

HOW TO SPOT A PHISHING EMAIL



What is a phishing email?

A phishing email is a fake message designed to trick people into giving away personal information like passwords, usernames and other sensitive information or include links to fake websites or attachments that install harmful software. Attackers may send emails that look like they are from trusted sources, such as government agencies or legal firms.

Cybercriminals' Strategies for Theft



Phishing attackers often send emails or messages that appear legitimate, posing as trusted sources. They use urgent language to instill fear or excitement, claiming you must verify your account to avoid losing access. Their goal is to trick you into revealing sensitive information without your awareness.

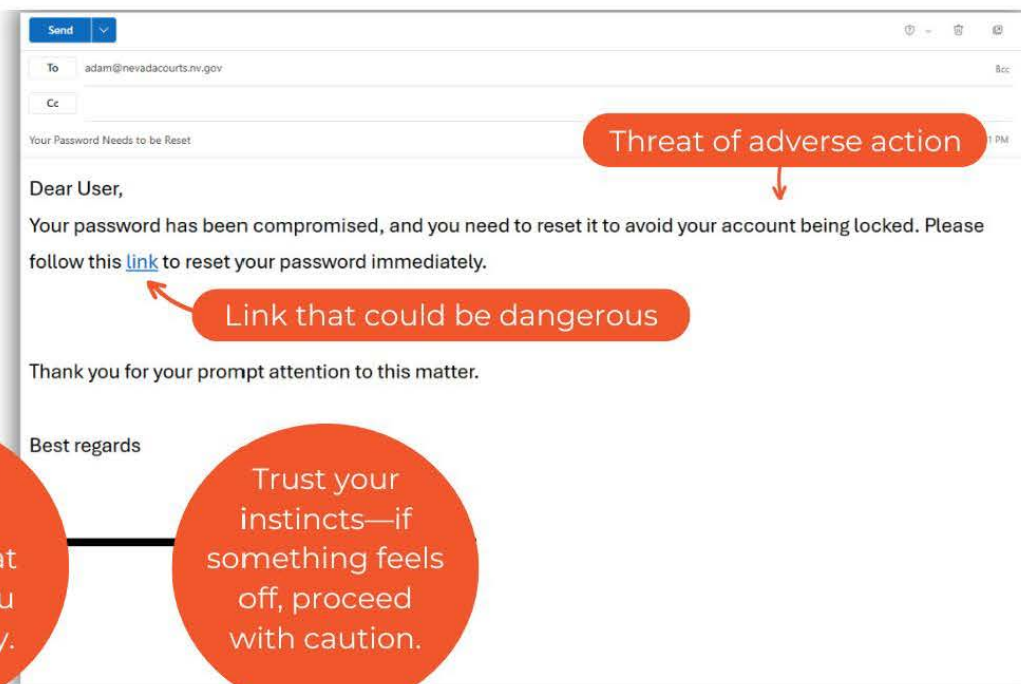
Red Flags of a Phishing Email

Check the sender's email address for slight differences or misspellings.

Be wary of urgent language that pressures you to act quickly.

Hover over links (without clicking) to verify their URLs. If they look suspicious or don't match the company's website, avoid clicking.

Trust your instincts—if something feels off, proceed with caution.



What to Do If You Suspect a Phishing Email

- If you receive a phishing email, do not engage or click any links.
- **Report any suspicious emails to your IT department using the "Phish Alert Button" in the Outlook menu.**
- If it appears to be from a legitimate organization, verify its authenticity using an alternate form of communication.
- Using the "Phish Alert" button will remove the email to avoid accidental interactions.
- Remain cautious with suspicious communications.

