తెలంగాణ గ్రామీణ బ్యాంక్

TELANGANA GRAMEENA BANK

Scheduled Bank Owned by Government

CYBER CRIME PREVENTION

ESSENTIAL HANDBOOK

CYBER SECURITY

Our Hands on JOB

DO'S

DONT'S

తెలంగాణ గ్రామీణ బ్యాంక్
TELANGANA GRAMEENA BANK
Scheduled Bank Owned by Government

Foreword

Esteemed Colleagues,

Computer Security Day—— Reinforcing Our Digital Safety Culture

Computer Security Day provides an opportunity for all of us to reflect on the importance of protecting the digital infrastructure that supports our work. As cyber threats grow more sophisticated each year, staying cautious and well-informed has become a necessity for everyone.

Many of our rural customers are now beginning to use digital banking channels, and while this opens new possibilities for convenience, it also exposes them to risks they may not fully understand. Fraudsters continue to adapt their techniques, especially with advancements in financial technology, making vulnerable users easy targets. Any cyber incident involving customer accounts can weaken the trust and confidence they place in our Bank.

It is therefore essential that we help our customers recognize the dangers of phishing, AI-based scams, and other online threats. At the same time, we must ensure that our systems and processes are strong enough to prevent fraudulent activities.

As we observe Computer Security Day, let us reaffirm our dedication to:

- **Encourage customers to practice good cybersecurity habits**, such as creating strong passwords, browsing safely, and keeping their devices updated.
- **Educate customers** not only to use digital banking services confidently but also to maintain strong, confidential passwords and safeguard their login information.
- **Keep customers informed about the latest scams**, particularly those that appear genuine and could easily mislead them.
- **Maintain strong communication and trust with customers** so they feel comfortable contacting the bank at the first sign of potential fraud.
- **Explain the benefits of the bank's fraud-detection and risk-management systems**, which are designed to identify and prevent abnormal or suspicious transactions.
- **Share real-life examples of fraud incidents** (without disclosing personal information) to help customers understand how scams typically occur.
- **Promote the bank's official communication channels** so customers can distinguish legitimate messages from fraudulent ones.

By taking these steps proactively, we can reduce risks before they escalate. Through this booklet, we put forth to you the various scams, frauds and do's / don'ts of computer security. We request you to please arrange to go through them.

Let us continue to safeguard our systems and uphold the trust our customers place in us.

Regards,
K. Prathapa Reddy,
CHAIRMAN

తెలంగాణ గ్రామీణ బ్యాంక్
TELANGANA GRAMEENA BANK
Scheduled Bank Owned by Government

Foreword

Dear Colleagues,

Computer Security Day — Protecting Our Customers, Strengthening Trust

In today's digital world, keeping information safe is more important than ever. Computer Security Day reminds us of our responsibility—not just to protect our systems, networks, and data— but also to ensure our customers navigate the digital banking landscape safely and confidently.

On this special day, we are sharing a **booklet of practical dos and don'ts**, highlighting the latest types of fraud and how cybercriminals operate. This resource is designed to help you understand these threats and take proactive steps to prevent them. We encourage every colleague to use this knowledge to **educate and support our customers**, especially those who are new to digital banking.

Ways bankers can make a real difference:

- Demonstrate safe digital habits: Show customers how to create strong passwords, enable two-factor authentication, and identify genuine bank communications.
- Offer personal guidance: When onboarding customers to mobile banking, UPI, or other digital services, take time to explain the do's and don'ts clearly.
- Reassure and protect: Remind customers that bank staff will never ask for OTPs, PINs, passwords, or other confidential details.
- Support those who need extra help: Give special attention to elderly or digitally inexperienced customers, guiding them patiently step by step.

By combining vigilance with empathy, we can make computer security a natural habit—not just a requirement

Every effort we take helps our customers feel secure, strengthens their trust in us!

Regards,
S.Sankara Rao,
General Manager-I

Foreword

Dear Team mates,

Computer Security Day: Strengthening Our Digital Defense:

As our lives and work move online, keeping digital systems secure is more important than ever. Protecting information is no longer optional—it's a responsibility.

Our Bank's vision is to empower rural customers, and that includes safeguarding them from various forms of fraud. Did you know financial institutions face cyberattacks every single day? Even the most knowledgeable customers can fall victim because cybercriminals are clever, the timing is perfect, and sometimes, a small gap in digital awareness is enough to succeed. This booklet is here to help. Its mission is simple: raise awareness about common scams and provide practical tips—the dos and don'ts—that help protect you, our customers, and the Bank.

Computer Security Day is about more than technology—it's about mindful digital habits. Every small action you take contributes to a safer online world. Stay alert, stay curious, and commit to at least one step today that strengthens your digital security.

Protect the Bank and our customers—every action counts.

Regards,

G.Sreedhar Reddy,
Assistant General Manager(IT)

తెలంగాణ గ్రామీణ బ్యాంక్
TELANGANA GRAMEENA BANK
Scheduled Bank Owned by Government

REPORT CYBERCRIMES ON

www.cybercrime.gov.in

Or

1930

KEEP YOURSELF UPDATED WITH LATEST CYBERCRIMES

INDEX

1. KYC Scam

Fraudsters pretend to be bank/financial institution officials and claim that the customer's KYC is expired. Their aim is to steal personal info, documents, or access to bank accounts.

How it Happens

- Fake SMS/calls/emails urging immediate KYC update.
- Customer is asked to click a link, share documents, OTP or install apps.
- Victim unknowingly shares confidential data, leading to account takeover.

✓ Do's	✗ Don'ts
• Verify KYC requests directly with the bank. • Use official bank websites/contact numbers. • Report suspicious activity immediately.	• Don't share OTP, PIN, login details, or documents with anyone. • Don't click unverified links for KYC updates.

2. Online Job Scam

Scammers post fake job openings offering high income with easy work. Their goal is to steal your personal details or collect money in the name of fees.

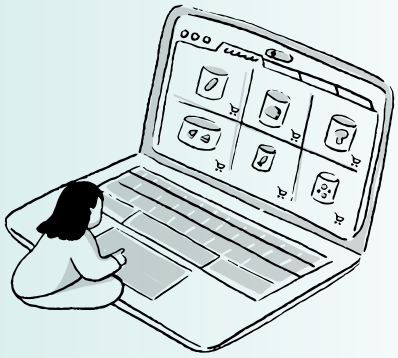
How it Happens

- Fake job ads on social media.
- Victims asked to pay registration, verification or training fees.
- Fake interview calls from prank HR emails.

✓ Do's	✗ Don'ts
• Apply only through trusted job portals. • Verify company credentials. • Ask questions during interviews.	• Don't pay any fee without verification. • Don't trust unsolicited job messages.

3. Online Shopping Fraud

Fraudsters create fake e-commerce websites or mislead customers on C2C platforms like OLX, Quikr.



How it Happens

- Attractive discounts or offers too good to be true.
- Asking for advance payment.
- Sharing fake tracking links.

✓ Do's	✗ Don'ts
• Buy from trusted/verified sellers. • Use Cash-on-Delivery for suspicious sites. • Compare prices across platforms.	• Don't scan QR codes to "receive money". • Don't save card details on unknown websites.

4. Digital Arrest Scam

Criminals impersonate police/CBI officials via video calls and threaten victims to pay money, claiming involvement in crimes.

How it Happens

- Fake officers accuse you of illegal activity.
- Threaten “digital arrest” and demand payment.

✓ Do’s	✕ Don’ts
• Stay calm; no government agency does video-call interrogations. • Report such calls on cybercrime.gov.in.	• Don’t send money to anyone claiming to be from police agencies. • Don’t stay on long suspicious video calls.

5. Investment Scam

Trickers promise high returns with zero risk to steal money.

How it Happens

- Fake trading groups on WhatsApp/Telegram.
- Fraud apps showing fake profits.
- Asking victims to invest small initially, then more.

✓ Do’s	✕ Don’ts
• Invest only through SEBI-registered entities. • Verify all schemes and apps.	• Don’t trust unbelievable returns. • Don’t join trading groups on social media.

6. Online Gaming Fraud

Fraudsters use gaming apps to steal data, money, or trick players.

How it Happens

- Fake gaming apps asking for permissions.
- Scammers befriending players and extracting data.
- Real-money apps promising guaranteed returns.

✓ Do’s	✕ Don’ts
• Supervise children’s gaming. • Download only verified games.	• Don’t share personal details with players. • Don’t install apps from unknown links.

7. Lottery Fraud

Victim receives fake messages stating they won a lottery.

How it Happens

- Fraudster demands “processing fee”, “tax”, “custom charges”.
- After payment, they disappear.

✓ Do’s	✕ Don’ts
• Be suspicious of unexpected prize messages.	• Don’t pay any fee to claim lotteries. • Don’t share personal/bank details.

8. Phishing (Fake Links/Emails)

Scammers send emails/SMS with fraudulent links that steal login details.

How it Happens

- Clicking the link leads to a fake website.
- Victim enters credentials & loses money.

✓ Do’s	✕ Don’ts
• Hover over links to check URL. • Keep software updated.	• Don’t click unknown links. • Don’t trust unexpected emails.

9. Spam/Vishing (Fraud Calls)

Scammers call pretending to be from banks, telecom, police, etc.

How it Happens

- Caller creates urgency to trick customers into revealing information.

✓ Do’s	✕ Don’ts
• Use call-blockers. • Educate family members	• Don’t share OTP or banking details. • Don’t return unknown missed calls.

10. Quishing (QR Code Scam)

Scanning fake QR codes leads to fraud transactions or phishing websites.

How it Happens

- QR codes placed on posters, social media, messages.
- Victim scans to “receive money”.

✓ Do’s	✕ Don’ts
• Scan only official QR codes.	• Never scan codes to receive money.

11. Search Engine Fraud

Fraudsters create fake customer care numbers appearing in Google search.

How it Happens

- Victim searches “XYZ bank customer care”.
- Calls fake number and shares details.

✓ Do’s	✕ Don’ts
• Check official websites only.	• Never trust numbers shown on Google search results.

12. Social Media Impersonation

Fake accounts created to trick victims into sending money or data.

How it Happens

- Fake profiles of relatives, friends, or celebrities.
- Asking for urgent money help.

✓ Do’s	✕ Don’ts
• Verify accounts with real person.	• Don’t make payments to unknown accounts.

13. SMS/Email/Call Scams (Loan Fraud)

Fake loan offers from fraudsters using NBFC/bank logos.

How it Happens

- Offering instant loan with low interest.
- Asking for upfront fee.

✓ Do's	✕ Don'ts
• Verify with official NBFC/bank.	• Don't pay any upfront charges.

14. Debit/Credit Card Fraud

Fraudsters misuse stolen card details or skim card info.

How it Happens

- Fake POS machine.
- Card skimming.
- Phishing messages asking for OTP.

✓ Do's	✕ Don'ts
• Cover keypad when entering PIN. • Turn off unused features	• Don't share card details. • Don't ignore suspicious alerts.

15. APK Fraud (Fake Mobile Banking Apps)

Fraudsters create apps that look like bank apps and steal login details.

How it Happens

- Customers download app from a link.
- App captures user credentials.

✓ Do's	✕ Don'ts
• Download only from official app stores.	• Don't install apps from links. • Don't jailbreak/root phone.

16. Cyber Slavery

People are trapped into forced digital labour via fake foreign job offers.

How it Happens

- Fake job abroad.
- Victims trafficked into illegal digital work.

✓ Do's	✗ Don'ts
• Check job offers thoroughly.	• Don't work abroad on tourist visa.

17. SIM Swapping

Fraudster gets a duplicate SIM for victim's number & intercepts OTPs.

How it Happens

- Pretends to be telecom staff.
- Uses stolen details to issue new SIM.

✓ Do's	✗ Don'ts
• Enable 2FA (two-factor authentication). • Monitor network issues.	• Don't share identity documents.

18. Money Mule Fraud

Scammers use individuals to move stolen money.

How it Happens

- Offering commission to receive and transfer funds.
- Victim becomes part of illegal activity.

✓ Do's	✗ Don'ts
• Report suspicious money requests.	• Don't let others use your bank account.

19. Juice Jacking

Malicious USB charging ports steal data or inject malware.

How it Happens

- Public charging stations with tampered USB ports.

✓ Do's	✕ Don'ts
• Use your own charger. • Prefer AC sockets.	• Don't use unknown USB ports.

20. Deepfake Cybercrime

AI-generated fake videos/audio used for blackmail, misinformation.

How it Happens

- Manipulated videos showing victims or officials.

✓ Do's	✕ Don'ts
• Verify before believing or sharing.	• Don't trust sensational content blindly.

21. Remote Access Fraud

Scammers trick victims into installing screen-sharing apps.

How it Happens

- Fake customer support asking: "Install AnyDesk/TeamViewer".

✓ Do's	✕ Don'ts
• Verify caller identity. • Uninstall screen-sharing apps after use.	• Don't give remote access to anyone (unknown persons) .

22. Secure Browsing

Staying safe while browsing online.

How it Happens

- Attackers use phishing or malicious websites to trick you into revealing personal information or downloading malware.

✓ Do's	✗ Don'ts
• Use HTTPS websites. • Install antivirus.	• Don't use public Wi-Fi for banking.

23. Ransomware

Malware encrypts your files and demands ransom.

How it Happens

- It spreads through downloading cracked software, free movies, pirated applications, or files from untrusted websites.
- Malware downloads automatically when victims visit infected or compromised websites.

✓ Do's	✗ Don'ts
• Regularly backup data. • Keep software updated.	• Don't pay ransom.

24. Smartphone Scams

Fraudsters misuse stolen phones, fake apps, SIM misuse.

How it Happens

- Smartphone scams happen when customers install fake apps or click suspicious links that steal data, OTPs, or banking information.
- Fraudsters also misuse stolen phones, duplicate SIMs, and fake customer-care calls to gain access to accounts.

✓ Do's	✗ Don'ts
• Report lost phones. • Check SIM count on Sanchar Saathi.	• Don't download apps from unknown sources.

తెలంగాణ గ్రామీణ బ్యాంక్
TELANGANA GRAMEENA BANK
Scheduled Bank Owned by Government

10 Common Tricks Used by Scammers- Be Aware. Be Alert. Be Safe.

1. **TRAI Phone Scam**
Scammers call pretending to be from TRAI and threaten to block your mobile number due to illegal activity or incomplete KYC.
Reality: TRAI never suspends mobile services—only telecom companies can.

2. **Parcel Stuck at Customs**
You receive a call saying a parcel in your name contains illegal goods and you must pay a fine.
Action: Hang up immediately and report the number.

3. **Digital Arrest**
Fraudsters pose as police officers and claim you are involved in a crime. They threaten online interrogation.
Reality: Police never perform "digital arrests" or conduct interrogations online.

4. **Family Member Arrested**
Scammers claim your relative has been arrested and demand money for their release.
Action: Contact your family directly and confirm before taking any action.

5. **Get-Rich-Quick Trading**
Social media ads promise high returns on investments or stock trading.
Reality: Any scheme offering unusually high returns is most likely a scam.

6. **Easy Online Tasks / Jobs for High Rewards**
Scammers promise large payments for simple tasks and later ask for a security deposit or investment.
Reality: Easy money schemes are always scams.

7. **Lottery in Your Name**
You receive an SMS or email claiming you've won a lottery and must share your bank details or pay a fee.
Action: Ignore and delete such messages immediately.

8. **Mistaken Money Transfer**
Scammers say money was accidentally deposited into your account and ask you to return it.
Action: Always verify with your bank before taking any step.

9. **KYC Expired**
Calls or messages ask you to update KYC using a link or phone number.
Reality: Banks never call or send links for KYC updates.

10. **Fake Tax Refund**
Fraudsters pretend to be from the tax department, claiming you are eligible for a refund and requesting your bank details.
Reality: Tax authorities already have your bank information and contact you through official channels only.

Fight Against Cyber Crimes ~ Stay Alert. Stay Safe.

తెలంగాణ గ్రామీణ బ్యాంక్

TELANGANA GRAMEENA BANK

Scheduled Bank Owned by Government

COMPUTER SECURITY DAY

NOVEMBER 30

CYBER SAFETY BEGINS WITH YOU!