threat level: human

The attack vector you can't patch.

Text and QR-Code Scams

Smishing texts and tampered QR codes, and the one rule that defuses both.

$470M
reported losses to text scams in 2024
FTC, 2025

5x
rise in text-scam losses since 2020
FTC, 2025

21 sec
median time to click a phishing link
Verizon DBIR, 2024

SPOTTING A SCAM TEXT

01 A link in an unexpected text
A delivery, toll, or bank 'alert' urging you to tap a link right now.

02 A sender that does not fit
A personal mobile number claiming to be a company, or a shortened link.

03 Urgency over a small problem
A tiny unpaid fee or a held package, with a threat if you do not act.

QR-CODE (QUISHING) TRAPS

04 A QR code placed over a real one
A sticker on a parking meter, menu, or invoice sending you to a fake site.

05 A code that asks you to log in or pay
Any QR that lands on a login or payment page deserves a hard stop.

COMMON TEXT AND QR LURES

06 Delivery and toll 'fees'
A package or unpaid toll that needs a small payment through a link.

07 Bank and account 'alerts'
A fraud warning that wants you to log in or 'confirm' through a link.

08 Wrong-number and job texts
A friendly 'wrong number' or an easy-money job that warms you up for a scam.

DO / DON'T

DO

- Open the company's app or a typed address and check the status there.
- Delete and report unexpected texts, and block the sender.
- Check where a QR code leads before you act, and beware stickers placed over real codes.
- Use phishing-resistant MFA so a stolen password alone is not enough.

DON'T

- Do not tap links in unexpected texts.
- Do not scan untrusted QR codes, especially in public places.
- Do not enter logins or card details on a page reached from a text or a QR.
- Do not reply to an obvious scam text. It confirms a live number.

THE ONE MOVE

Do not tap links in unexpected texts or scan untrusted QR codes. Go to the company yourself through its app or a typed address and check the real status there. The link is the trap.

IF IT HAPPENS

1. Do not click further. If you entered details, change that password now.
2. Call your bank if you shared card or login details.
3. Report the text (forward to 7726 in the US) and to reportfraud.ftc.gov.
4. Watch for follow-up scams that use the information you gave.

Get a briefing like this every week, free.
threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: U.S. FTC (2025); Verizon DBIR (2024). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.