This sophisticated scheme is growing fast, costing consumers and companies big money. Here's how to prevent becoming a victim of a bogus wire transfer.

How it works

Bad guys research the names, phone numbers and email addresses of executives, employees or consumers who have access to money such as a corporate bank account or a consumer's real estate closing funds.

The bad guys, often involved with organized crime, send emails and make phone calls pretending to be an executive, an attorney or someone in authority. They instruct the recipient to wire money to the bad guys' account.

The victim is convinced the urgent communication (often labeled "confidential") is legitimate, wants to do the right thing and follows instructions to wire the funds immediately.

Funds are transferred from the victim's bank account into a bank account controlled by the organized crime group. Once the wire transfer is made, the victim usually has no recourse to get the money back.

How to stay safe

Slow down! Just because a communication is labeled "Urgent!" and appears to come from someone in charge doesn't mean you should act right away. Take time to double-check that the email or phone call is legit.

Remember, bad guys know how to "spoof" an email address so it appears to be coming from someone important. Double-check by contacting the company or executive directly, not using contact information contained in the email.

Know that documents, invoices or requests for an employee's W-2 or other sensitive information that appear to come from a trusted colleague, attorney, vendor or executive may look real, but could be fake.

If you are the victim of wire fraud, contact the financial institution immediately to see if the funds transfer can be reversed. Talk to the bank's financial crimes division to request that the recipient's account be frozen.

Sources: FBI, law.com, Realtor Daily News, Washington Post, Barkly, Trend Micro, TechTarget