CYBER SECURITY AWARENESS MONTH – OCTOBER

Stay Alert. Stay Secure. Stay Cyber-Safe.

October is observed as **Cyber Security Awareness Month** nationwide to promote safe and secure cyber practices with the increasing use of digital technologies for communication, banking, payments, and other online services, it is essential to remain vigilant and follow good cyber hygiene practices.

To strengthen our collective cyber security and protect ourselves against online fraud, data theft, and emerging cyber threats, all are encouraged to follow the below guidelines.

1. Password and Account Security

- Create strong passwords using a combination of uppercase and lowercase letters, numbers, and special characters.
- Use unique passwords for different accounts and avoid reusing passwords.
- Avoid saving passwords on shared devices or unsecured platforms. Use a trusted password manager where appropriate.
- Enable Multi-Factor Authentication (MFA) wherever available, particularly for sensitive accounts.
- Never share your password, One-Time Password (OTP), PIN, or Card Verification Value (CVV) with anyone, including individuals claiming to be bank employees.

2. Safe Internet Browsing and Device Security

- Always verify the authenticity of websites and prefer secure connections using HTTPS.
- Install trusted antivirus and endpoint security software, wherever applicable, and keep it updated.
- Regularly update operating systems, applications, browsers, and security software.
- Download and install applications only from official platforms, such as the Google Play Store and Apple App Store.
- Avoid accessing banking services or performing sensitive transactions over unsecured public Wi-Fi networks.

3. Email, SMS and Phishing Awareness

- Never click on suspicious links received through emails, SMS messages, or messaging applications.
- Do not open unexpected attachments or download files from unknown senders.
- Be cautious of messages requesting urgent action, confidential information, or immediate payments.
- Never click on links asking you to update bank account details, complete KYC, or verify personal information.
- Verify suspicious communications through official websites, applications, or customer support channels before taking action.

4. Banking and Digital Payment Security

- Enable transaction alerts and monitor bank account activity regularly.
- Use trusted payment applications and secure payment methods for digital transactions.
- Always verify the recipient's details and the transaction amount before authorizing a payment.
- Never disclose your UPI PIN, OTP, card PIN, CVV, or other banking credentials.
- Remember that a UPI PIN is required to authorize a payment, not to receive money.
- Consider using a secondary bank account with limited funds for routine UPI transactions, wherever appropriate.
- Never install screen-sharing or remote-access applications at the request of unknown callers claiming to assist with banking issues.

5. KYC, Aadhaar and Personal Information Protection

- Share a masked Aadhaar wherever accepted and appropriate for KYC purposes.
- Never share Aadhaar details, PAN details, banking information, or identity documents with unverified individuals.
- Do not respond to unsolicited calls, emails, or messages requesting personal or financial information.
- Verify KYC-related requests directly through the bank's official website, application, branch, or customer care channel.
- Remember that legitimate service providers will never ask you to disclose confidential credentials such as OTPs, PINs, or passwords.

6. Social media and Privacy Protection

- Avoid posting personal details, financial information, identity documents, travel plans, or other sensitive information on social media.
- Review privacy settings on social media accounts regularly.
- Accept friend requests and messages only from verified or familiar individuals.
- Do not share confidential workplace information, internal documents, or sensitive business data on public platforms.
- Be cautious of fake profiles, fraudulent job offers, investment schemes, and impersonation attempts.

7. AI-Generated Scams and Impersonation Fraud

- Be alert to AI-generated voices, manipulated videos, deepfakes, and fabricated messages used to impersonate colleagues, senior officials, family members, or trusted organizations.
- Independently verify unusual requests for money, confidential information, or urgent action, even when they appear to come from a familiar person.
- Use a known and trusted contact number to verify the identity of the caller.
- Avoid responding to suspicious video calls from unknown numbers.
- Exercise caution with unexpected international calls and unfamiliar country codes. Do not call back suspicious numbers or share personal information.

8. Mobile and UPI Safety

- Keep your mobile device locked using a strong PIN, password, or biometric authentication.
- Do not install applications through links received from unknown sources or unofficial websites.
- Never share your screen, provide remote access, or disclose confidential information to unknown callers.
- Do not scan unknown QR codes or approve unexpected UPI payment requests.
- Never enter your UPI PIN to receive money or claim a refund.
- Report a lost or stolen mobile device promptly, particularly if it is linked to banking or payment applications.

9. Incident Reporting and Response

- Report suspected cyber fraud, phishing emails, suspicious links, unauthorized transactions, and other cyber incidents immediately through the appropriate official channels.
- In case of suspected financial cyber fraud in India, call the National Cyber Crime Helpline at 1930 as soon as possible.
- Lodge a complaint through the official National Cyber Crime Reporting Portal: **https://cybercrime.gov.in**
- Inform your bank immediately if you notice unauthorized transactions or suspect that your banking credentials have been compromised.
- Preserve relevant evidence, such as screenshots, transaction references, phone numbers, messages, and emails, for investigation.
- Do not delay reporting an incident, even if the financial loss appears small or no loss has occurred.

10. General Cyber Security Best Practices

- Stay informed about emerging cyber threats, fraud techniques, and security advisories.
- Think before clicking, sharing information, downloading files, or approving transactions.
- Verify the authenticity of unusual requests through trusted channels.
- Follow your organization's information security policies and report suspected security incidents promptly.
- Remember that cyber security is everyone's responsibility, both at the workplace and in personal life.

Let Us Build a Safer Digital Environment

Cyber security begins with awareness and is strengthened through responsible digital behaviour. By following these practices, we can help protect our information, financial assets, and digital identities against evolving cyber threats.

Stay Alert. Think Before You Click. Protect Your Information. Report Cybercrime Promptly.

LIC Pension Fund Ltd (Cyber Security Department)