



Is your email closing-safe?

A 3-minute self-check for title offices and real estate brokerages. Check Yes or No for each statement, then count your Yes answers. Wire fraud starts with email, so that's where to look.

	YES	NO
1 Multi-factor sign-in is on for every email account, including the owner's, assistants' and shared inboxes.	☐	☐
2 Someone checked every mailbox for forwarding and inbox rules in the last 30 days.	☐	☐
3 Buyers and sellers are told in writing, at the start, that wiring instructions will never change by email.	☐	☐
4 Staff confirm wiring instructions by calling a number they looked up themselves, never one from the email.	☐	☐
5 Your email domain has a DMARC record set to quarantine or reject, so others can't send as you.	☐	☐
6 You would be alerted if someone registered a lookalike of your domain (for example, yourbrokerage-title.com).	☐	☐
7 Former employees' and agents' email accounts are shut off on their last day.	☐	☐
8 Everyone who handles closings has had phishing or wire-fraud training in the last 12 months.	☐	☐
9 Your team knows to call the bank's fraud line within minutes if money goes to the wrong account.	☐	☐
10 You have insurance that covers funds-transfer fraud (social engineering), and you know the limit.	☐	☐

YOUR SCORE _____ Yes answers out of 10

9–10

Closing-safe

Keep it up. Recheck every quarter.

6–8

Gaps attackers look for

One missing control is all it takes.

0–5

High risk

Fix this before your next closing.

U.S. real estate fraud losses rose 58% in 2025, to \$275 million. Source: FBI Internet Crime Complaint Center, 2025 Internet Crime Report.

Scored under 9? Book a Closing Security Check.

A local specialist checks your email setup and sends a written fix list. \$750 for up to 10 users.

Ed Dupuy · Sealbridge Security · sealbridgesecurity.com

