

ADDITIONAL RISK MEASURES & DOS AND DON'TS

1. Beware of Fake Loan Approval Emails / Messages

If customer receive an email, SMS, WhatsApp message or any other communication claiming to be from OXYZO Financial Services Limited (“OXYZO”) regarding loan approval and asking you to pay processing fees, insurance charges, security deposits or any other amount, **do not make any payment without verifying its authenticity.**

Customers may forward such suspicious communications to getsupport@oxyzo.in or call +917353013499 for verification.

2. Do Not Pay Cash

OXYZO does not collect cash towards processing fees, insurance charges or other loan-related charges. Customers are advised not to make any cash payment to any employee, agent, intermediary or third party claiming to represent the Company.

Customers are requested to always make payments only through **official and authorized payment channels** communicated by the Company.

3. Unauthorized Transactions – Customer Liability

Customers should immediately report any suspected unauthorized transaction to OXYZO by emailing at getsupport@oxyzo.in or call +917353013499.

4. Report Cyber Fraud Immediately – Call at 1930

If Customer suspect that he/she has become a victim of a cyber scam or unauthorized financial transaction, he/she should immediately **call the National Cyber Crime Helpline at 1930** and report the incident through the official Government cyber-crime reporting mechanism.

The Customer should immediately inform to OXYZO by writing to getsupport@oxyzo.in.

DOS – WHAT CUSTOMERS SHOULD DO

1. Read All Loan Documents Carefully

Before signing the **sanction letter, loan agreement or any other loan-related document**, customers are requested to carefully read and understand:

- Loan amount and disbursement terms
- Interest rate and applicable charges
- Processing fees and other charges
- Repayment schedule
- Penal charges, if applicable
- Security / collateral requirements
- Prepayment / foreclosure terms
- Other terms and conditions

Customers are advised not to sign any document unless they have fully read and understood its contents. In case of any doubt or requiring clarification, customers should contact OXYZO through its official communication channels at getsupport@oxyzo.in or call +917353013499 before signing.

2. Use Strong and Unique Passwords

Customers are advised to use strong and unique passwords for your online accounts.

- Avoid using easily identifiable information such as your name, date of birth or mobile number.
- Use different passwords for different websites and applications.
- Consider using a reputable password manager to securely manage your passwords.
- Change passwords immediately if you suspect that they have been compromised.

3. Protect OTP, PIN and KYC Information

OXYZO customers should remain vigilant against phishing, impersonation and social-engineering attempts.

Customer must never disclose **OTPs, PINs, passwords, CVV, login credentials or other confidential information** to anyone over telephone, email, SMS, WhatsApp or social media, or any other communication channel.

Customers should be particularly cautious of **SIM-swap fraud, fraudulent KYC update requests** and requests to download or install unknown applications

4. Enable Two-Factor Authentication

Wherever available, enable **two-factor authentication (2FA) or multi-factor authentication (MFA)** for email, banking, financial and other important accounts.

Keep your operating system, web browser, applications and antivirus/security software updated with the latest security patches.

Secure your home Wi-Fi network with a strong, unique password and appropriate security settings.

5. Verify Before Clicking Links

When customer is in doubt, he/she is advised access the OXYZO website or other official online services by **manually typing the official website address in the browser** or by visiting <https://www.oxyzo.in/>.

Customers should avoid accessing websites or online services by clicking links received through unsolicited emails, SMS, WhatsApp messages or social media, as such links may lead to fraudulent or malicious websites.

6. Report Suspicious Communications

OXYZO will never ask customers to disclose confidential credentials, such as **OTP, PIN, Password or CVV** through unsolicited emails, SMS or telephone calls, or any other communication channel.

Customers should immediately report any suspicious or fraudulent communication claiming to originate from OXYZO by emailing at fraud@oxyzo.in.

DON'TS – WHAT CUSTOMERS SHOULD AVOID

1. Do Not Deal with Illegal Loan Apps

Customers are advised not to obtain loans through **illegal, fraudulent or unregistered loan applications / digital lending platforms**.

Before availing any loan through a digital lending platform, customers should **verify the authenticity of the platform and confirm its association with OXYZO** through the Company's official channels.

2. Do Not Share Confidential Information

Customers should **never share personal, financial, or sensitive information** with unknown or unauthorised persons through telephone calls, SMS, email, WhatsApp, social media, or any other communication channel, including:

- OTP
- PIN
- Password
- CVV
- Internet banking credentials
- Debit / credit card details
- KYC documents
- Aadhaar/PAN details
- Bank account details

3. Avoid Pop-up Advertisements

Customers should not respond to suspicious pop-up advertisements or click on unknown pop-ups that appear while browsing the internet, particularly those claiming that the customer has won a prize, received a loan approval or need to urgently update KYC information.

4. Avoid Public or Open Wi-Fi

Customer should avoid accessing banking, financial or other sensitive accounts through **public, open or unsecured Wi-Fi networks**.

Customers are advised to use a trusted and secure internet connection when accessing financial services.

5. Do Not Trust Urgent or Threatening Calls

Fraudsters may create a sense of urgency by claiming that a loan will be cancelled, KYC will expire, an account will be blocked or immediate payment is required.

Customers should not act under pressure. If you receive such a communication, disconnect the call and independently contact OXYZO through getsupport@oxyzo.in or +917353013499 to verify the information.

6. Do Not Install Unknown Applications

Customers should not install mobile applications, screen-sharing applications or remote-access software at the request of an unknown person claiming to represent OXYZO.

7. Verify Before Making Any Payment

Before making any payment towards **processing fees, insurance, documentation charges or other loan-related charges**, customers should verify the payment request through OXYZO's official communication channels i.e. getsupport@oxyzo.in.

Customers should never **transfer money to any personal bank account, UPI ID, or digital wallet** provided by an unknown person claiming to be an OXYZO employee, agent, intermediary, or representative.



DATA SECURITY

1. OXYZO maintains appropriate **security controls and safeguards** to protect customer information and restrict access to authorized personnel based on legitimate business requirements and applicable policies.
2. Customer information is accessed and processed only for **legitimate and authorized purposes** in accordance with the Company's applicable **Privacy Policy and information-security requirements**.
3. Customers are also advised to exercise caution while sharing their **personal, financial, or other sensitive information** and to immediately report any suspected misuse or unauthorized disclosure through OXYZO official communication channels i.e. getsupport@oxyzo.in or call +917353013499.