International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-06

Cybersecurity for Protecting Your Digital Life: A Review of Personal Threats, Defensive Technologies and User Awareness

Gholap Bhagwati Sudhir[1] Prof. C. A. Kolse[2] Prof. M. C. Kolse[3] Prof. S. K. Said[4]
Department of Artificial Intelligence and Data Science
Jaihind College of Engineering
Pune, Maharashtra, India

Abstract—Digital communication, online banking, shopping, education and social networking are now part of everyday life, and with this dependence comes exposure to phishing, malware, ransomware, identity theft, password attacks and unauthorized access to personal information. This paper reviews cybersecurity from the perspective of the individual user. It examines the most common threats to personal digital life and the technical and behavioural defences that counter them, including strong password management, multi-factor and passwordless authentication, encryption, firewalls, antivirus and endpoint protection, secure browsing, software updates, backups and phishing detection. Research on how attackers obtain credentials, why users fall for phishing and how experts differ from non-experts in their security habits is surveyed to explain why technology alone is insufficient. A layered personal security architecture is proposed that combines identity protection, device security, network security, data protection and user awareness under continuous monitoring. A research gap analysis, objectives, a comparison of authentication methods and a discussion of challenges are presented, with reference to the NIST Cybersecurity Framework and Indian incident-reporting guidance. The review concludes that a small set of well-chosen habits, supported by usable security tools, can greatly reduce the risk of data breaches, financial fraud and identity theft.

Index Terms—Cybersecurity, personal security, phishing, malware, ransomware, password management, multi-factor authentication, security awareness

I. Introduction

A smartphone today holds a person's bank accounts, identity documents, photographs, messages and work files. Losing control of it, or of the online accounts it connects to, can lead to financial loss, embarrassment and long recovery efforts. The Verizon Data Breach Investigations Report [1] consistently finds that the human element, through stolen credentials, phishing or errors, is involved in a majority of breaches.Cybersecurity is often discussed at the level of organizations, but individuals face many of the same threats with far fewer resources. Their defence depends on the security built into devices and services and on their own habits. Adams and Sasse [2] argued that users are not the enemy; when security fails, it is often because tools are hard to use or policies ignore real behaviour.This paper reviews cybersecurity for personal digital life, connecting research on threats and defences with practical recommendations. It proposes a layered personal security model and discusses research gaps and challenges.

II. Theoretical Background

2.1 The CIA Triad

Security aims to protect confidentiality (only authorized people see data), integrity (data is not altered without authorization) and availability (data and services are accessible when needed). Ransomware, for example, attacks availability by encrypting files, while identity theft violates confidentiality.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-06

2.2 Common Threats to Individuals

Fig. 1 classifies the most common personal threats. Phishing tricks users into revealing credentials; malware infects devices through downloads or attachments; ransomware encrypts data and demands payment; password attacks guess or reuse leaked passwords; and social engineering manipulates people through phone calls or messages.

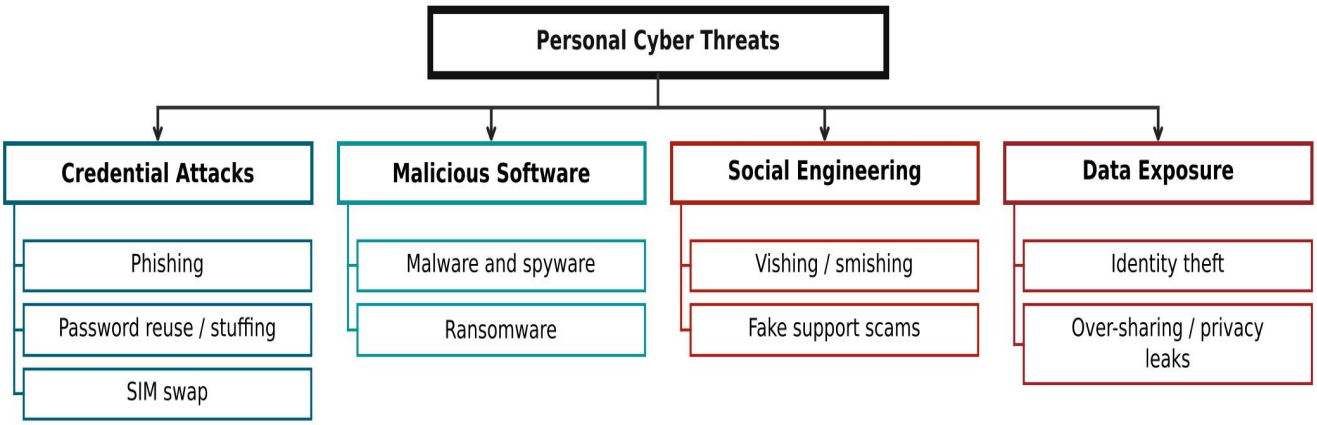


Fig. 1. Common cybersecurity threats to individuals.

2.3 Survey of Existing Approaches

Thomas *et al.* [3] studied how credentials are stolen by analysing data from breaches, phishing kits and keyloggers, and found that victims of phishing kits were far more likely to have their accounts hijacked than those exposed in third-party breaches. Their later work [4] showed that alerting users when their password appears in a known breach led many to change it, demonstrating the value of breach-alerting tools.

On password behaviour, Bonneau [5] analysed an anonymized corpus of seventy million passwords and showed that many users choose easily guessed passwords, regardless of demographic group. Bonneau *et al.* [6] compared dozens of proposals to replace passwords on usability, deployability and security and concluded that none dominated passwords on all criteria, which explains why passwords persist and must be strengthened with additional factors.

Phishing remains effective because of human factors. Dhamija *et al.* [7] found that well-designed phishing websites fooled a large fraction of participants, who often ignored browser security indicators. Kumaraguru *et al.* [8] showed that embedded training, delivered at the moment a user falls for a simulated phish, improves later recognition.

Ion *et al.* [9] compared security practices of experts and non-experts; experts emphasized software updates, unique passwords with password managers and two-factor authentication, whereas non-experts emphasized antivirus software and visiting only known websites. Kharraz *et al.* [10] analysed ransomware families and observed that many relied on simple techniques that could be detected by monitoring file-system activity.

Modern standards provide guidance. NIST SP 800-63B [11] recommends long passphrases, checking passwords against breached lists and avoiding forced periodic changes, while WebAuthn [12] enables phishing-resistant passwordless login with device-bound keys. Table I summarizes these works.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-06

TABLE I Summary of Literature Survey

Sr. No.	Ref.	Year	Methodology	Findings	Research Gap
1	[7]	2006	User study on phishing websites	Users often ignore security indicators	Laboratory setting
2	[8]	2007	Embedded phishing training	Improved recognition of later phishing	Short-term evaluation
3	[5]	2012	Analysis of 70 million passwords	Showed widespread weak password choices	Single service population
4	[6]	2012	Framework comparing password replacements	No scheme dominated passwords on all criteria	Pre-dates passkeys
5	[9]	2015	Expert vs. non-expert security practices	Experts favour updates, password managers, 2FA	Self-reported survey data
6	[10]	2015	Analysis of ransomware families	Many detectable by file-activity monitoring	Newer ransomware is more advanced
7	[3]	2017	Study of credential theft sources	Phishing kits most likely to cause hijacking	Focused on one large provider
8	[11]	2017	Digital identity guidelines	Modern password and MFA recommendations	Guidance, not enforcement
9	[4]	2019	Password breach alerting	Many users changed exposed passwords	Relies on known breach data

III. Comparative Study

Table II compares authentication methods. Passwords alone are weakest; SMS codes add protection but can be intercepted through SIM swapping; authenticator apps are stronger; and hardware keys or passkeys are resistant to phishing because the key is bound to the genuine website.

Method	Security	Phishing Resistant	Usability
Password only	Low	No	High
Password + SMS OTP	Medium	No	Medium
Password + authenticator app	High	Partly	Medium
Hardware security key	Very high	Yes	Medium
Passkey (WebAuthn)	Very high	Yes	High

TABLE II Comparison of Authentication Methods

IV. Research Gaps

The following gaps are identified:

- **G1:** Security advice for individuals is fragmented and often contradictory, leading to confusion and fatigue.
- **G2:** Awareness programmes are rarely evaluated for long-term behaviour change.
- **G3:** Adoption of password managers and multi-factor authentication remains low among non-experts.
- **G4:** Mobile-first users in India face specific threats, such as UPI and SMS fraud, that are under-studied.
- **G5:** Tools that combine multiple protections in a simple personal dashboard are scarce.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-06

4.1 Aims and Objectives

The objectives of this review are:

- **O1:** To identify the main cybersecurity threats affecting individuals' digital lives.
- **O2:** To review technical defences such as authentication, encryption, firewalls and endpoint protection.
- **O3:** To examine human factors and the role of awareness in preventing attacks.
- **O4:** To propose a layered personal security architecture.
- **O5:** To recommend practical, prioritized security practices and identify future research directions.

V. Proposed Architecture

Fig. 2 presents a layered model for protecting personal digital life, inspired by the identify, protect, detect, respond and recover functions of the NIST Cybersecurity Framework [13].

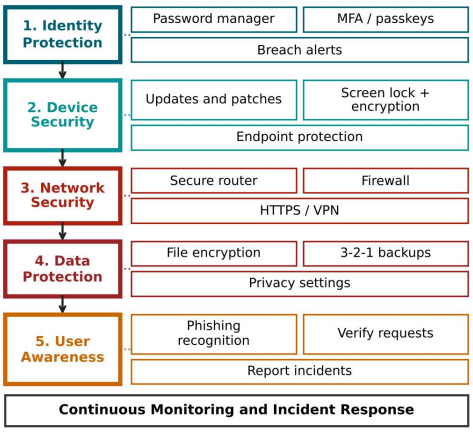


Fig. 2. Proposed layered architecture for protecting personal digital life.

5.1 Identity Protection Layer

Unique, strong passphrases are stored in a password manager. Multi-factor authentication, preferably with passkeys or authenticator apps rather than SMS, protects important accounts such as email and banking. Breach-alert services warn when credentials are exposed.

5.2 Device Security Layer

Operating systems and applications are kept up to date, screen locks and device encryption are enabled, endpoint protection detects malware, and apps are installed only from official stores.

5.3 Network Security Layer

Home routers use strong passwords and current firmware, firewalls are enabled, public Wi-Fi is used with caution, and websites are accessed over HTTPS secured by TLS [14].

International Journal of Computational Research in
Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct- 2026, PP 01-06

5.4 Data Protection Layer

Sensitive files are encrypted, regular backups follow the 3-2-1 rule (three copies, two media, one off-site), and privacy settings limit data shared with apps and social networks.

5.5 Awareness Layer

Users learn to recognize phishing, verify unexpected requests through a second channel, and report incidents. In India, incidents can be reported to CERT-In and the national cybercrime portal [15].

VI. Process Flow and Evaluation

The everyday decision process for handling a suspicious message is shown in Fig. 3. The strength of a random password can be expressed as entropy

$$H = L \cdot \log_2(N) \quad (1)$$

where L is the length and N the size of the character set. A randomly generated 16-character password from 94 printable characters has about 105 bits of entropy, while a short, human-chosen password has far less because users choose predictable patterns [5].

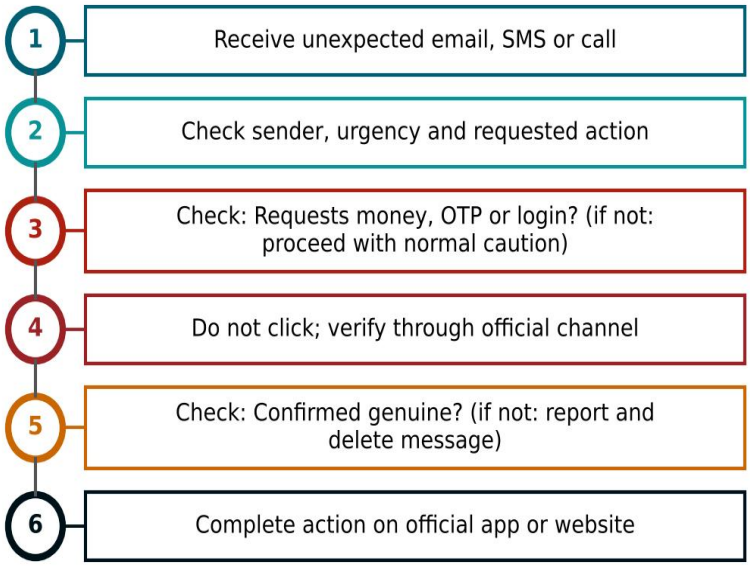


Fig. 3. Decision workflow for handling a suspicious message or link.

Risk can be assessed for each account as the product of the likelihood of compromise and its impact, so that protection effort is concentrated on high-impact accounts such as primary email, which is often used to reset all other passwords.

VII. Limitations and Future Scope

Table III summarizes challenges. Future directions include wider adoption of passkeys, AI-based scam detection integrated into messaging and payment apps, privacy-respecting personal security assistants that monitor accounts and devices, and cybersecurity education embedded in school and college curricula.

TABLE III Challenges and Mitigation

Challenge	Mitigation
Password fatigue	Password managers and passkeys
Sophisticated phishing	Phishing-resistant MFA; verification habits
Outdated devices	Automatic updates; replace unsupported devices
Ransomware	Offline backups; endpoint protection
Low awareness	Short, repeated, practical training

VIII. Conclusion

Protecting one's digital life does not require expert knowledge, but it does require consistent use of a few effective measures. The reviewed research shows that stolen credentials and phishing are the most common causes of compromise, that unique passwords with a manager and multi-factor authentication sharply reduce risk, and that updates and backups protect against malware and ransomware. Because attackers exploit human trust, awareness and usable tools are as important as technology. A layered personal security approach empowers individuals to safeguard their identity, data and online activities in an increasingly connected world.

8.1 Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

References

1. Verizon, “2024 Data Breach Investigations Report,” Verizon Business, 2024.
2. A. Adams and M. A. Sasse, “Users are not the enemy,” Commun. ACM, vol. 42, no. 12, pp. 40–46, 1999.
3. K. Thomas et al., “Data breaches, phishing, or malware? Understanding the risks of stolen credentials,” in Proc. ACM CCS, 2017, pp. 1421–1434.
4. K. Thomas et al., “Protecting accounts from credential stuffing with password breach alerting,” in Proc. 28th USENIX Security Symp., 2019, pp. 1556–1571.
5. J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Proc. IEEE Symp. Security Privacy, 2012, pp. 538–552.
6. 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,” in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567.
7. R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI), 2006, pp. 581–590.
8. P. Kumaraguru et al., “Protecting people from phishing: The design and evaluation of an embedded training email system,” in Proc. CHI, 2007, pp. 905–914.

9. I. Ion, R. Reeder, and S. Consolvo, ""...no one can hack my mind": Comparing expert and non-expert security practices," in Proc. Symp. Usable Privacy Security (SOUPS), 2015, pp. 327–346.
10. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian knot: A look under the hood of ransomware attacks," in Proc. DIMVA, 2015, pp. 3–24.
11. P. A. Grassi et al., "Digital identity guidelines: Authentication and lifecycle management," NIST Special Publication 800-63B, 2017.
12. W3C, "Web Authentication: An API for accessing public key credentials, Level 2," W3C Recommendation, Apr. 2021.
13. National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, 2024.
14. E. Rescorla, "The Transport Layer Security (TLS) protocol version 1.3," IETF RFC 8446, 2018.
15. CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000," Ministry of Electronics and IT, Government of India, Apr. 2022.