NC REALTORS®

Member Safety & Fraud Prevention Series

Spotting Online & Phone Scams: A Safety Guide for Realtors

Washington-Beaufort County Board of REALTORS®

Real estate professionals are prime targets for scammers because you routinely handle large sums of money, personal client data, and urgent, time-sensitive transactions. This sheet covers the most common online and phone scams affecting NC agents and brokers, the red flags to watch for, and what to do if you're targeted.

1. Common Scams Targeting Realtors

Scam Type	How It Shows Up	Red Flags
Wire Fraud / Closing Scam	Email appears to come from the attorney, or lender with 'updated' wiring instructions right before closing.	Urgent tone, last-minute change to account/routing numbers, slightly altered sender email address.
Business Email Compromise	A hacked or spoofed agent/broker email requests earnest money or commission be sent to a new account.	Request bypasses your normal process, poor grammar, reply-to address differs from display name.
Phone/Caller ID Spoofing	Caller ID shows a local NC number, your MLS, closing attorney's office, or a bank, but it's not who they claim to be.	Caller pressures immediate action, asks you to 'confirm' info they should already have, refuses to let you call back on a verified number.
Fake Buyer / Rental Scam	A 'buyer' overseas or unavailable to meet asks you to accept an overpayment and wire back the difference.	Overpays with a check, urgent request to refund the excess, avoids in-person meetings or video calls.
Phishing Texts/Emails (Smishing)	Message claims to be from Docusign, Dot Loop, Zip Forms, MLS, NC REALTORS®, or your brokerage asking you to 'verify' your login.	Generic greeting, shortened/mismatched links, urgent account-suspension language.
Vendor / Home Repair Impersonation	Caller poses as a contractor, inspector, or utility company tied to a listing, asking for payment or access info.	Unsolicited call about a property, requests gift cards or wire payment, can't be verified through the actual company.

2. Red Flags in Any Suspicious Call or Message

- **Urgency and pressure.** "This must be done today or the deal falls through." Scammers rely on rushing you past normal verification steps.
- **Last-minute changes to payment details.** Any change to wiring instructions, account numbers, or payee names should be treated as suspicious by default.
- **Requests for unusual payment methods.** Gift cards, cryptocurrency, or wire transfers to personal accounts are hallmarks of fraud.
- **Mismatched contact details.** The email domain, phone number, or reply-to address doesn't quite match the organization's real one (e.g., an extra letter or different domain).
- **Requests to bypass normal channels.** A client, colleague, or vendor asking you to communicate only by text or a new email "for this transaction only."

- **Unusual grammar or formatting.** Awkward phrasing, generic greetings (“Dear Customer”), or logos that look slightly off.
- **Requests for sensitive data.** Social Security numbers, bank logins, or MLS credentials requested by phone, email, or text.

3. Protective Habits to Build into Every Transaction

- **Verify wiring instructions by phone — always.** Call the closing attorney using a number you already have on file (not one provided in the email) before sending or accepting any funds.
- **Confirm changes independently.** If any party requests a change to payment details, call them back using a previously verified number to confirm before acting.
- **Use secure, established channels.** Keep sensitive documents and financial instructions inside your brokerage's secure transaction platform rather than plain email.
- **Slow down under pressure.** Legitimate closings rarely require instant, unverified wire transfers. Treat urgency itself as a warning sign.
- **Check the sender, not just the name.** Hover over or tap the sender's email address to confirm the full domain matches exactly.
- **Enable multi-factor authentication.** Turn on MFA for email, MLS, and transaction management accounts so a stolen password alone isn't enough to get in.
- **Educate clients early.** Tell buyers and sellers at the start of a transaction that you will never change wiring instructions by email or text, so they know to be suspicious if it happens.
- **Trust your instinct — hang up and call back.** If a call feels off, end it and call the organization back using a number from their official website or your own records.

If You Suspect You've Been Targeted

• Stop all communication and do not send any funds or information.
• If money has already been sent, contact your bank immediately and request a wire recall.
• Notify your broker-in-charge immediately.
• File a report with local law enforcement and keep records of all communications.
• Report phishing emails or texts to the FTC at reportfraud.ftc.gov.

4. Quick Reference: Verify Before You Trust

- Does this request involve money, payment details, or sensitive data? Verify by phone using a known number.
- Is there pressure to act immediately? Slow down and confirm independently.
- Does the sender's email or phone number match exactly what you have on file? Check character by character.
- Would an attorney’s office, loan officer or brokerage normally ask for this by text or email? If not, don't respond — call instead.

This information sheet is provided for general awareness and does not constitute legal advice. For transaction-specific concerns, consult your broker-in-charge.