Cyber Security Awareness Tips - July 2025

Do's 👍	Don'ts 👎
Verify the source of QR codes, emails, messages or calls before doing any activity / task.	Don't scan QR codes from unknown sources, emails, or public places without verification.
Use strong, unique passwords for banking apps and accounts and change them regularly.	Don't click on links or attachments in unsolicited emails, popups, or messages.
Enable two-factor authentication (2FA) for all digital services / Apps.	Don't share passwords, PINs, card details or personal info with anyone, even if they claim urgency.
Download banking apps only from official app stores	Don't use public Wi-Fi for banking; use mobile data or a VPN instead.
Keep your endpoints, phones, apps and antivirus software updated to fix security issues.	Don't store sensitive info like passwords or account details on your phone or unsecured devices.
Monitor your bank accounts regularly for unusual activity.	Don't believe threats of "digital arrest" or demands for money over calls or video.
Use secure websites (https) and trusted Wi-Fi or mobile data for banking.	Don't reuse the same password across multiple sites or apps.
Report suspicious calls, emails, or scams to your bank or cybercrime helplines (e.g. 1930 or https://cybercrime.gov.in in India).	Don't respond to urgent requests for money or account details without verifying independently.
Hover over links or preview QR code URLs to ensure they're legitimate before clicking.	Don't download apps or files prompted by QR codes or messages unless the source is trusted or verified.
Stay informed about common scams through official government or bank websites.	Don't ignore security warnings or delay updating your device's software or apps.