THE KARAD URBAN CO-OPERATIVE BANK LTD., KARAD
(Scheduled Bank)

CYBERSECURITY AWARENESS- GUIDELINES

STAY ALERT 2026

Protect Your Money, Shield Your Identity

Digital banking provides ultimate convenience, but cybercriminals deploy sophisticated social engineering tactics to manipulate human emotions. Treat this guide as your defensive shield against rising automated and AI-driven frauds.

THE DO'S

√ **Verify UPI Beneficiary Identity**
Always double-check the recipient's name and payment amount on your screen before typing your UPI PIN.

√ **Download Apps from Official Sources**
Only install banking applications directly via the official Google Play Store or Apple App Store. Check developer verification.

√ **Enforce Device Locks & MFA**
Secure your smartphone with biometrics or strong PINs. Activate Multi-Factor Authentication (MFA) across your accounts.

√ **Validate URLs and Site Security**
Ensure the website address starts explicitly with **https://** and look for the secure lock icon before logging into net-banking.

√ **Report Irregular Account Activity**
Monitor your transaction SMS and statements closely. Inform the bank immediately upon noticing any unrecognized transaction / change.

THE DON'TS

× **Never Disclose Sensitive Credentials**
Do not share your OTP, CVV, Password, or PIN with anyone—including individuals claiming to be bank officers.

× **Never Interact with Unverified Links**
Do not tap links or open unexpected attachments embedded in SMS, emails, messages, posts from unknown numbers / sources.

× **Never Execute Transactions on Public Wi-Fi**
Avoid financial transactions or making online purchases while connected to open, public, or unencrypted Wi-Fi hotspots.

× **Never Fall for "Digital Arrest" Threats**
Law enforcement or CBI will never "digitally arrest" you over WhatsApp or Video Call. Do not send money to anyone out of fear.

× **Never Authorize Inflated UPI Requests**
Do not approve random collect requests or incoming payment links on Google Pay, PhonePe, or Paytm to "receive prize money."

THE KARAD URBAN CO-OPERATIVE BANK LTD., KARAD
(Scheduled Bank)

CYBERSECURITY AWARENESS - GUIDELINES

STAY ALERT 2026

Protect Your Money, Shield Your Identity

EMERGING CYBER THREATS & MODUS OPERANDI

THREAT TYPOLOGY	HOW IT OPERATES	CRITICAL SAFEGUARD
AI-Powered Deepfakes HIGH	Scammers use artificial intelligence to replicate the exact voice or video of bank executives, family members, or corporate vendors requesting emergency fund transfers.	Establish a secondary, offline verification channel. Never trust voice/video requests involving immediate financial distress without independent confirmation.
"Digital Arrest" Scams CRITICAL	Fraudsters impersonate police, CBI, or telecom authorities via video calls. Ex. They claim illegal contraband was found in your parcels and threaten immediate jail unless money is sent.	**Real police never conduct legal processes via video call.** Hang up instantly. Do not share personal details or do not send money on fraudster demand.
QR Code & Quishing MEDIUM	Attackers manipulate physical posters, bills, or send digital emails containing malicious QR codes that bypass automated spam filters.	Scanning a QR code is exclusively for **sending money**, never for receiving funds or verifying your KYC profile.
Search Engine Ad Mimicry MEDIUM	Cybercriminals purchase sponsored search ads on Google/Bing that look identical to official bank portals, routing users to credential-stealing fake login screens.	Type the official website domain directly into your browser address bar. Avoid clicking on search entries marked as "Sponsored" or "Ad".

ESSENTIAL SMART-BANKING MICRO-TIPS

1. Set Transaction Limits

Utilize your mobile banking application to set daily transactional caps/limits and disable international card usage unless actively traveling abroad.

2. The 10-Minute Rule

If a call or message creates a sense of urgency, fear, or panic, pause before responding. Wait at least 10 minutes and verify the situation with a trusted friend or family member.

3. Delete Saved Details

Periodically clear autofill passwords and saved credit/debit card data from your browsers and generic merchant apps.

Have you been defrauded? Act within Golden Hour (in 1 hour).
Dial 1930 or register at cybercrime.gov.in
File refund requests at mrm-ncrp.mha.gov.in