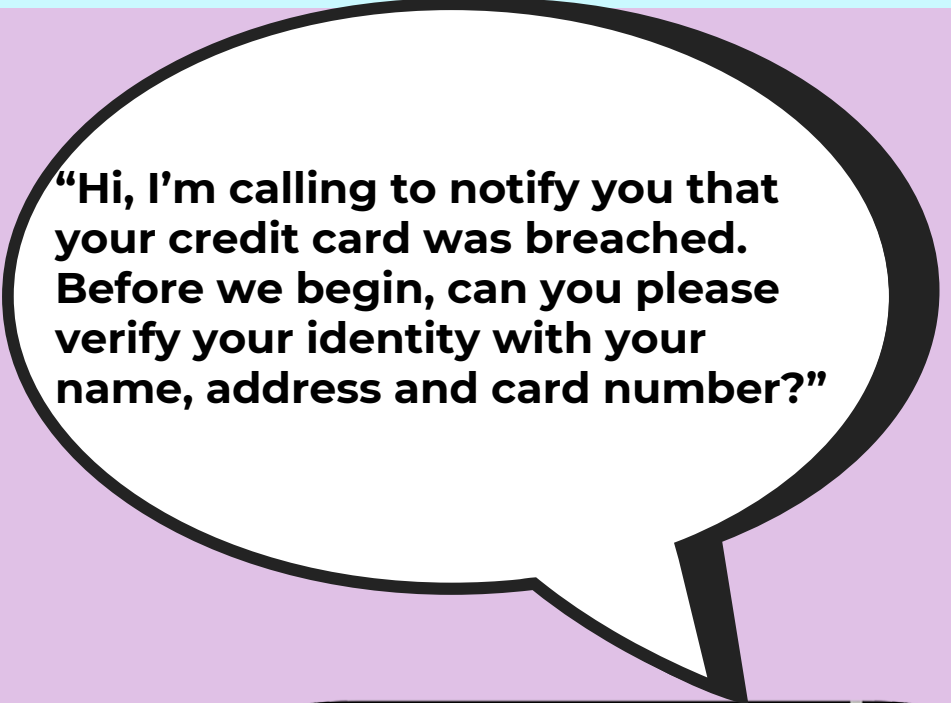


The **RED FLAGS** of Phishing Phone Call Scams

- **Unusual Caller ID:** Don't rely on Caller ID - it can be "spoofed." Legitimate calls from your bank are more likely to display an official phone number or a known identifier. If not, be very skeptical.
- **Scare Tactics or Threats:** Phishing calls rely on a sense of urgency. If the caller pressures you into immediate action or threatens negative consequences, just hang up and call the number on the bank's website, your bank statement, or the back of your bank card.
- **Asking for Personal Information:** Banks will rarely ask for your account number, PIN, or password during a phone call — and will never ask for a one-time login code. Never share such confidential details unless you've called the number on the back of your bank card, bank statement or on the bank's website.
- **Calling you unexpectedly:** Be very skeptical of calls you receive out of the blue. Normally, bank representatives will only reach out if you initiate contact first. Stay safe by ending the call and dialing the number on the back of your bank card, bank statement, or the number on the bank website.



"Hi, I'm calling to notify you that your credit card was breached. Before we begin, can you please verify your identity with your name, address and card number?"

