HOW TO SPOT A SCAM

A Public Trust Guide by VELURYN AGNECY

Based on 11 real scam cases observed across LinkedIn, Threads, X, WhatsApp, Facebook Messenger, Email, and SMS — analysed using VASD Trust Authority Infrastructure.

Every scam in this guide was shared publicly by real people who almost — or did — fall for it. The patterns repeat. The techniques are identical. Once you know them, they become impossible to miss.

velurynagnecy.com — Trust First. Everything Follows.

THE 6 THINGS EVERY SCAM DOES

Across every scam reviewed — fake job offers, Meta phishing, WhatsApp impersonation, fake PayPal invoices, Illuminati recruitment, dying orphan stories — the same six mechanics appear. Not similar. Identical.

1 PRETENDS TO BE SOMEONE YOU TRUST

Meta. Amazon. PayPal. Elon Musk. HR Manager. WhatsApp Support. The name is chosen because it bypasses your first question. You stop asking 'who is this?' and start responding to 'what do they want?'. The name is the trap. Everything else is the bait.

ASK: Would this entity actually contact me this way, on this platform, from this address?

2 CREATES PRESSURE SO YOU DON'T THINK

'Your account will be permanently deleted in 24 hours.' 'Submit before midnight.' 'Report within 24hrs for instant refund.' Urgency is not information. Urgency is a weapon. It is designed to make you act before you verify. Any message that needs you to act immediately, before you can think — that's the scam.

ASK: What happens if I take 30 minutes to verify this independently before I do anything?

3 MOVES YOU AWAY FROM THE SAFE ENVIRONMENT

'Click Here to Apply.' 'Call +1 (805) 721-7732.' 'Submit details through the link only.' 'Please verify using the file attached below.' Legitimate platforms resolve legitimate issues in-platform. Amazon doesn't link you to dtmg.arsbjl.shop. PayPal doesn't ask you to call a random phone number. The redirect is the scam.

ASK: Why am I being moved away from the official platform to complete this action?

4 USES A FAKE SENDER ADDRESS

The display name says 'Poonam Sharma HR' — the actual email is sanjoli.raj@freshersindia.in. The display name says 'Amazon' — the actual sender is xbox22027xbox@gmail.com. The display name says 'Meta Verified' — the account name has a spelling error. The display name costs nothing to fake. The actual address always reveals the truth.

ASK: What does the actual sender email/number say — not the display name?

5 HITS YOU IN THE FEELINGS

Fear: 'Your account will be deleted / You've been accused of fraud.' Greed: 'You've been shortlisted / 65,000 per month / $2.19M left for you.' Sympathy: 'I'm a dying orphan with no one to leave my money to.' Every one of these is designed to activate an emotion that shuts down logic. When you feel panic, excitement, or pity — that's the exact moment to slow down.

ASK: Is this message designed to make me feel something before I've verified anything?

6 CREATES FAKE EVIDENCE

Professional-looking PDFs. Fake PayPal invoices. Fake Meta letterhead. Formatted HR emails. Invoice numbers. Receipt IDs. Transaction codes. All of these take less than 10 minutes to design. Visual legitimacy proves nothing. A PDF that looks official is not an official PDF.

ASK: Is this document from a verified source, or does it just look like one?

THE SCAMS WE ANALYSED — AND WHAT GAVE THEM AWAY

These are all real cases shared publicly online. Here's what the immediate giveaways were.

FAKE JOB OFFERS (India — freshersindia.in)

LinkedIn + Email

- Emails from sanjoli.raj@freshersindia.in — not from any actual company
- Multiple different HR 'display names' using the same address
- Asks you to submit details through an external link — not the company's career portal
- Same template, different names: Sutherland, Data Science, Front End Developer
- Google 'freshersindia.in scam' — you will find dozens of identical reports

THE RULE: If a job email doesn't come from the actual company's domain, it's not from the company.

PLATFORM IMPERSONATION — META / FACEBOOK

Facebook Messenger

- Account name: 'Meta Verrified' (double R) / 'Meta Buinsniness Cennter' — misspelled
- Sends threat of account deletion within 24 hours
- Attaches fake PDFs: 'Facebook_Account_Support_Center.pdf'
- Facebook/Meta never communicates account security through Messenger DMs from external accounts
- Any message threatening account deletion with an attachment is phishing

THE RULE: Meta contacts you through official in-app notifications. Never through Messenger from unknown accounts.

PLATFORM IMPERSONATION — WHATSAPP

WhatsApp / Threads

- Message from +258 82 095 0092 — Mozambique number, nothing to do with WhatsApp
- Claims your account is 'suspected of violating security rules'
- WhatsApp sends security alerts in-app only — never from random external numbers
- The prior 'disappearing messages' setting reveals the scammer erased earlier evidence

THE RULE: WhatsApp will never text you from a phone number about security. Ever.

CELEBRITY IMPERSONATION — ELON MUSK (X DM)

X (Twitter)

- Account: 'Mr Elon' with anime profile picture — not a verified account
- Opens with 'I'd love to speak with the rightful owner' — scripted rapport-building
- Continues with the same script regardless of what you say
- Blocks when you don't comply — scammers abandon when the target doesn't engage
- No real celebrity builds DM-based fan relationships with random accounts

THE RULE: If 'Elon Musk' is messaging you on X, it is not Elon Musk.

SMISHING — AMAZON PRODUCT RECALL (SMS)

iMessage / SMS

- Sent from xbox22027xbox@gmail.com — Gmail is never Amazon's communication channel
- Link goes to dtmg.arsbjl.shop — has nothing to do with Amazon
- Asks you to 'Reply Y' — confirms your number is active for more spam
- Amazon communicates recalls through the app, your email on file, and amazon.com

THE RULE: Amazon will never send you an official SMS from a Gmail address.

CALLBACK FRAUD — FAKE PAYPAL FIREARM INVOICE

Threads / Email

- Fake invoice claiming you purchased a SIG Sauer P365 handgun for $479.99
- Designed to cause panic so you call the provided number immediately
- Phone number +1 (805) 721-7732 is not PayPal — PayPal support is via paypal.com
- If you call: scammer asks to 'verify your identity' via screen share and steals your real accounts
- The firearm item is chosen deliberately — it creates legal fear, not just financial fear

THE RULE: Never call a phone number from an unexpected invoice. Go to the company's official website.

ADVANCE FEE — DYING ORPHAN STORY (X DM)

X (Twitter)

- Emotional story of dying orphan leaving $2.19M to strangers
- Provides 'login credentials' upfront — this is bait, not generosity
- If you log in to 'check', you are then asked to verify your own identity — that's the steal
- Account @JoHenry380767 — numbered suffix = mass-created account
- Link to t.co shortened URL with no verifiable destination

THE RULE: No one dies and leaves millions to random strangers via X DM. The money shown is bait for your own credentials.

ILLUMINATI RECRUITMENT (WhatsApp/X DM)

X / WhatsApp

- Opens with a spiritual, warm message to build emotional rapport
- Waits, then invites you to join the 'GRAND LODGE' and 'brotherhood of the Illuminati'
- Next step (not shown) would be an initiation fee or cryptocurrency transfer
- No organization recruits members via unsolicited DM from strangers

THE RULE: Any unsolicited invitation to join a secret or exclusive organization will eventually ask for money.

MUSIC INDUSTRY / DEF JAM DEAL SMS

Threads / SMS

- Claims you have a deal with 'Mark and Def Jam'
- Says your email was 'hacked' — isolation tactic to prevent you verifying
- Demands you publish an announcement 'before midnight'
- Link goes to indieinc.live — not a Def Jam or industry-recognized domain
- Extreme deadline pressure combined with isolation from verification channels

THE RULE: Real record deals are documented through lawyers and verified contracts. Not SMS.

WHAT TO DO WHEN SOMETHING FEELS WRONG

1	**STOP** Do not click the link. Do not call the number. Do not open the attachment. Do not reply. Stopping costs you nothing. Acting costs you everything.
2	**VERIFY THE SENDER** Check the actual email address or phone number — not the display name. Look for domain mismatches. If it claims to be Amazon but sends from Gmail, it's not Amazon.
3	**GO DIRECTLY TO THE SOURCE** If the message claims to be from your bank, PayPal, Amazon, Meta — open a fresh browser tab and go directly to the official website. Do not use any link provided in the message.
4	**SEARCH THE EXACT TEXT** Copy a sentence from the suspicious message and search it on Google. Scam templates are reused across millions of targets. Someone else has almost certainly reported it.
5	**ASK SOMEONE** Show the message to someone you trust before you act. Scams work better in isolation. A second opinion breaks the urgency spell.
6	**REPORT IT** Report the message as spam on the platform. Report phishing emails to your email provider. In India, report to cybercrime.gov.in. Your report protects someone else.

> *"The gap between looking legitimate and being legitimate is where the world's trust is being stolen."*

VASD — VELURYN AGNECY // Trust First. Everything Follows.
velurynagnecy.com // @velurynagnecy // velurynandoc@gmail.com

This guide is issued under VASD Trust Authority Infrastructure. All cases are based on publicly shared real-world specimens. VASD classifications are probabilistic trust assessments, not legal determinations.