

Impersonation, Pretexting, and Identity Fraud: The Story Is the Weapon

Tue, Aug 11, 9:00 AM EDT · <https://scottslab.io/posts/impersonation-pretexting-identity-fraud>



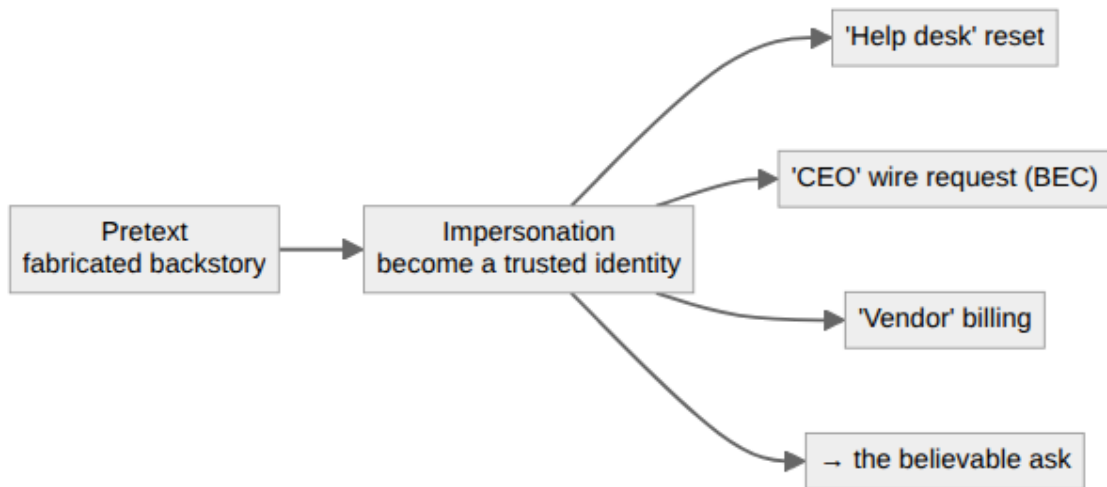
TL;DR

These three are the "who I'm pretending to be" family of social engineering. Pretexting is the fabricated backstory that makes the ask believable; impersonation is stepping into a specific trusted identity (the help desk, a vendor, the CEO); and identity fraud is using someone's real stolen details to become them on paper. The defense is the same across all three: verify identity through something the attacker can't easily supply, and never let a good story stand in for proof.

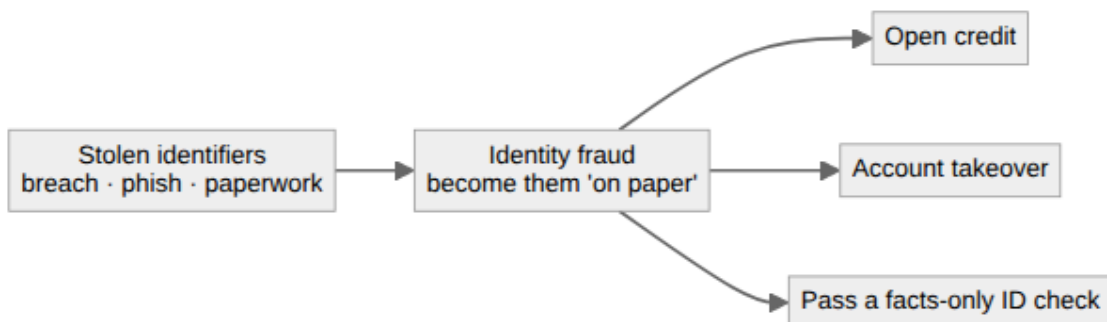
Where broad phishing is a wide net, this family is targeted and personal. It's about convincing you that the person on the other end is someone they're not.

Pretexting is the foundation: the invented scenario that makes a request make sense. "I'm from the vendor's billing team, reconciling last quarter's invoices" isn't an attack on its own. It's the stage set that makes the coming ask ("can you confirm the account details?") feel routine. The better the pretext, the less the target questions the request, because people evaluate plausibility, not authenticity. A story that fits your day is one you tend not to interrogate.

Impersonation is pretexting pointed at a specific trusted identity. Instead of a generic role, the attacker becomes the help desk resetting your password, the executive urgently wiring funds (business email compromise is exactly this), or a supplier you actually use. It works because we extend standing trust to roles and relationships. We do what the help desk says, because the help desk is the thing that's supposed to help.



Identity fraud is the heaviest version: using someone's real, stolen identifying information, pulled from a breach, a phish, or discarded paperwork, to actually pass as them. Now it isn't just a convincing story, it's your name, your account number, your date of birth, deployed to open credit, take over an account, or clear a verification check that only ever asks for facts an attacker already bought.



The defense collapses to one habit across all three: verify the person, not the plausibility. Static facts (name, birthday, account number, the last four of a card) are not authentication anymore, because they've all leaked. Real verification means something the attacker can't easily supply on demand: a callback to a number of record, a code to an enrolled device, a challenge only the real party can

answer. When someone's identity is the thing in question, a good story should raise the bar for proof, not lower it.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — <https://scottslab.io/posts/impersonation-pretexting-identity-fraud>