Social Engineering: How Scammers Make It Feel Real

Social engineering scams have become increasingly sophisticated, preying on people's trust and emotions to steal personal information and money. These scams involve manipulating individuals into divulging confidential information, often by masquerading as a trustworthy entity. The tactics scammers use can be incredibly convincing, making it difficult to distinguish between a legitimate request and a fraudulent one. Here are some of the common techniques that scammers use to make their cons feel legitimate.

• **Impersonating Trusted Entities** – Scammers often pose as representatives of well-known companies, banks, or government agencies. They frequently use *spoofed phone numbers and email addresses* that appear legitimate. For example, they might call you from a number that looks like your bank's customer service line or send an email from an address resembling a government agency. This is intended to lower your guard and increase the chances of you sharing sensitive information.

• **Using Familiar Information** – Scammers often start with information that seems familiar to their targets. For instance, *they might share the first 6-8 digits of your debit or credit card number*, known as the Bank Identification Number (BIN). *These digits are not secret* and are consistent for all cards issued by the same bank. By sharing this information, scammers create an illusion of having access to your full card details, making their requests for additional information even more convincing.

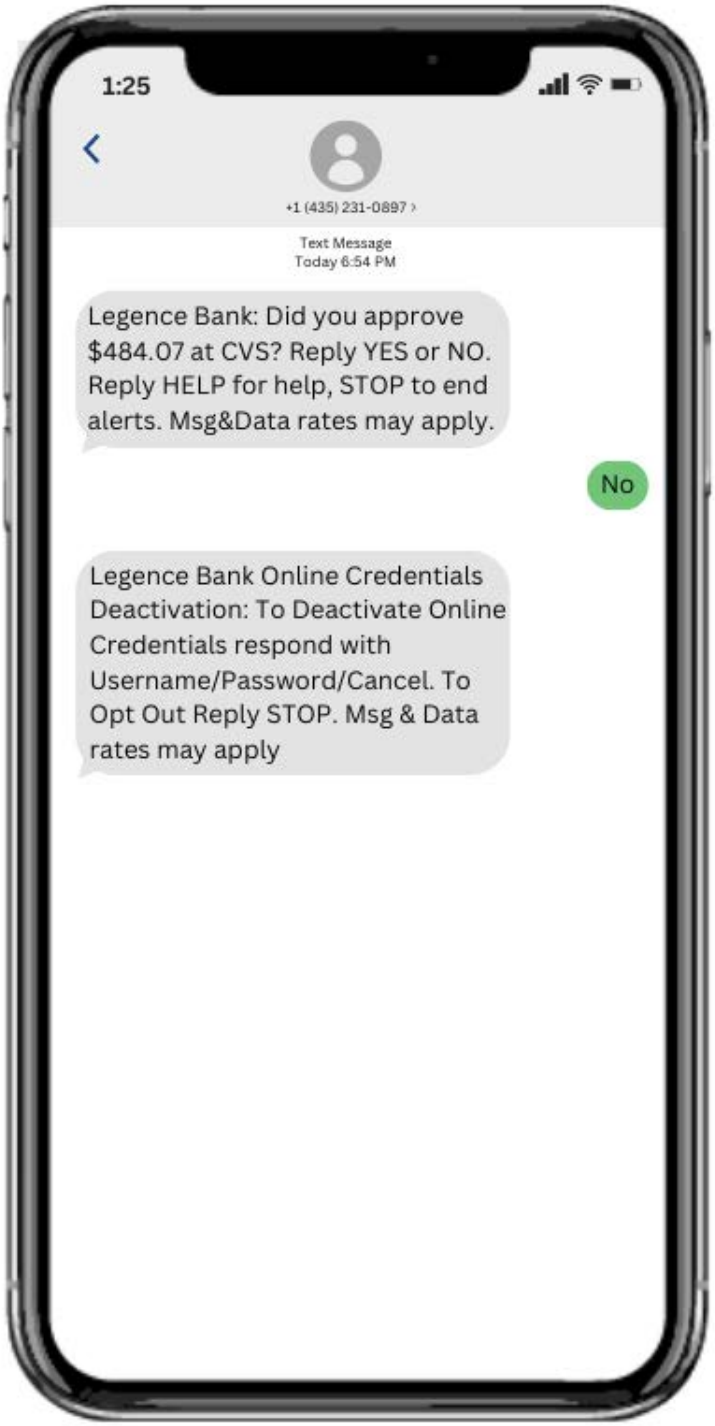
• **Creating Urgency and Fear** – Creating a sense of urgency is a classic tactic. Scammers might claim that your bank account has been compromised and needs immediate action, or that you owe back taxes and face arrest if you don't pay immediately. This fear and urgency pressure you to act quickly without thoroughly thinking things through or verifying the information first.

• **Mimicking Official Language and Format** – Scammers often use language and formats that mimic official communication. *Emails might include logos, formal language, and even disclaimers that appear legitimate.* Phone calls typically follow scripts that sound professional and convincing. By replicating the look and feel of real communication, scammers make it difficult for you to distinguish between genuine and fraudulent messages.

• **Sharing Partial Information** – To gain your trust, scammers might share partial information about you that they've obtained from other sources. This could include *the last four digits of your Social Security number, your home address, or even the names of family members*. By providing these details, they create an impression of legitimacy and encourage you to provide the missing pieces of information they need to commit fraud.

• **Leveraging Social Media Information** – Scammers can gather a lot of personal information from social media. They might use details like *your job title, recent vacations, or family members' names* to craft convincing stories. For example, they might pretend to be a colleague needing urgent help or a friend stuck in a foreign country. The personalization based on your online presence makes their stories more believable.

By understanding these tactics and staying vigilant, you can better protect yourself against social engineering scams. Always verify unsolicited requests, be skeptical of urgency, limit information sharing, use security measures like multi-factor authentication, and stay informed about popular scams. Slow things down and verify the situation before taking any action.



The above image is a real life example of a scammer text message. This scammer is using most of the tactics listed above; **impersonating a trusted entity, using familiar information, creating urgency and fear, mimicking official language and format, and sharing partial information.**