# Public Info, Private Scams: Card Edition

You receive a text message.

*"Legence Bank Alert: Did you Authorize a payment of $500 today at Walmart in Houston, TX? Reply Yes or No."*

You didn't make the charge – so you reply "No."

Shortly after, you receive a call from someone claiming to be with the bank. They know your name, phone number, and some of your card details. They also mention a card of yours that was compromised a few months ago. It all feels real.

Here's the unfortunate truth: much of the information they're using to build your trust is *publicly available.* The first 6-8 digits of every card (*the BIN*) are no secret, and the last four digits often appear on receipts or even in past data breaches. Add in your name and phone number from the web, and a scammer suddenly sounds a lot like your bank's fraud department.

Once they have your trust, scammers don't need to steal your physical card – they just need you to hand over a few details they're missing. Once they have you convinced that they really are with the bank, they'll ask you to verify your entire card number. Then they'll prompt you for the expiration date and the CVV on the back of the card, or perhaps even a one-time passcode. Once they have those details, scammers can shop online, clone your card, or even connect it to a P2P app and move money from your account instantly. *Either way, it starts with the same trick: using bits of public data to gain your trust.*

**What's Public (and Why It Matters)**

- **BINs (first 6-8 digits of every card):** These identify the card type (Visa, MasterCard, AMEX, etc.) and the bank that issued it. They're not secret – anyone with internet access can find out which bank issued your card in seconds.
- **Last Four Digits:** Often printed on receipts, emails, or found in past breaches. They're easily obtainable by fraudsters.
- **Your Name & Contact Information:** Your details can be pulled from social media, public records, data breaches, or even a simple online search.
- **Common Bank Scripts:** Phrases like "fraud department" or "unusual activity" are commonly associated with finance. Scammers also use tools like AI to generate custom scripts for their specific needs.

**How to Protect Yourself**

- **If someone calls claiming to be your bank, never share codes or full card details.** Legitimate bank employees already have access to your card information, and they won't ask you to share a code you've been sent. *Ever.*
- **Hang up and call back using a number you know is legitimate**. Never trust an inbound call. Even if you have received a call from a real bank employee – they will appreciate and understand using caution.
- **Be suspicious of urgency** – fear and pressure are almost always tools of the scam. *Slow down.*
- **Set up alerts and card controls –** familiarizing yourself with real alerts will help you spot the impersonators quickly. Plus, they'll notify you if someone really does have your information.