

Social Engineering: Hacking the Human, and How to Make It Harder

Mon, Aug 10, 4:00 PM EDT · <https://scottslab.io/posts/social-engineering-tactics-and-defenses>



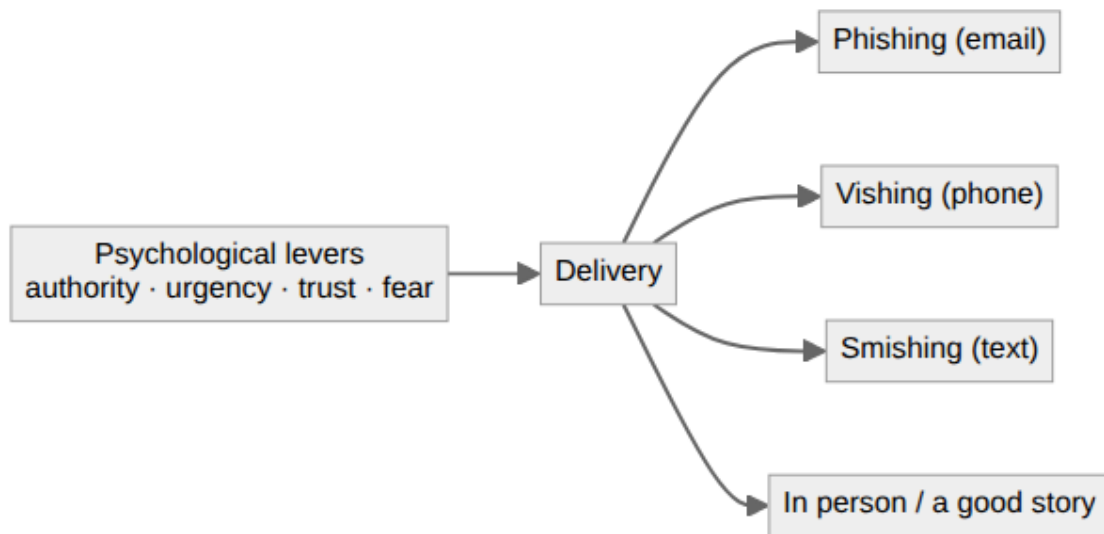
TL;DR

Social engineering skips the firewall and targets the person, because it's cheaper and it works. A human element shows up in most breaches (Verizon's DBIR puts it around 60%): a person convinced or tricked, not just something cracked. The tactics lean on a few psychological levers (authority, urgency, trust, fear) delivered by phishing, vishing, or a good story. The defense isn't a product; it's friction in the right place: verification habits, out-of-band callbacks, and a culture where "let me confirm that" is treated as competence, not obstruction.

The uncomfortable truth of most incidents is that nothing was hacked in the movie sense. Someone got a convincing email, or a phone call from "IT," and did exactly what they were asked. Social engineering is attacking the human instead of the machine, and it stays popular because it's cheap, it scales, and the target, a helpful person under time pressure, is standing right there.

The tactics all pull on the same few psychological levers. Authority: people comply with someone who sounds like the boss or the bank. Urgency: "your account locks in an hour" shuts off the part of the brain that would otherwise pause and check. Trust and familiarity: a message that looks like it's from a coworker or a vendor you actually use. Fear: the threat of consequences. The delivery

changes: phishing over email, vishing over the phone, a smishing text, or just a confident story in a lobby. The lever underneath is almost always one of those four.



What makes this hard to defend is that the "vulnerability" is a feature: people are supposed to be helpful and responsive. So the defenses aren't about switching that off, they're about adding friction exactly where it matters. Verification is the core: for anything sensitive (a payment, a password reset, a data request), confirm through a second channel you already trust, not the one the request arrived on. If "IT" calls asking for your MFA code, you hang up and call IT back on the number you already have. That out-of-band callback defeats most of it, because the attacker controls the inbound channel, not your directory.



The rest is culture and reps. Training that shows real examples beats a policy nobody reads; simulated phishing that teaches instead of punishing; and, most importantly, a workplace where "let me verify that before I send it" reads as competence, not obstruction. The organizations that get burned are usually the ones where slowing down to check felt like it would get you in trouble. Make checking the easy, praised default and you've quietly removed the pressure the whole attack was counting on.

