

Subject: Immediate Action Needed: Your Account Is Locked

From: security@ yourbank-online.com

Looks official, right? That's exactly what the scammer wants.

"Urgent Action Required"

Cybercriminals LOVE turning up the panic.

If they can make you rush, they know you're less likely to think clearly.

Always pause and ask: Is this really urgent?



From: security@yourbank-online.com

Looks fine in the preview pane... until you zoom in.
Legitimate banks don't usually use odd domains like "-online.com"

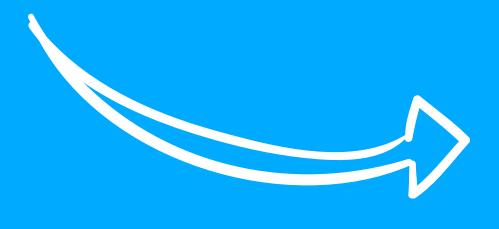
A quick search for the bank's real support email can expose the fake.



"Dear Customer"

If this were truly your bank, wouldn't they greet you by name?

Phishing emails often use vague, generic openings because they don't actually know who you are.



Click here to "restore access now".

Before you click anything, hover your mouse over the link. Does the address match the real website, or something completely different?

Scammers love hiding dangerous links behind friendly-looking text.

Notice the emotional cocktail in that message:



Pressure: "You must act immediately

That one-two punch is designed to get you to click first and think later.

Looks polished and professional,

maybe even showing your bank's logo front and center. Logos and layouts are easy to copy.

If you weren't expecting the message, treat it with suspicion.

"Download the form to verify your account"

NEVER open an attachment you were not expecting.

Malicious files can quietly install malware and compromise your whole system.



So, what is the safer move?

- Take a breath
- Don't click anything
- Contact the company directly using a known phone number or website



Phishing attacks are getting slicker and harder to spot.

Would everyone on your team recognise all of these warning signs?

Ongoing security training + everyday awareness = your strongest frontline defense

Want support turning your people into scamsmart, security-savvy users?

Reach out and let's protect your organization together.

