2019).

● Adopt a risk-prioritised deployment plan that focuses first on the users and assets that contribute most to organisational exposure, then extend protections more broadly as operational processes mature (IBM, 2024; Verizon, 2024).

CONCLUSION

The convergence of cryptographic advances, empirical incident analyses, and human-centred usability research paints a clear policy-relevant conclusion: replacing or heavily augmenting password-based authentication with phishing-resistant, cryptographic, and managed identity solutions is both technically viable and financially prudent for many organisations, provided deployments are managed with attention to usability, recovery, and enterprise-scale logistics. The theoretical foundations established by Diffie and Hellman (1976) underpin the security properties of modern possession-based cryptographic authenticators, while the comparative evaluation framework of Bonneau et al. (2012) supplies the multi-dimensional lens required to assess tradeoffs. Breach-cost data and incident analyses (IBM, 2024; Verizon, 2024; Thomas et al., 2017) inform the prioritisation of investments that reduce the most common and damaging forms of compromise, notably phishing and credential misuse.

However, the transition away from passwords is not instantaneous: organisations must plan staged rollouts, robust recovery policies, and continuous usability monitoring to avoid introducing new vulnerabilities or unacceptable operational burdens. Federated and delegated authorization standards (Hardt, 2012) remain useful when applied with disciplined scope management and short-lived tokens. Finally, recognising the organisational realities emphasised by compliance-budget research (Beautement et al., 2008), any recommended security control must be designed and implemented with the explicit aim of reducing friction and long-term support costs.

This article’s primary contribution is an integrative, evidence-based framework that provides a clear pathway for organisations to migrate toward phishing-resistant, usable, and scalable authentication. It draws exclusively from the supplied literature and distils cross-disciplinary insights into practical heuristics. Future work should empirically validate the framework’s recommendations across diverse organisational contexts and refine recovery and federated patterns to further reduce adoption barriers.

REFERENCES

1. J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2012, pp. 553-567. Available: https://ieeexplore.ieee.org/document/6234436
2. IBM Security, "Cost of a Data Breach Report 2024," IBM, Jul. 2024. Available: https://www.ibm.com/reports/data-breach
3. D. Hardt, Ed., "The OAuth 2.0 Authorization Framework," IETF, RFC 6749, Oct. 2012. Available: https://tools.ietf.org/html/rfc6749
4. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976. Available: https://ieeexplore.ieee.org/document/1055638
5. K. Thomas et al., "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1421-1434. Available: https://dl.acm.org/doi/10.1145/3133956.3134067
6. Verizon, "2024 Data Breach Investigations Report," Verizon, June 2024. Available: https://www.verizon.com/business/resources/reports/dbir/
7. J. Lang, A. Czeskis, D. Balfanz, M. Schilder and S. Srinivas, "Security Keys: Practical Cryptographic Second Factors for the Modern Web," in Financial Cryptography and Data Security, Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 422-440. Available: https://doi.org/10.1007/978-3-662-54970-4_25
8. Adam Beautement, M. Angela Sasse, and Mike Wonham. "The Compliance Budget: Managing Security Behaviour in Organisations." New Security Paradigms Workshop, NSPW ’08, Lake Tahoe, California, USA, September 2008. ACM.
9. "Bridging Identity Assurance Gaps: Integrating FIDO2 and Certificate-Based Authentication for Phishing-Resistant, Scalable Enterprise Security." International Journal of Data Science and Machine Learning, 5(02), 9-24, 2025. https://doi.org/10.55640/ijdsml-05-02-02
10. Clement Bellet, Jan-Emmanuel De Neve, and George Ward. "Does Employee Happiness Have an Impact on Productivity?" Management Science, 70(3):1656–1679, May 2023.
11. John Brooke. "SUS: A Quick and Dirty Usability Scale." Usability Evaluation in Industry, 189, 1995.
12. Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus, and Recommendations." IEEE Access, 10:85701–85719, August 2022.
13. Stéphane Ciolino, Simon Parkin, and Paul Dunphy. "Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling." Symposium on Usable Privacy and Security, SOUPS ’19, pages 339–356, Santa Clara, California, USA, August 2019. USENIX.
14. European Council. "Top Cyber Threats in the EU." www.consilium.europa.eu/cyber-threats-eu, as of June 10, 2025.

Published Date: - 31-10-2025

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

15. Cybersecurity and Infrastructure Security Agency (CISA). "Implementing Phishing-Resistant MFA," 2023. www.cisa.gov/phishing-resistant-mfa, as of June 10, 2025.

16. Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. "The Tangled Web of Password Reuse." Symposium on Network and Distributed System Security, NDSS ’14, San Diego, California, USA, February 2014.