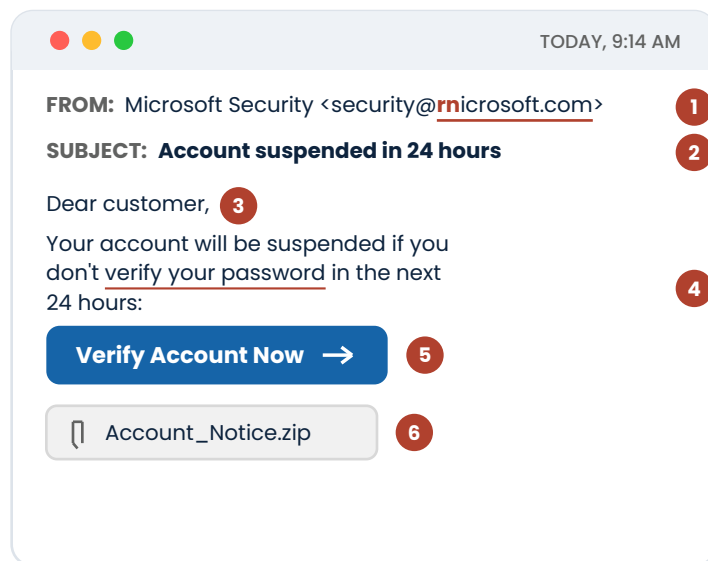


Even if the email looks real, it might still be **a scam.**

How to spot a phishing email, and how to verify before you click.

01 ANATOMY OF A PHISHING EMAIL



- 1 Lookalike domain**
“rn” is built to look like the “m” in microsoft
- 2 Urgency**
a 24-hour deadline to rush you
- 3 Generic greeting**
“Dear customer,” not your name
- 4 Asks for credentials**
wants you to enter your password
- 5 “Verify” button**
a link masking where it really goes
- 6 Attachment**
an unexpected file to open



If you're not 100% sure,
don't click. Call us at

541.696.5555 · Option 1

02 HOW TO VERIFY IF IT'S A SCAM

- 1 Did you expect this email?**
If no, and it is asking you to click, log in, or send something, treat it as untrusted by default.
- 2 Don't act. Pause and verify.**
The attacker counts on you reacting fast. Hold off on clicking, replying, or opening attachments.
- 3 Inspect the sender and every link.**
Hover over the email and link. Even if the link looks real, it could be masked. Don't trust it.
- 4 Verify through a separate channel.**
Don't reply or use any contact info from the email. Type the company's URL yourself, or call us directly.
- 5 Report it, then delete.**
Forward it to us at support@systech.io, or use your “Report” button, then empty it from trash.

The golden rule

If you are not 100% sure, don't click. Call the helpdesk at 541.696.5555, Option 1, and we will check it for you.



Veteran-led managed IT & cybersecurity, proudly serving Southwest Oregon.
435 NE Casper St., Roseburg, OR 97470
Helpdesk: **541.696.5555 · Option 1**
systech.io