Scam Detection Tool Companion Guide

Tool · How To Get The Most Out Of The Live Scam Detector — Plus A Manual Backup Method.

The on-site Scam Detector analyses suspicious emails, texts, and messages instantly. This guide explains how to use it well — and what to do if it's not handy.

Using The Live Tool

1. Visit the Scam Detector page on the site.
2. Paste the suspicious message (email body, text, social DM) into the input field.
3. If applicable, paste the sender address or phone number separately.
4. Click 'Analyse.' Results return in 5-10 seconds.
5. Read the score (0-100) and the breakdown of red flags identified.
6. Click any flag for a deeper explanation.

How To Read The Results

Score	Meaning	What To Do
80-100	Almost certainly a scam.	Don't reply, don't click. Report to the platform. Forward to FTC.
50-79	Likely scam, but not certain.	Verify out-of-band: open the company's site directly or call the number on the back of
30-49	Suspicious — investigate.	Hover all links to check destinations. Check sender domain carefully.
10-29	Possibly legitimate, low-risk indicators.	Still verify before acting on any urgent request.
0-9	No flags found.	Doesn't guarantee safety. Apply common sense.

Manual Detection — When The Tool Isn't Available

Score the message yourself using this 8-point check. Each 'yes' = +10 points (toward scam).

- Creates urgency — 'act now,' 'final notice,' 'account suspended.'
- Sender domain looks slightly off (paypa1.com, arnazon-shop.net).
- Generic greeting ('Dear customer') from a service that knows your name.
- Asks for credentials, full SSN, or banking details via email/text.
- Asks for money via gift card, wire, Zelle, or crypto.
- Threatens (lawsuit, arrest, deportation, account closure).
- Hovering links shows a destination different from what's displayed.
- Spelling/grammar errors in supposedly corporate communication.

False Positives & Edge Cases

- **Legitimate marketing email** with promotional urgency — usually scores 30-50. Verify the sender domain matches the brand.
- **Forwarded emails** — the original sender is buried. Score the original message, not the forwarder.
- **HTML emails with hidden text** — open in plain-text mode if your client allows.
- **Internal corporate emails** with standard 'verify your account' phrasing — verify the URL matches your company's actual SSO domain.

If You Already Clicked Or Replied

1. Don't panic. Don't engage further with the scammer.
2. Disconnect Wi-Fi if you downloaded anything.
3. Change passwords on any account you submitted credentials for, immediately, from a clean device. Enable MFA.
4. Run a malware scan.
5. Notify your bank if any financial info was shared. Consider a credit freeze.
6. Report at reportfraud.ftc.gov and to the platform where the scam reached you.
7. If money was sent: contact the bank/payment platform within 24 hours — fastest recovery.

Train The Family

Forward analysed scams to your family with the score and red flags highlighted. Real examples teach more than any article — and your family library of past scams becomes the best inoculation against future ones.