

# DON'T GET HOOKED!

## How to Recognize and Avoid Phishing Attacks

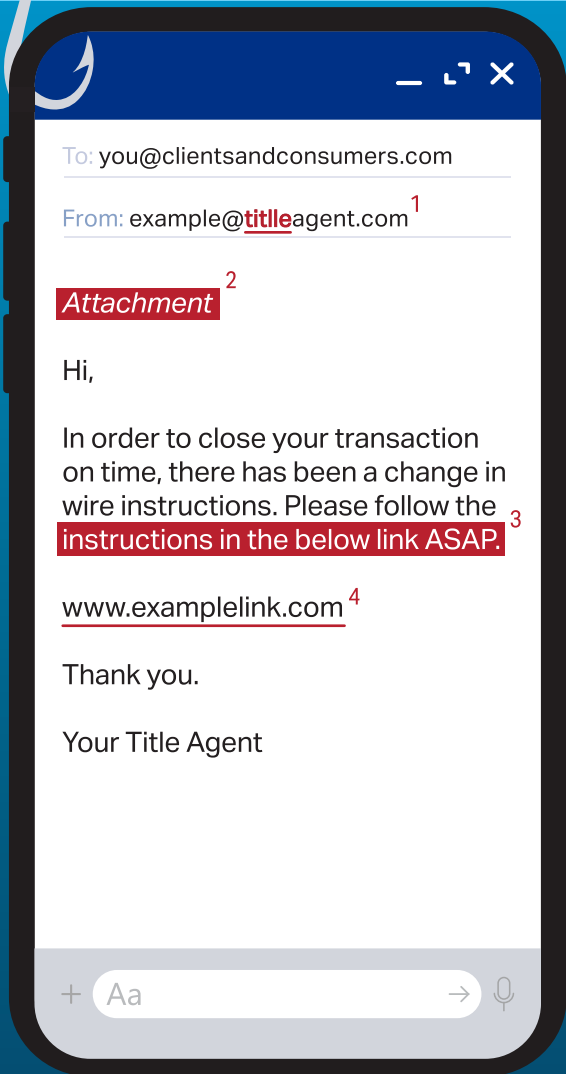


Phishing is a tactic used by cybercriminals to trick you into clicking on a link or giving up sensitive information through emails, text messages and phone calls.

In order to accomplish their mission, cybercriminals will also impersonate a known and trusted source - a tactic known as spoofing. It's very important not to take the bait!

So how can you avoid getting caught hook, line and sinker? Watch out for these red flags:

- 1 Misspellings in the email address, subject line, or body.
- 2 An unexpected attachment.
- 3 Demand for immediate attention.
- 4 A link you can't verify (hover over to check). Always call to verify before clicking an unfamiliar site.



### Think before you click, send or speak.

- Is the message or call expected?
- Can I verify the sender or caller?
- Does the request(s) make sense?

If you become a victim of identity theft, report it to the Federal Trade Commission. They can assist you with a recovery plan of action. Visit: [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (438-4338).

All-Virginia Title & Escrow  
530 Main Street, Suite 292  
Danville, VA 24541  
O: 434.791.4060  
F: 434.791.2133  
[www.allvirginiatitle.net](http://www.allvirginiatitle.net)