OLD REPUBLIC TITLE

EMAIL SCAMS TARGET CLOSING FUNDS

Email phishing scams attempt to trick people into clicking a link, opening an attachment or responding to a message so criminals can exploit personal information. The Federal Trade Commission and the National Association of REALTORS® have warned consumers of an email phishing scam in which hackers compromise the email accounts of buyers and/or sellers, pose as a trusted real estate agent or title insurance company, and attempt to fool their targets into wiring closing funds into the hacker's own account.

Old Republic Title® is committed to protecting clients, and takes security measures to prevent unauthorized access to its network. Criminals know secure networks are difficult to access, so instead, they target consumers' popular web-based email, which is more vulnerable to cyber attacks.

THE SCAM

Once hackers gain access to a buyer or seller's unsecure email account, they look for the source of an upcoming financial transaction (e.g. oldrepublictitle.com). Hackers use this information to register a fake domain name that mimics the domain name of the legitimate source, making spelling changes so subtle that most people would never notice (e.g. oldrepublictltle.com). The hackers then use the fake domain name to email false wire transfer instructions to their target. If the consumer responds with financial information, he or she could lose significant sums of money.

WIRE FRAUD NOTICE: If you receive wiring instructions from Old Republic Title, including any changes, you should call the escrow officer to verify the instructions before wiring any funds.

EASY TIPS FOR AVOIDING EMAIL PHISHING SCAMS

1. Be wary of emails that are unusual, unexpected or require a change in routine. Look carefully for grammar or spelling mistakes, and be leery of those that use threats if swift action is not taken.
2. Avoid conveying sensitive information through unsecure email accounts or websites, and be aware that information you share on social networks can be used by scammers.
3. Do not click on links in emails. Instead, hover your mouse over a link to view its true web address. If it's different than what displays in the email, beware.
4. Create "fake" answers to password recovery questions; "real" answers can be discovered. Write down the false answers to help you remember them.
5. If anything in an email – even one from a trusted source – seems suspicious, call the sender using a previously known or verifiable phone number. Never reply to the email or information in the message.