

Basics of Cyber Security in Everyday Computer Applications: A Review Focusing on E-mail Clients and Web Browsers

Mr. Vikhyath Prabhu¹, Ms. Chandana Naik², Ms. Sushma Shetty³

¹Vice-Principal, Department of Computer Application, Shree Guru Sudhindra College, Bhatkal, Karnataka

^{2,3}Educator, Department of Computer Application, Shree Guru Sudhindra College, Bhatkal, Karnataka

ABSTRACT

Everyday computer applications such as email clients and web browsers serve as primary gateways for digital communication and information access, making them high-value targets for cyber threats. This review examines fundamental cyber security practices in these applications, with emphasis on prevalent threats including phishing, malware delivery, spoofing, and drive-by downloads. Drawing on established guidance from sources such as CERT-In, CISA, and industry analyses, it outlines layered protection strategies encompassing technical controls (multi-factor authentication, email authentication protocols, safe browsing features), configuration best practices, and user awareness. The Indian context is highlighted through CERT-In recommendations relevant to individual and organizational users. The paper concludes that a combination of updated software, authentication mechanisms, cautious user behaviour, and continuous awareness forms the foundation of effective everyday cyber security.

Keywords: cyber security, phishing, email security, web browser security, multi-factor authentication, CERT-In

1. Introduction

Cyber security has become essential for individuals and organisations as daily activities increasingly rely on digital tools. Email clients and web browsers are among the most frequently used applications and remain the dominant vectors for cyber-attacks. Phishing alone accounts for a substantial proportion of successful breaches, often serving as the entry point for malware, credential theft, and further compromise (IBM, n.d.; Verizon Data Breach Investigations Report references in industry analyses). [1] In the Indian context, the Indian Computer Emergency Response Team (CERT-In) has issued practical guidelines emphasising secure email and browser usage for government entities, organisations, and citizens. These include multi-factor authentication (MFA), caution with links and attachments, browser updates, and verification of HTTPS sites. This review synthesises fundamental threats and basic protection strategies applicable to everyday use of email clients (desktop, web, and mobile) and web browsers, aiming to provide scholars, practitioners, and users with a clear overview of defensive practices.

2. Overview of Cyber security Fundamentals in Everyday Applications

Cyber security in this domain focuses on confidentiality, integrity, and availability of communications and browsing sessions. Core principles include least privilege, defence-in-depth, continuous updating, and human-centric controls. Threats exploit both technical vulnerabilities (unpatched software, weak authentication) and human factors (social engineering). Everyday applications amplify risk because they handle credentials, sensitive data, and connections to banking, e-commerce, and official services. [2]

3. Cyber security in Email Clients

Email remains the leading attack vector. More than 90% of successful cyber-attacks frequently begin with a phishing email in organisational settings, and malware delivery via email continues to rise.

3.1 Common Threats

- **Phishing and variants:** Attackers craft messages impersonating banks, government agencies, delivery services, or colleagues to induce clicks on malicious links or disclosure of credentials. Spear phishing and business email compromise (BEC) target specific individuals with contextual information. Generative tools have increased the sophistication and multilingual reach of such campaigns.[3]
- **Malicious attachments and links:** Files (documents, archives, executable) or URLs deliver malware, ransomware, or credential-harvesting pages. Techniques include HTML smuggling, password-protected archives, and delayed payload activation.
- **Spoofing and impersonation:** Display-name or domain spoofing makes messages appear legitimate. Without proper authentication, forged senders reach inboxes.
- **Account takeover:** Stolen credentials enable further attacks, data exfiltration, or lateral movement.

3.2 Basic Protection Strategies

Technical and procedural controls form a layered defence:

- Enable multi-factor authentication (MFA) or phishing-resistant methods (authenticator apps, passkeys, hardware keys) on all email accounts. MFA significantly reduces account takeover risk even if passwords are compromised.
- Implement or rely on email authentication protocols: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC). These verify sender legitimacy and help reject spoofed messages.
- Use provider-level filtering, anti-phishing detection, attachment scanning, and time-of-click URL rewriting where available (e.g., Gmail, Microsoft 365).
- Avoid clicking links or opening attachments from unexpected or urgent messages. Verify by navigating directly to the official site or contacting the purported sender through a separate channel. Hover over links to inspect actual destinations.
- Employ strong, unique passwords managed via a password manager; never reuse credentials.
- Keep email clients and operating systems updated; enable spam filtering and review forwarding rules and connected apps regularly.
- For organisational use, apply sandboxing for attachments and security awareness training with simulated phishing.

CERT-In guidance specifically advises enabling MFA, verifying sender domains and avoiding misspell-

ed addresses, not opening links/attachments from unknown or urgent sources, using strong passwords, and reporting suspicious emails to incident@cert-in.org.in.

4. Cyber security in Web Browsers

Browsers mediate access to websites and are frequently the final stage of phishing or malware delivery.[4]

4.1 Common Threats

- Malicious websites and phishing pages: Lookalike domains or compromised legitimate sites harvest credentials or deliver malware.
- Drive-by downloads and exploits: Visiting vulnerable or malicious sites can trigger silent installation of malware via browser or plugin vulnerabilities.
- Cross-site scripting (XSS) and other web attacks: Injection of malicious scripts.
- Tracking, adware, and malicious extensions: Privacy invasion or secondary compromise.
- Man-in-the-middle risks on unencrypted connections.

4.2 Basic Protection Strategies

- Prefer HTTPS sites (padlock icon or “https://” in the address bar) and avoid entering sensitive data on HTTP pages.
- Keep browsers and extensions fully updated; enable automatic updates.
- Activate built-in safe browsing features (e.g., Google Safe Browsing in Chrome/Edge, equivalent protections in Firefox/Safari) that warn about or block known malicious sites. Enhanced Safe Browsing modes offer stronger protection.
- Disable or carefully manage pop-ups, unnecessary plugins, and password-saving features on shared devices. Regularly clear cookies and cache; use private/incognito mode for sensitive sessions when appropriate.
- Expand and verify shortened URLs before clicking. Type official addresses rather than following email or message links.
- Install only trusted extensions from official stores and review permissions.
- Use browser privacy and security settings (block third-party cookies where feasible, enable warnings for site installations).
- Complement with endpoint antivirus/anti-malware that includes web protection, and consider DNS-level filtering for additional blocking of malicious domains.

CERT-In browser recommendations include updating the browser, disabling pop-ups, regular cache/cookie deletion, enabling private browsing when needed, verifying HTTPS, expanding shortened URLs, using built-in privacy settings, and disabling password remember options on public systems. [5]

5. Interconnected Practices and Cross-Cutting Strategies

Email and browser threats are tightly linked: a phishing email typically directs the user to a malicious web page. Therefore, consistent habits across both are essential—never reuse passwords, maintain software updates, apply MFA everywhere feasible, and cultivate a “pause and verify” mindset. Endpoint protection, regular backups, and reporting mechanisms (CERT-In, national cybercrime portals) complete the basic posture. Awareness training remains critical because no technical filter catches every socially engineered message.

6. Indian Perspective

CERT-In's information security practices and citizen-oriented advisories stress practical, low-cost measures suitable for diverse users: MFA (including Kavach where applicable), avoidance of unsolicited links/attachments, browser hygiene, genuine software, and timely reporting of incidents (within prescribed timelines for obligated entities). These align with global best practices while addressing local threat patterns involving banking, government services, and digital payments. [6]

7. Recommendations

1. Users and organisations should adopt a defence-in-depth approach:
2. Enable MFA and strong unique passwords on email and critical accounts.
3. Configure SPF/DKIM/DMARC where domain control exists and rely on provider protections.
4. Keep all software updated and use safe-browsing features.
5. Practise verification of senders, links, and sites; prefer direct navigation.
6. Deploy reputable antivirus and report incidents promptly.
7. Conduct periodic awareness reinforcement.

8. Conclusion

Fundamental cyber security in everyday applications rests on a combination of technical controls, secure configurations, and informed user behaviour. Phishing and related social-engineering attacks remain the predominant threat to email and browser use, yet basic measures—MFA, authentication protocols, software hygiene, HTTPS verification, and caution—substantially reduce risk. Continuous adherence to guidance from bodies such as CERT-In, alongside evolving platform protections, enables safer digital participation. Future work may examine the impact of AI-generated phishing and the effectiveness of phishing-resistant authentication in diverse Indian user populations.

References

1. Canadian Centre for Cyber Security. (n.d.). Email security best practices (ITSM.60.002) . <https://www.cyber.gc.ca/en/guidance/email-security-best-practices-itsm60002>
2. CERT-In. (n.d.). Guidelines on information security practices for government entities and related advisories/booklets. <https://www.cert-in.org.in/>
3. CISA. (n.d.). Enhanced email and web security . <https://www.cisa.gov/resources-tools/resources/enhanced-email-and-web-security>
4. IBM. (n.d.). What is phishing? <https://www.ibm.com/think/topics/phishing>
5. Kaseya. (2026). What is email security? Threats, types & how to improve it . <https://www.kaseya.com/blog/what-is-email-security/>
6. National Informatics Centre / CERT-In related materials. (Various). Cyber security do's and don'ts and browser/email best-practice guidance.
7. Additional supporting analyses drawn from industry reports on phishing prevalence, email authentication (SPF, DKIM, DMARC), and browser safe-browsing features (Google Safe Browsing and equivalents).