How Can I Protect Against Wire Transfer Scams?

Since bank wires remain the preferred method of closing escrow on a real estate transaction, the best protection is to be overly cautious.

Question: I am buying a house and have been warned about the various scams, especially those involving wires. I spoke with the closing agent, and they will not accept a check to buy my new home. How can I protect myself when sending a wire? — Nick

Answer: Whenever large sums of money are involved, scammers seem to come out of the woodwork. Throughout my career, there seems to be a never-ending variety of scams to watch out for.

Despite the dangers, bank wires remain the preferred, and often only, method of closing escrow on your real estate transaction. This is partly because checks, even certified or bank checks, can be stopped or easily counterfeited.

“Hard” funds, such as those sent by wire transfer, are required at closing so the escrow agent can pay the seller, lender, and other parties without delay.

Due to the large sums involved, criminals are constantly developing methods to trick people into redirecting the wire transfer to their accounts

rather than the escrow agent. A persistent scam involves the fraudster hacking into one of the participants' unsecured email accounts.

While many parties involved will have secure accounts, it only takes a careless mistake by any of the many people involved to expose someone's account.

Once the criminal has access, they lie in wait, monitoring emails until an opening presents itself so they can spring their trap. The criminal will then send a fake email that looks like it came from your agent or the closing company containing fraudulent wiring instructions.

Even though most of these fraudulent emails contain telltale inconsistencies, they are often missed in the excitement and flurry of activities leading up to the closing.

The best way to protect against this scam is to be cautious, almost to the point of being paranoid. If possible, deal with your closing and escrow agent in person. If this is not possible, call them using an independently verified phone number, not the one listed on an unverified email, which could also be a fake email from the fraudster.

Do your homework and insist on only dealing with professionals who take security seriously.

Because the information perpetuating this scam can come from anyone involved email account, you are only as secure as the weakest link. Ask the people involved in your transaction what precautions they take to protect you.

Sadly, because criminals are constantly changing tactics, there is no perfect protection, so you need to do all you can, paying attention to the details and following up on anything that looks suspicious.

By Gary M. Singer