Cyber Jaagrookta Diwas November 2023: "Use separate email for social media so that main email account is protected from any spam and phishing."

Enable Multi-Factor Authentication.
Always secure all your accounts with two-factor authentication, especially while doing any online financial transaction.

Use Strong Passwords.
A Strong password should always include upper and lowercase letters, numbers, and at least one special character.

Recognise and Report Phishing/Smishing/Vishing.
Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web. Vishing is an attempt where fraudsters try to seek personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

Do not fall into any financial fraud trap.
Never disclose net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. Avoid using public Wi-Fi for conducting financial transactions.

Update your Software.
Update your Software periodically. Install antivirus software, firewalls, and email filters and keep them updated.

Be cyber security aware on Social Media.
Select the right privacy settings on social media platforms and make sure that you are sharing your information, photos and videos with your trusted ones only.