

Watering Holes and Tailgating: Attacking Where People Already Trust

Tue, Aug 11, 4:00 PM EDT · <https://scottslab.io/posts/watering-hole-and-physical-social-engineering>



TL;DR

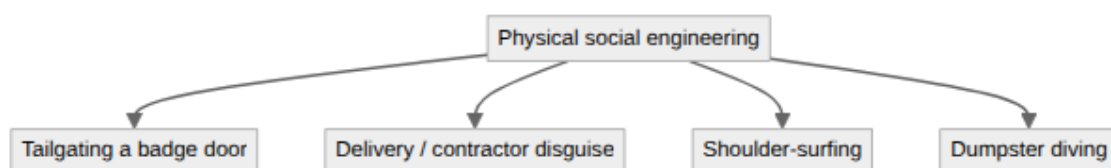
Two social-engineering plays that skip your inbox. A watering hole attack compromises a site the target already trusts and visits (an industry forum, a vendor portal) and lets the victims come to it. That sails right past "don't click strange links." Physical social engineering just walks in: tailgating through a badge door, posing as a delivery or contractor, shoulder-surfing, dumpster diving. Both exploit trust in a *place* rather than a message. Both are beaten by the same instinct: verify before you grant access, digital or physical.

Not every social-engineering attack comes at you head-on. Two of the sneakier ones work by planting themselves where your trust already lives.

A watering hole attack borrows its name from a predator waiting at the pond instead of chasing prey across the plain. Rather than phishing a hardened target directly, the attacker compromises a website that target is known to trust and visit (an industry association, a niche forum, a supplier's portal) and waits. The victims arrive on their own, to a site they've been to a hundred times, and get served the payload there. It's effective precisely because it defeats the advice we drill into everyone: there's no suspicious link to not-click; they went to a bookmark. That's why it's aimed at specific industries or groups, where the attacker knows exactly which watering hole everyone drinks from.



Physical social engineering drops the keyboard entirely and exploits the same helpfulness in the lobby. Tailgating is the classic: follow someone through a badge-controlled door while carrying a box, and most people hold it for you, because holding doors is polite. Add a hi-vis vest and a clipboard and you're a contractor; a delivery uniform and you're expected. Once inside, the low-tech attacks pay off: shoulder-surfing a password, walking off with an unlocked laptop, reading the sticky note on the monitor, or dumpster diving for the paperwork that feeds the pretexts and identity fraud from the last post.



The through-line is that the trust being exploited lives in a place, not a message, so the defense has to live at the place too. For watering holes that means the boring technical hygiene that catches drive-bys regardless of where they came from: patching, endpoint protection, least-privilege browsers. You can't tell people to distrust their own bookmarks. For the physical side it's culture again: one badge swipe per person, challenge the unbadged stranger without feeling rude, lock the screen (the habit that keeps coming up in this series), and shred what you throw away. Same instinct in both worlds: verify before you grant access, and never let familiarity stand in for authorization.