Wire Scams Are Big Business
Learn how to spot common wire transfer scams

Wire transfers are a fast, easy way to send money to individuals and businesses. However, because wire transfers are an immediate form of payment and typically irreversible, they are also frequently used in fraud schemes. According to the Federal Trade Commission, roughly $314 million was lost to wire transfer fraud in 2020.

To help protect yourself from wire transfer fraud, here are some flags to watch out for:

REAL ESTATE WIRE SCAMS

Real estate wire scams target people in the closing process of buying or refinancing a home. A scammer gains access to a legitimate email account to impersonate a realtor, escrow officer, attorney, or lender and then provides fraudulent wiring instructions to funnel the money directly into the scammer's account.

To help avoid this scam:

- Know what to expect before closing on a loan by confirming the process with your lender. If you receive a last-minute change or urgent request to wire money, contact your mortgage consultant.
- Before wiring money, confirm instructions with your mortgage consultant or title company by calling a phone number you trust. Do not call a new number or respond to an email with new instructions.

How the scam works:

These scams target customers in the process of closing on a home purchase or refinance. Scammers are often successful because they gain access to legitimate email accounts in order to impersonate realtors, escrow officers, attorneys, or lenders.

With the closing details, scammers can craft an email that looks very authentic, down to the email address, signature and company logo. This phishing email provides false wiring instructions, directing the money to be transferred to a different account that is controlled by the scammer.

These emails often include an urgent request to send the money immediately or the deal will fall through or the closing date will be postponed. The email may even appear

to carbon copy (CC) others involved in the transaction; however, at closer inspection, those email addresses are altered.

How to help protect yourself

- Don’t be rushed: Know what to expect as part of the closing process. Although closing dates may change, there is typically not a last-minute requirement that you send the money to avoid a change in date or risk losing the property.
- Confirm the intended recipient: Be highly suspicious of any communication stating your wiring instructions have changed. Before wiring funds, confirm instructions with your mortgage consultant or title representative by calling a phone number you trust. Do not call a new number or respond to an email with new instructions.

How to take action if this happens to you

- If you wired money through your Credit Union, request a wire recall immediately. Because wire transfers are typically irreversible, you may not be able to get your money back.
- If you used a money transfer service, call the company’s complaint line right away.
- Report the incident to the Federal Trade Commission and the FBI’s Internet Crime Complaint Center as soon as possible and provide all of the incident details. If your Credit Union asks for a police report, give them a copy of your report to the FBI.

TECH SUPPORT / COMPUTER REPAIR SCAMS

Tech support scams happen when someone contacts you claiming to be from a well-known technology company and requests remote access to your computer.

Sometimes the caller says they have identified a problem and offers to fix your computer for a fee. If you give them access, they may install malicious software on your computer to track and steal your personal or financial information.

Other times, the scammer offers a "refund" for a discontinued service or an accidental overcharge. If you give them access to your online banking, they will make it appear as if they're sending you a refund, but they're actually transferring money from your own

accounts. Often, the refund is for much more than promised (e.g., $40,000 instead of $400), so the scammer makes a plea for you to send the extra money back so they don't lose their job. They may ask you to wire money to a foreign country, purchase gift cards, or mail cash.

You receive an unexpected call or pop-up message on your computer warning of an issue, such as a virus or other malware. The caller or pop-up claims to be from tech support and asks for access to your computer to fix the issue or offer you a refund. Typically, the scammer will ask you to type a specific command to enable this access. Once they have control of your computer, they may require payment for technical assistance, install malicious software, change settings to leave your computer vulnerable, or ask you to log on to your Credit Union account to steal your financial information.

To help avoid this scam:

- Never give control of your computer to anyone who contacts you. If you receive a call about a computer problem, hang up. If you suspect something is wrong with your computer or believe the scammer obtained access to it, bring it in person to a reputable company for a malware check.
- Don't trust phone numbers provided to you in an email, voicemail, or pop-up ad. If you want to call the company, use the customer service number on their official website. Note: Scammers sometimes purchase ads and create fake customer service websites that will show up on search results.
- If you are asked to wire money from a recent deposit or overpayment, discuss the situation with a banker or trusted friend or family member. Be truthful about the situation, since many scammers direct you to lie about why you're sending the money.
- Review your account activity to spot signs of fraud, such as an online transfer from your own savings, credit card, or home equity line of credit. If you're unsure of the descriptions used for a transaction, ask a banker to help since many scammers will add a memo to make the transfer appear legitimate.

What you can do

- Never give control of your computer to anyone who contacts you.

- If you get an unexpected or urgent call from someone who claims to be tech support, hang up. It’s not a real call.
- Don’t rely on caller ID. Scammers can spoof the name of a company to make the call seem legitimate.
- If you get a pop-up message warning you about a computer problem or telling you to call tech support, ignore it.
- If you’re concerned about your computer, call your security software company directly using the number on the company’s website.

ONLINE SHOPPING SCAMS

Online shopping scams can be difficult to spot because scammers often create realistic websites and social media ads with great deals, fake assurances, and bogus warranties for their products. Typically, the scammer requests payment through a mobile payment app or wire transfer because they are usually irreversible. If you wire money to the scammer, you'll never receive the product and likely not get your money back.

To help avoid this scam:

- Know that anyone can set up a realistic website and social media ad. Scammers will sometimes purchase ads to direct you to their website, so research the seller or product before you buy.
- Watch out for deals that are too good to be true. A deep discount could be the sign of a scammer trying to lure you in, only to tack on additional fees once you make the first payment.
- Don't pay for online products with a wire transfer or mobile payment app. Use a credit card, when you can.

OTHER WIRE TRANSFER SCAMS

- **Foreign business or investment scam**: You're approached with an offer to fund a lucrative investment or business opportunity, usually in another country. You're directed to act quickly and keep the deal a secret, especially if questioned by your Credit Union when sending the wire.
- **Family emergency or grandparent scam**: You receive an urgent call or email from someone claiming to be a friend or family member who needs money for

an emergency. To appear legitimate, they may provide details (pulled from social media) about your friend or relative in need.

- **Romance scam**: You meet someone, typically through an online app or social media site, and begin a relationship. Your online interest starts professing their love for you and then begins to ask for money to help with costs such as medical bills or travel expenses to visit you.

If you're a victim of a wire transfer scam, report it to your Credit Union immediately. You can also report the scam to the Federal Trade Commission at ReportFraud.ftc.gov

For more information please review “Before You Wire Money” published by the Federal Trade Commission:

https://www.consumer.ftc.gov/articles/before-you-wire-money