

Six Signs an Email is a Phish

Wolf Creek security guide

Security reminder: Stop when a request feels unusual or urgent. Verify it using a trusted method and contact Technology Services if you are unsure.

STEP 1 Check the sender

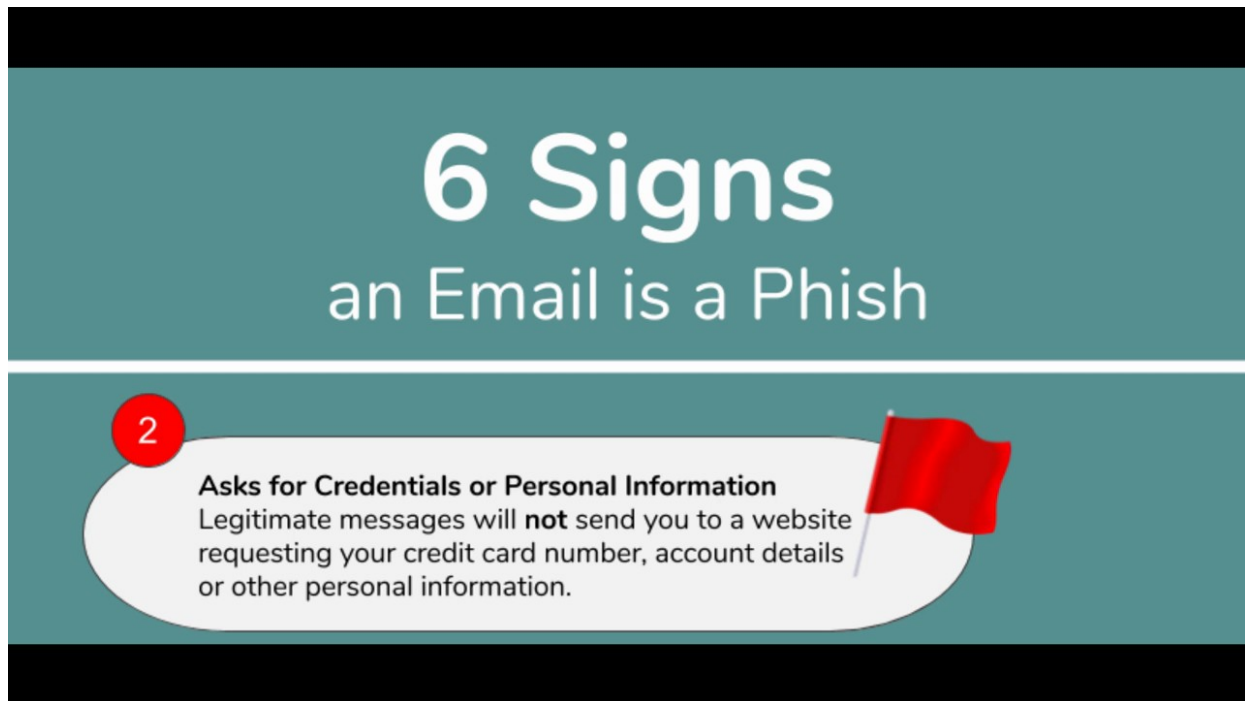
Look for a mismatched address, unusual display name, or message that does not sound like the sender.



Video reference: Check the sender.

STEP 2 Watch for pressure

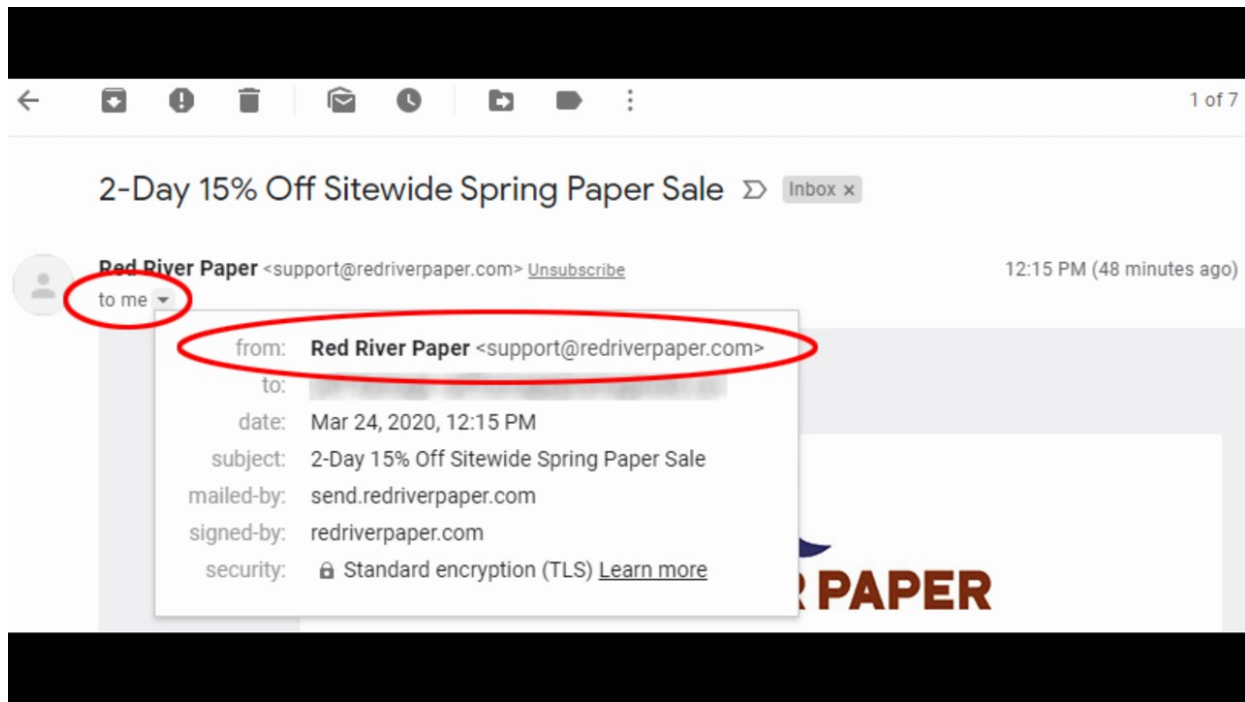
Be suspicious of urgent demands, threats, prizes, secrecy, or unexpected requests for money or credentials.



Video reference: Watch for pressure.

STEP 3 Inspect links and attachments

Hover over links and confirm the real destination. Do not open unexpected attachments.



Video reference: Inspect links and attachments.

STEP 4 Verify and report

Contact the sender another way when unsure, then use Gmail's Report phishing option or contact Technology Services.



Video reference: Verify and report.

Need help?

If you are unsure whether a message, sign-in, extension, or request is safe, stop and submit a Technology Services work order at <https://wcps.freshdesk.com/>.