Phishing Awareness

side

Security

Hackers are targeting Real Estate Professionals

Attackers are going after real estate professionals directly, and their messages are getting harder to tell apart from the real thing. Many impersonate a team, brokerage, title company or familiar contact by name to earn your trust. Here's how to spot a suspicious message and what to do when one lands in your inbox.

BEFORE YOU CLICK



Check the real sender address

The display name can say anything, so look at the address behind it. A message that appears to come from your own team or a trusted partner may be sent from an unfamiliar domain.

> Example: **yourteamname@goagle.com** instead of your team's real domain



Pressure to act now

Phrases like “urgent,” “expiring today” or “closing is at risk” are designed to rush you past the moment where you'd stop and think.



Unexpected links, files or e-sign requests

Be cautious with a shared document or signature request you weren't expecting, especially one that asks you to sign in.



Changed payment or wire details

Treat any request to update wiring instructions or send money as a red flag until you verify it by phone.

WHAT TO DO



Verify another way

Call the person at a number you already know. Never use a phone number or link that came in the email itself.



Report it

In Gmail, open the message menu and choose “Report phishing.” Every report helps us (and Google) block the sender for everyone.



Clicked something? Tell us fast

Contact Side Support right away. Speed matters most, and there's no blame or shame because we've all clicked something we shouldn’t have.

Side Support: help@side.com

Questions about a message? When in doubt, don’t click. Forward it to Side Support and we’ll take a look.