Wire Transfer Safety Tips

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 a payment form preferred by fraudsters.

Never wire money to anyone:

- You haven't met in person (or businesses that you don't have an established relationship with and you have verified the request to be legitimate)
- who says they work at a government agency like the IRS or Social Security Administration
- who pressures you into paying immediately
- who says a wire transfer is the only way you can pay
- who tries to sell you something over the phone

Protect your confidential information - never give out personally identifying information to someone contacting you by email, text message, or phone. Scammers will often try to convince you to give out your bank account number, social security number, debit card number, credit card number, one time passcode, or account balances. They then use that information to impersonate you or attempt to access your account and send funds to themselves from your account.

If you are a business, implement a verification process for your employees to follow, making sure you are transferring funds to a legitimate source and that the wire transfer request is truly authorized. When verifying a request, be sure that is done verbally and not by email or text message. A common tactic that is used by scammers is they will pose as a manager or executive at a business, create a fake email address to go along with it, and email an employee asking for a wire transfer. Another common tactic scammers use is to pose as a legitimate vendor of the business and request a change in payment instructions so that the scammer receives the payment instead of the legitimate vendor.

BRYANT BANK

SPOT THE SCAM

Here are some common ways scammers try to convince people to wire money:

Fake Check Scams

Someone sends you a check and tells you to deposit it. They tell you to wire some or all of the money back to them or to another person and will put pressure on you to do that immediately. In a few days, the check you deposited will be returned to the bank and debited from your account balance. You will most likely not be able to recover any funds that you sent to the scammer.

Scammers make up lots of stories to try to convince you to deposit a check and wire money:

- They say you've won a prize and need to wire money back to cover taxes and fees.
- They say it's part of a mystery shopping assignment to evaluate a wire transfer service.
- They overpay you for something you're selling online, then ask you to wire back the extra money.
- They say you got a job you applied for online and they send you a check to buy supplies but ask you to wire back part of the money.

Romance Scams

Romance scammers create fake profiles on dating sites and apps. They strike up a relationship with you and work to build your trust, sometimes talking or chatting several times a day. Then, they make up a story — like saying they have an emergency — and ask for money. A romance scammer might also contact you through social media sites.

Family Emergency Scams

You get an unexpected call from someone who pretends to be a friend or relative. They say they need cash for an emergency and beg you to wire money right away. They might say they need your help to get out of jail, pay a hospital bill, or leave a foreign country. They often ask you not to tell anyone in your family. Their goal is to trick you into sending money before you realize it's a scam.

Apartment Rental Scams

You respond to an ad for an apartment with surprisingly low rent. Before you've even seen the apartment, you apply and are told to wire money — maybe for an application fee, security deposit, or the first month's rent. After you wire the money, you find out that there is no apartment for rent, or that the scammer put their contact information on someone else's photo or rental ad. Scammers run a similar scam with vacation rentals.

Real Estate 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.

BRYANT BANK

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 to avoid losing the property, contact your lender.

- Before wiring money, confirm instructions with your lender or title company by calling a phone number you trust. Do not call a new number or respond to an email with new instructions.

Tech Support 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 to 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.

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, disconnect it from the internet immediately and bring it 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 in 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.

- Set up alerts in your online banking to notify you when certain activity occurs. You can set up alerts in online banking by selecting the account from your dashboard and then selecting Alert Preferences or from the Menu by selecting your name › Settings › Bryant Bank › select the account and Add alert.

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.

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

BRYANT BANK