



The Complete Guide to Scam Detection & Prevention

Your Essential Handbook for Staying Safe Online



Table of Contents

1. What Are Scams?
2. Common Types of Scams
3. Homoglyph & Domain Spoofing Attacks
4. Red Flags to Watch For
5. Real Examples of Scam Messages
6. How to Protect Yourself
7. What to Do If You've Been Scammed
8. Quick Reference Checklist



What Are Scams?

Scams are fraudulent schemes designed to steal your money, personal information, or both. Scammers use sophisticated psychological tactics to create urgency, fear, or excitement to make you act without thinking.

Key Facts:

1. **Billions of dollars** are lost to scams globally every year
2. Scams target people of **all ages, backgrounds, and income levels**
3. Modern scams use **AI and advanced technology** to appear more legitimate
4. **Prevention through awareness** is your best defense



Common Types of Scams



Prize & Lottery Scams

How it works: You receive a message claiming you've won money, but must pay fees to claim it.

Reality Check: Legitimate contests never require upfront payments.

Job & Employment Scams

How it works: Fake job offers requiring registration fees or personal information.

Red Flag: Any job requiring you to pay money upfront is a scam.

Banking & Financial Scams

How it works: Fake messages claiming your account is suspended or compromised.

Warning: Banks never ask for passwords, PINs, or OTPs via email or SMS.

Romance Scams

How it works: Fake online relationships leading to requests for money.

Reality: Someone you've never met in person asking for money is a major red flag.

Government Scheme Scams

How it works: Fake messages about COVID relief, subsidies, or tax refunds requiring fees.

Fact: Government agencies never ask for processing fees via phone or email.

Homoglyph & Domain Spoofing Attacks

What Are Homoglyphs?

Homoglyphs are characters that look identical but are actually different. Scammers use these to create fake websites and emails that appear legitimate.

Common Examples:

Visual Lookalikes:

<u>Legitimate</u>	<u>Fake Version</u>	<u>What Changed</u>
google.com	goog I e.com	Capital I instead of lowercase l
google.com	g 00 gle.com	Zeros instead of O's
paypal.com	paypa I .com	Capital I instead of lowercase l

amazon.com amaz0n.com Zero instead of O
microsoft.com rnicrosoft.com "rn" looks like "m"

Unicode Character Substitution:

<u>Legitimate</u>	<u>Fake Version</u>	<u>Character Used</u>
-------------------	---------------------	-----------------------

apple.com	apple.com	Cyrillic 'a' instead of Latin 'a'
google.com	google.com	Cyrillic 'o' instead of Latin 'o'
paypal.com	paypal.com	Cyrillic 'p' instead of Latin 'p'

Suspicious Domain Patterns:

1. **Prefixes:** secure-, verify-, payment-, official-
2. **Suffixes:** -secure, -verify, -support, -help
3. **Suspicious TLDs:** .tk, .ml, .ga, .cf, .xyz, .top, .club



Red Flags to Watch For



IMMEDIATE DANGER SIGNS

Prize/Money Related:

1. "You have won" + "pay fee to claim"
2. "Congratulations, you're selected"
3. "Pay processing/verification fee"
4. "Show legitimacy by paying first"

Urgency Tactics:

1. "Urgent action required"
2. "Account will be suspended"
3. "Limited time offer"
4. "Act now or lose money"

Information Requests:

1. "Share your OTP/PIN"
2. "Send Aadhaar/PAN details"

3. "Verify via this link"
4. "Update your KYC immediately"

Job/Government Scams:

1. "Work from home - pay registration fee"
2. "Government scheme - pay to apply"
3. "COVID relief fund - processing fee required"
4. "Selected for job - pay security deposit"

SUSPICIOUS PATTERNS

Generic Greetings:

1. "Dear Customer" instead of your name
2. "Valued User" or "Account Holder"

Poor Grammar/Spelling:

1. Multiple spelling errors
2. Awkward phrasing
3. Mixed languages inappropriately

Contact Information:

1. Gmail/Yahoo addresses for "official" communication
2. WhatsApp numbers for bank support
3. Shortened URLs (bit.ly, tinyurl.com)

Real Examples of Scam Messages

Example 1: Lottery Scam

 **SCAM ALERT** 

"CONGRATULATIONS! You have won ₹25,00,000 in Google Lucky Draw 2024. To claim your prize, pay processing fee of ₹5,000 to account: XXXX-XXXX-XXXX.
Contact: +91-XXXXXXXXXX"

RED FLAGS:

- ✗ Unsolicited prize notification
- ✗ Requires upfront payment

- ✗ Uses unofficial contact methods
- ✗ Creates false urgency

Example 2: Banking Scam

 SCAM ALERT 

"URGENT: Your SBI account has been temporarily suspended due to suspicious activity. Click here to verify: <http://sbi-secure-login.tk>
Share OTP within 24 hours to avoid permanent closure."

RED FLAGS:

- ✗ Creates panic with "suspended account"
- ✗ Suspicious domain (.tk extension)
- ✗ Requests OTP sharing
- ✗ Unofficial communication channel

Example 3: Job Scam

 SCAM ALERT 

"Congratulations! You are selected for Data Entry work from home. Salary: ₹25,000/month.
Pay registration fee ₹2,500 to confirm your position.
WhatsApp: +91-XXXXXXXXXX"

RED FLAGS:

- ✗ Unsolicited job offer
- ✗ Requires registration fee
- ✗ Too good to be true salary
- ✗ Uses WhatsApp for business communication



How to Protect Yourself

 **DO's**

Verification:

1. **Always verify** through official channels
2. **Double-check** URLs character by character

3. **Call the organization directly** using official numbers
4. **Ask trusted friends/family** for second opinions

Safe Practices:

1. **Use official apps** instead of clicking links
2. **Enable two-factor authentication** on all accounts
3. **Keep software updated** on all devices
4. **Use reputable antivirus software**

Information Sharing:

1. **Never share** OTPs, PINs, or passwords
2. **Be cautious** with personal information on social media
3. **Verify identity** before sharing sensitive data

DON'Ts

Never Pay Upfront:

1. Don't pay fees to claim prizes
2. Don't pay for job applications
3. Don't pay processing fees for loans
4. Don't pay to access "government schemes"

Never Share Sensitive Info:

1. Don't share OTPs with anyone
2. Don't give banking details over phone/email
3. Don't click suspicious links
4. Don't download attachments from unknown sources

What to Do If You've Been Scammed

Immediate Actions:

1. Stop Further Damage

1. **Change all passwords** immediately
2. **Contact your bank** to freeze accounts
3. **Report unauthorized transactions**
4. **Scan devices** for malware

2. Document Everything

1. **Save all communications** (emails, messages, call logs)
2. **Take screenshots** of fraudulent websites
3. **Keep transaction records**
4. **Note dates and times**

3. Report the Scam

1. **File police complaint** at local cyber crime cell
2. **Report to bank** if financial fraud occurred
3. **Contact telecom provider** for SIM-related fraud
4. **Report to relevant authorities**

Recovery Steps:

Financial Recovery:

1. **Contact bank immediately** for transaction disputes
2. **File insurance claims** if applicable
3. **Monitor credit reports** for unauthorized activities
4. **Consider legal action** for significant losses

Identity Protection:

1. **Monitor all accounts** regularly
2. **Set up fraud alerts** with credit agencies
3. **Consider identity monitoring services**
4. **Be extra vigilant** for future attempts

Quick Reference Checklist

Before Clicking Any Link:

1. Is the sender's email address legitimate?
2. Does the URL match the official website exactly?
3. Are there any spelling errors in the domain?
4. Does the message create unnecessary urgency?

Before Sharing Information:

1. Did I initiate this communication?

2. Is the request coming through official channels?
3. Would a legitimate organization ask for this information?
4. Have I verified the identity of the requester?

Before Making Any Payment:

1. Is this payment request legitimate?
2. Have I verified through official channels?
3. Am I being pressured to pay immediately?
4. Does this seem too good to be true?

Red Flag Phrases to Watch For:

1. "You have won" + payment request
2. "Urgent action required"
3. "Share your OTP/PIN"
4. "Pay to claim/verify/process"
5. "Limited time offer"
6. "Account suspended"
7. "Click here immediately"

Emergency Contacts

India:

1. **Cyber Crime Helpline:** 1930
2. **National Consumer Helpline:** 1915
3. **Banking Fraud:** Contact your bank immediately

International:


1. **USA:** FBI Internet Crime Complaint Center (IC3)
2. **UK:** Action Fraud (0300 123 2040)
3. **Canada:** Canadian Anti-Fraud Centre (1-888-495-8501)

Remember: The Golden Rule

"If it sounds too good to be true, it probably is."

Trust your instincts. If something feels wrong, it probably is. When in doubt:

1. **Pause** and think
2. **Verify** through official channels
3. **Consult** trusted friends or family
4. **Report** suspicious activity

Stay informed, stay vigilant, stay safe! 

Document Version: 1.0

Last Updated: June 2025

Source: Comprehensive Scam Detection Guide