HOW SOCIAL ENGINEERS ATTACK

Social engineers are essentially con artists; they manipulate situations and take advantage of human nature. Social engineering attacks have a common motive: to trick people into taking an action or revealing sensitive information.

These attacks aren't always about a short-term gain. In many cases, social engineers attempt to build a relationship over time, creating a foundation of trust before striking. And there are many methods scammers might use to try to fool their target: YOU.

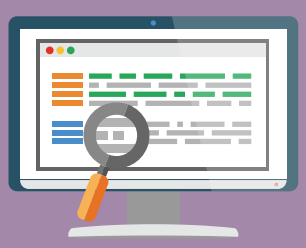
Report suspicious emails to abuse@bankofthewest.com

You Can Stop Social Engineers in Their Tracks

Social engineers count on one thing: your buy-in. If you don't fall for the bait, the scam won't succeed. Keep these tips in mind:

Verify people are who they say they are. It's particularly easy to pretend to be someone else in a faceless medium, like emails, text messages, and phone calls.

Don't take things at face value. Malicious websites, ads, communications, and social profiles often seem safe on the surface.



Be aware of your surroundings. Shield passwords, PINs, and sensitive data from prying eyes. Don't let unauthorized visitors sneak into secure areas.

BANK OF THE WEST
BNP PARIBAS