

d. User Awareness Campaigns: Social networks should engage in campaigns that raise awareness about secure practices, such as creating strong passwords, recognizing phishing attacks, and avoiding suspicious links.

Stronger Regulation and Enforcement: Governments and regulatory bodies should enforce data privacy laws (e.g., GDPR) and work with social networks to ensure proper security measures are in place to protect user data and privacy.

Better Detection of Fake Accounts and Bots: Social networks should implement systems to detect fake accounts and bots, which can be used for malicious purposes such as spreading malware or misinformation.

Regular Software Updates: Social networks should ensure their platforms are up to date with the latest security patches and fixes to mitigate vulnerabilities.

What Can Be Done to Protect Social Networks?