Fidelity National Title
Trusted everywhere,
every day.

Important Reminder

About Defending Against Phishing Attacks & Scams During the COVID-19 Pandemic

In the midst of stress and distraction, please remain on alert for possible phishing emails and scams that may be sent based on the coronavirus (COVID-19).

Cyber attackers may send emails with malicious links or attachments to fraudulent websites to trick individuals into providing sensitive or confidential information. Please **exercise extreme caution** in handling any emails with COVID-19-related subject lines, attachments, or hyperlinks. Use caution in response to social media pleas, texts, or calls related to COVID-19 or ANY suspicious topic.

A FEW WAYS TO SPOT WHAT COULD BE A FRAUDULENT EMAIL:

- Were you expecting the email?
- Does something look off to you? Is the wording, graphics or spelling causing suspicion? Trust your instincts and don't click until you confirm!
- Are you being asked to link to an official-looking sites requesting sensitive data. These spoofed sites are often very convincing, so before revealing personal information or confidential data examine the site and reach out to a known contact to confirm authenticity.
- "Verify your account." These messages spoof real emails asking you to verify your account with a site or organization. Always question why you're being asked to verify. There is a good chance it's a scam.
- Do you recognize the sender's email address? Hover over the email address to see if the sender is masking his or her identity. Compare the email address carefully with the address you know is authentic.

It only takes a click to result in a data breach & it's always better to be safe than sorry!
Be vigilant and informed to protecting against cyber attacks.

And remember:

ALWAYS CALL BEFORE YOU WIRE!