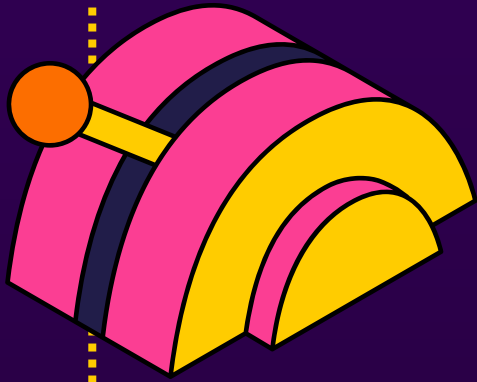




Basic Digital Safety



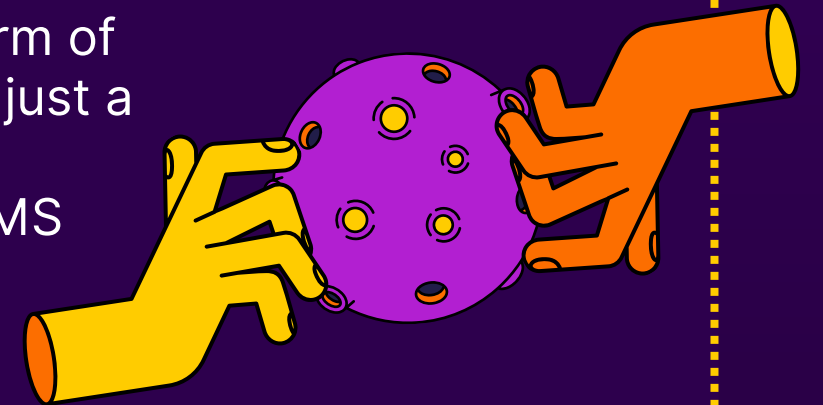
Use Strong, Unique Passwords



Avoid common passwords: Use a mix of letters, numbers, and special characters.
Use a password manager: Tools like LastPass or 1Password can help manage complex passwords.

Enable Two-Factor Authentication (2FA)

Extra layer of security:
Requires a second form of identification beyond just a password.
Common methods: SMS codes, authentication apps, or biometric verification



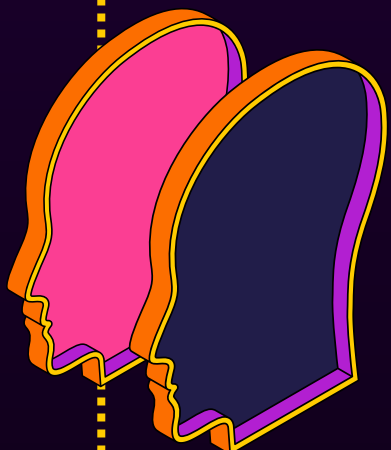
Be Wary of Phishing Scams

Suspicious emails or messages: Look out for misspelled words, unfamiliar senders, and urgent requests.
Verify links and attachments: Hover over links to see the actual URL before clicking.



Modern security software uses advanced techniques such as heuristic analysis and machine learning to detect and block threats in real-time.
Regular updates to the software and virus definitions are crucial to protect a

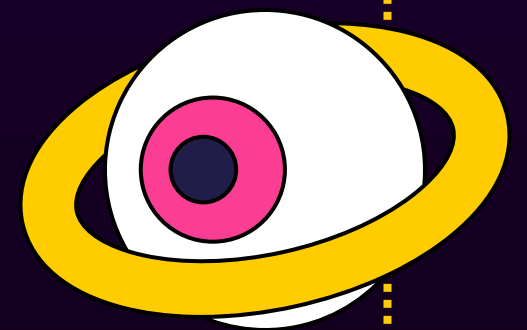
Backup Important Data



Regular backups: Use cloud services or external hard drives to back up critical information.
Test backups: Periodically check that backups are functioning correctly and data can be restored.

Install Antivirus and Anti-Malware Software

Protection against threats:
Use reputable security software to detect and remove malicious programs.
Regular scans: Schedule regular scans to ensure your device is free of threats.



Use Secure Wi-Fi Connections



Avoid public Wi-Fi for sensitive activities: Public networks can be insecure and easily exploited.
Use a VPN: Encrypts your internet connection and hides your IP address for added security.

References

National Cyber Security Centre. (2021). Password Guidance. Retrieved from [ncsc.gov.uk](https://www.ncsc.gov.uk)
Federal Trade Commission. (2022). How to Recognize and Avoid Phishing Scams. Retrieved from [ftc.gov](https://www.ftc.gov)

