

How to Spot a Phishing Email

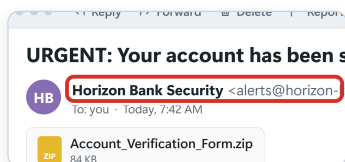
7 warning signs every home and business user should know, and what to do when you spot one.



*We Make
I.T.
Happen!*

1 Check the Sender

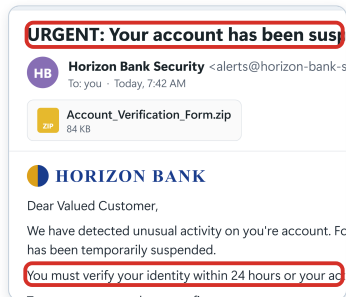
The name looks official, but the **real address** is a look-alike domain.



Look at the full email address, not just the display name.

2 Urgent or Threatening?

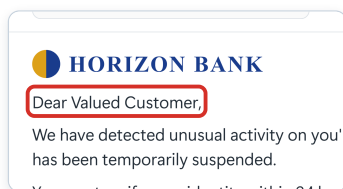
Countdowns and threats are designed to make you **panic and act fast**.



Slow down. Real companies rarely give you 24 hours.

3 Generic Greeting

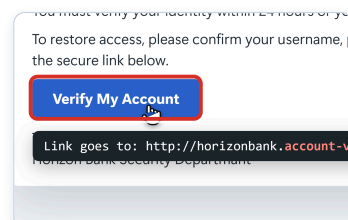
"Dear Valued Customer" means they **don't know who you are**.



Your bank knows your name, and uses it.

4 Hover Over Links

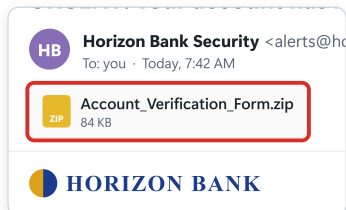
The button says one thing; the **real web address** says another.



Hover with your mouse (or press and hold on a phone) to preview the link.

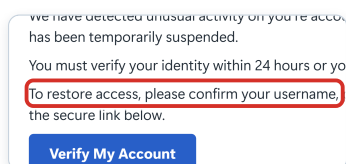
5 Unexpected Attachments

Zip files, web pages and Office files that ask you to **"enable content"** can install malware.



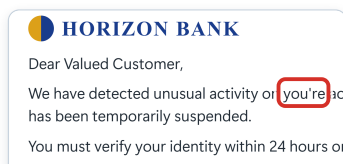
6 Requests for Personal Info

No real company asks for your **password, SSN or card number** by email.



7 Spelling & Grammar

Typos, awkward wording and odd formatting are common giveaways.



8 Spotted One? Don't Bite

Don't click, don't reply. Use **Report phishing**, then **delete** it.



Not sure? Call the company using a number you know



Good to Know

- **Fake requests from the boss or a vendor** (gift cards, new bank details, rush wires)? Always confirm by phone.
- Already clicked? **Change your password** right away and turn on **multi-factor authentication**.
- Businesses: call us for **email security and staff training**. The sooner, the better.



Need Help?

Contact Naples Computers
239-513-1960
We Make I.T. Happen!