Science & Technology · GS - III

Examine the emerging challenges of personal and institutional cybersecurity arising from the widespread use of web-based messaging platforms. Suggest measures to strengthen cyber hygiene and protect sensitive digital communications.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 23/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Account hijacking, linked-device vulnerabilities, phishing, data privacy, cyber hygiene, multi-factor authentication, institutional security, I4C, digital literacy

Model Answer

Introduction

The increasing use of web-based messaging platforms for personal and professional communication has expanded the digital attack surface. Unsecured sessions on shared devices can expose confidential information and facilitate account misuse.

Emerging Cybersecurity Challenges

1. **Unauthorised account access:** Active sessions left unattended on public or shared computers may allow others to access private conversations and associated information.

2. **Data exposure:** Unsecured devices can expose personal information, business communications, documents and institutional data.

3. **Phishing and social engineering:** Cybercriminals use fraudulent links, impersonation and deceptive messages to obtain credentials or manipulate users.

4. **Identity misuse:** Compromised messaging accounts can be exploited to impersonate individuals, circulate fraudulent requests and target their contacts.

5. **Institutional vulnerabilities:** Employees using personal messaging accounts for official communication may inadvertently expose sensitive government or organisational information.

Measures to Strengthen Cyber Hygiene

1. **Session management:** Users should manually log out of linked devices, particularly after using public or shared computers.

2. **Strong authentication:** Multi-factor authentication, strong passwords and device-level security can reduce unauthorised access.

3. **User awareness:** Individuals should avoid suspicious links, verify unusual requests and regularly review active sessions.

4. **Institutional protocols:** Organisations should establish clear policies governing official communication, data sharing and the use of personal messaging platforms.

5. **Cybercrime reporting:** Suspicious activity should be reported promptly through appropriate cybercrime reporting mechanisms, including the National Cyber Crime Reporting Portal.

Conclusion

Cybersecurity requires both technological safeguards and responsible user behaviour. Strengthening digital literacy, secure authentication and institutional protocols is essential for protecting privacy and maintaining trust in digital communication.

BECOME IAS
AI POWERED UPSC PREP