

May 2026 – Watch Out for Fake Friend Requests

The internet is full of attempts by individuals to use relationships to acquire money from unsuspecting victims. Some scammers like to play on a person's sympathies or natural compassion, while others rely on a person's desire to help a known friend quickly and not leave them in the lurch. Still others are hoping that their intended victim will not verify claims of payments or quick sales. Below are listed some of the most common ways thieves attempt to acquire your money online, as well as some simple steps that you can take to safeguard yourself from these scams.

Here are some ways that people get tricked into accepting a fake payment request from a scammer:

- **“Accidental payment” scams** – They send a fraudulent payment and ask you to refund it, leaving you responsible when the original payment bounces.
- **Fake sales offers** – They promote deals that look very cheap, but they take your money without ever delivering the items.
- **Donation pleas** – They make up stories about personal struggles or create fake charities to take advantage of your kindness.
- **Investment opportunities** – They promise quick cash transfers with high returns, but these returns eventually disappear.
- **Requests to send money quickly** – They create an urgent situation that needs immediate financial help.

How to Protect Yourself

- **Only accept people you know** – Keep your payment apps like your wallet. Only connect with people you know and trust.
- **Make transactions private** – Go into your settings and change your default transaction privacy to “Private.” This prevents strangers from snooping on your financial habits.
- **Avoid outside links** – Never click on links sent by strangers, even if they claim it leads to a receipt or tracking number.
- **Ignore "accidental" payments** – Do not send money back to fix a mistaken payment. Instead, contact the support team of the payment platform and ask them to officially reverse the transaction.
- **Verify offline** – If a friend asks you for money because of an emergency, call or text them at their real phone number to make sure it's truly them.
- **Strengthen your account** – Use strong, unique passwords and enable two-factor authentication (2FA) immediately.
- **Report suspicious activity** – Use the app's reporting tools to flag strange accounts, helping protect yourself and other users.

SOURCE: Scambusters.org

