Spot the phish:

5 red flags in a dodgy email

Can you spot what's wrong before you click?

From: National Bank Security <alerts@nationa1-bank-secure.com> 1

Subject: URGENT: Your account has been suspended 2

To: you

Dear Customer, 3

We have detected suspicious activity on your account. For your security, access has been temporarily restricted. If you do not verify your identity within **24 hours,** your account will be **permanently closed.**

Please click below to confirm your details and restore access immediately:

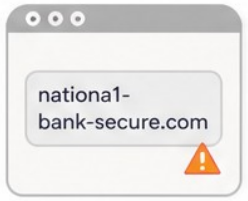
Verify my account now 4

national-bank-secure.com/login/verify-id-938271

If you did not make this request, please ignore this email. Thank you for you're continued trust in National Bank. 5

Stay safe. Think before you click!

- ✓ Never click links or share details from unexpected emails.
- ✓ Always verify by visiting the official website or contacting the company directly.
- ✓ When in doubt, don't click – report it.

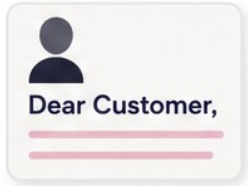


1 Dodgy sender address

It says "National Bank" but the actual email domain is *nationa1-bank-secure.com* — that's a number 1, not a letter L. Real banks send from their real domain.

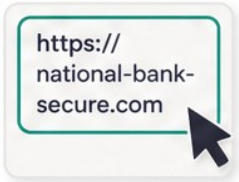
2 Pressure and urgency

"URGENT", "suspended", "24 hours", "permanently closed" — all designed to panic you into clicking before you think. Legitimate organisations don't threaten you in subject lines.



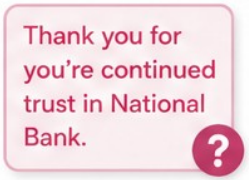
3 Generic greeting

"Dear Customer" — your bank knows your name. If they're not using it, they probably don't know it.



4 Suspicious link

The button looks official, but hovering reveals a URL on the same fake domain. Always check where a link actually goes before you click.



5 Grammar slip

"Thank you for you're continued trust" — that should be "your". A small mistake, but professional communications from banks go through multiple checks. Errors like this are a giveaway.

riskready