Be Aware

Together, we can fight fraud

You are our partner. While Western Union works hard to help prevent fraud, we believe that fraud prevention is everyone's responsibility. Your best defense is to be aware, educate yourself and use good judgment.

Don't fall victim: Learn how to spot the warning signs of a scam or scammer before it's too late.

General warning signs

- Scammers have many excuses why they can't meet you in person. They list numerous reasons why they need money and always seem to be in trouble.
- Scammers claim they have been in an accident, are in the hospital and their medical bills have to be paid in full before they can leave.
- Scammers will tell you to send the money in the name of a friend or family member to verify you have funds or to act as an escrow until you receive the purchased goods or services.
- Scammers need money because they were mugged and their money, passport, and ID were stolen while traveling.
- Scammers continue to ask for money for a plane ticket to see you, or to "float" them until payday.
- Scammers claim they've been in an accident or have a sudden family tragedy right before boarding a plane to meet you, or are held up in Customs and needs money for their release.

Emails and Phishing

Passwords and IDs hold high value with cyber criminals. Sending phishing emails to a lot of random email addresses is one easy way scammers steal information from unsuspecting people.

It's probably a phishing email if:

- The email is poorly written with misspellings and incorrect grammar, or a familiar company name is misspelled.
- Your name isn't in the "To" line. This email has likely been sent to thousands of people.
- The sender's email address is suspicious; it might have a familiar company or government organization that is misspelled.
- The email doesn't use your name. Any financial institution you have an account with knows your name. Email beginning with "Dear valued customer," "To Whom It May Concern," or even "Hello," could signal a scam.
- The URL is a fake. Hover over the "click here" or "take action now" link with your mouse. If you see a strange URL instead of a legitimate company website, don't click.
- You're informed that there's a security breach on your account, and if you don't take the action recommended in the email, your account will be temporarily suspended.
- The email asks for your personal, credit card or online account information or takes you to a website that asks for it. Legitimate companies don't usually do that.

If you receive a suspicious email:

Don't open it; delete it immediately.

Don't follow any links in the email - even if its to "unsubscribe" from the sender - or open any files attached to it.

Western Union wil never send you an email asking for your ID, password or personal information.

If you're not sure whether an email is from Western Union or not, don't open any links, click on any attachments, or provide any passwords or user IDs.

Forward the email to spoof@westernunion.com and then delete it.

Read more at https://www.westernunion.com/au/en/fraudawareness/fraud-be-aware.html#YDiW6xuydEz413sR.99