When a Friend Request Isn’t a Friend

Social media is a great way to stay connected with family, old classmates, and neighbors. But not every friend request is friendly, scammers are creating fake profiles designed to trick you.

🎭 How the Scam Works

- You get a friend request from someone who looks familiar — maybe they use the name of someone you already know.
- Once you accept, they can:
    - Send you **phishing links** or scam messages.
    - Pretend to be your friend and ask for **money**.
    - Collect personal details (birthdays, family names, addresses) from your posts.

Some even copy a real friend’s profile picture and name to make it look legitimate.

🚩 Red Flags to Watch For

- A duplicate request from a friend you’re already connected with.
- Very few photos, posts, or friends on their page.
- Messages that immediately ask for help, money, or gift cards.

✅ How to Stay Safe

- **Verify before you accept.** If you get a duplicate request, call or message your friend outside of social media.
- **Check their profile.** If it looks empty or suspicious, skip it.
- **Keep your info private.** Avoid posting sensitive details like your home address or travel plans.
- **Report fake profiles.** Social media platforms have tools to report impersonators.

💡 Bottom Line

Not every “friend” online is who they say they are. Take a minute to double-check before you click accept — because sometimes the nicest-looking profile is just a scammer in disguise.