

NAPLES COMPUTERS HOW-TO • EMAIL SECURITY

How to Spot a Phishing Email

Phishing emails are one of the most common ways scammers break into home computers and business networks. They pretend to be your bank, a delivery company, a vendor, or even your boss, and try to get you to click a bad link, open an infected file, or hand over a password. Use this guide to spot the warning signs before you click.

What is **phishing**?

A fake email designed to trick you. It often looks like it came from your bank, a shipping company, or even your boss.

Click a bad link

That leads to a fake login page or a malicious website.

Open an infected file

That quietly installs malware or ransomware.

Hand over your info

Passwords, account numbers, or payment details.

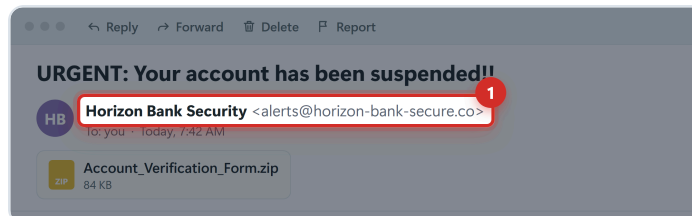
The 7 warning signs

1**Check the sender's address**

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

WHAT TO DO

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



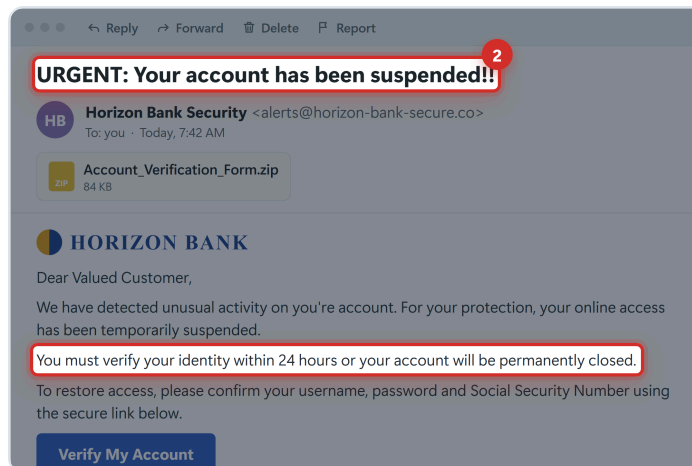
2

Watch for urgent or threatening language

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

WHAT TO DO

Slow down. Real companies rarely give you 24 hours.



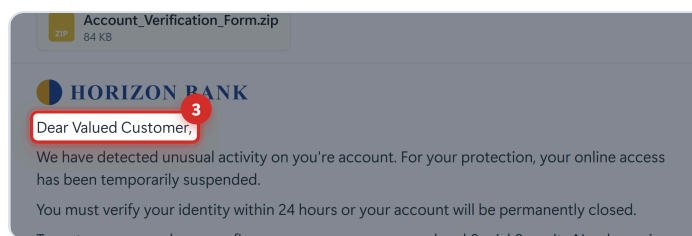
3

Beware of generic greetings

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

WHAT TO DO

Your bank knows your name, and uses it.



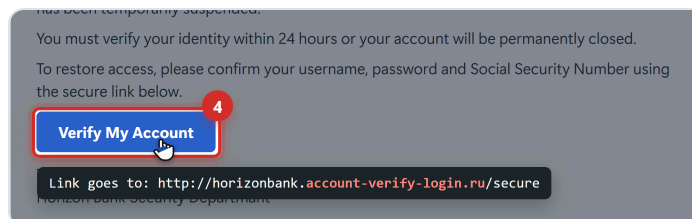
4

Hover over links before you click

The button says one thing. The real web address says another.

WHAT TO DO

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



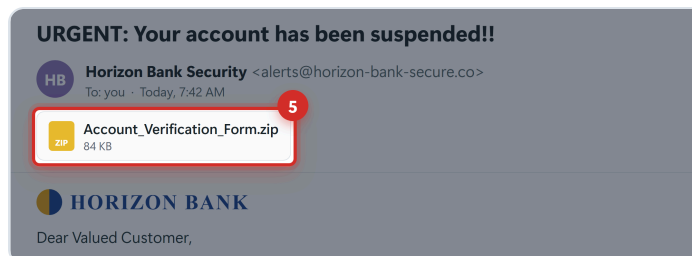
5

Don't open unexpected attachments

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

WHAT TO DO

Not expecting it? Don't open it. Verify first.



6

Never send personal info by email

No real company will ask for your password or Social Security number in an email.

WHAT TO DO

Requests for passwords, SSNs or card numbers mean it's a scam.

Dear valued Customer,

We have detected unusual activity on your account. For your protection, your online access has been temporarily suspended.

You must verify your identity within 24 hours or your account will be permanently closed.

To restore access, please confirm your username, password and Social Security Number using the secure link below.

[Verify My Account](#)

Thank you for your cooperation.

7

Look for spelling and grammar mistakes

Typos, awkward wording and odd formatting are common giveaways.

WHAT TO DO

Professional companies proofread. Scammers often don't.

 **HORIZON BANK**

Dear Valued Customer,

We have detected unusual activity on your account. For your protection, your online access has been temporarily suspended.

You must verify your identity within 24 hours or your account will be permanently closed.

To restore access, please confirm your username, password and Social Security Number using the secure link below.

[Verify My Account](#)

Thank you for your cooperation.
Horizon Bank Security Department

BUSINESS ALERT

!

Fake requests from your boss or a vendor

Gift cards, changed bank details or rush wire transfers, sent quietly and in a hurry.

PROTECT YOUR BUSINESS

Always confirm by phone, using a number you already know.

⋮ ⋮ ⋮ [Reply](#) [Forward](#) [Delete](#) [Report](#)

Quick favor - are you at your desk?

 **Mike Thompson** <mike.thompson.office@gmail.com>

To: you · today, 9:15 AM

Hi,

I'm stuck in back-to-back meetings and can't take calls. I need you to buy five \$200 gift cards for a client today.

Please keep this between us for now - it's a surprise. Scratch off the back and send me photos of the codes ASAP. I'll pay you back this afternoon.

Thanks,
Mike

Sent from my phone

Spotted one? Here's what to do.

- ☐ Don't click links or open attachments
- ☐ Don't reply to the sender
- ☐ Report it
Use the "Report phishing" button, or forward it to your I.T. team
- ☐ Delete it

Not sure? Contact the company using a phone number or website you already trust.

Already clicked? Act fast.

- ☐ Change your password
Start with the account you entered it into, then any account that uses the same password
- ☐ Turn on multi-factor authentication
A code on your phone stops attackers even if they have your password
- ☐ Call Naples Computers: 239-513-1960
We'll check your computer and accounts. The sooner, the better.

Recap: spot the scam

- ☐ Check the sender's address
- ☐ Watch for urgent threats
- ☐ Be wary of generic greetings
- ☐ Hover before you click
- ☐ Avoid unexpected attachments
- ☐ Never email personal info
- ☐ Look for spelling mistakes
- ☐ Verify money requests by phone

When in doubt, throw it out. If an email makes you nervous, don't click anything. Call the company using a phone number you already know, or call us.



Questions about email security for your home or business?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**