Spot the Scam

5 Signs of a Phishing Email or Fake MFA Prompt

1

Urgent Pressure or Threats

Demands to act now, like “account locked in 1 hour” or “wire the money today,” are meant to rush you past checking.

2

Lookalike Sender or Link

One small spelling change in an email or web address. Hover before you click and check the real domain.

3

Unexpected MFA Prompts

A sign-in approval request you did not start. Deny it right away and report it.

4

Requests for Passwords or Codes

Real IT support will never ask for your password or a sign-in code by email, text, or phone.

5

Strange Attachments or Sign-In Pages

Surprise invoices, shared files, or Microsoft 365 sign-in pages not on login.microsoftonline.com.

When in Doubt, Pause and Verify

- **Don’t click** links or open attachments you weren’t expecting.
- **Don’t approve** a sign-in prompt you didn’t start.
- **Call back** on a number you know, never one in the message.
- **Report it** to your IT contact, even if you already clicked.

RESOLVEIT 365

Made by Resolve IT 365

resolveit365.com · 858.331.6713