

8 ATTACKS TARGETING EVERYDAY PEOPLE RIGHT NOW.

01 · EMAIL — PHISHING. Fake email from a trusted brand. Goal: steal login or payment info. Red flag: urgency plus a link.

02 · SMS — SMISHING. Fake text, usually a package delivery or bank alert. The link goes to a spoofed site. Never click.

03 · VOICE — VISHING. Caller claims to be the IRS, your bank, or tech support. Creates fear, demands immediate action.

04 · CARRIER — SIM SWAP. Attacker calls your carrier, pretends to be you, transfers your number. Bypasses SMS two-factor.

05 · SOCIAL — ROMANCE. A long con: weeks of a fake relationship online, then a request for money or crypto.

06 · POP-UP — TECH SUPPORT. A fake Windows or Mac error tells you to call a number. They remote in and steal data or charge a fee.

07 · CALL/EMAIL — GOVERNMENT IMPERSONATION. IRS, Social Security, FBI. Threat of arrest or a fine unless you pay in gift cards today.

08 · SMS/EMAIL — PACKAGE DELIVERY. A fake UPS, FedEx, or USPS text: "click to reschedule delivery." Goes to a phishing site or malware.

Golden rule: slow down before acting. Every scam on this page uses urgency. Pressure is the weapon.

Sources: FTC Consumer Sentinel, FBI IC3, AARP Fraud Watch Network.

Want the psychology behind why these work, not just the list? The Social Engineering Defense Playbook goes deeper: real scripts annotated, the pretext library, the verification protocol. \$11.99.

→ [**rexcalloway.com/shop**](https://rexcalloway.com/shop)

Disclaimer: Educational content only. Not financial, legal, tax, or professional cybersecurity advice. No professional-client relationship is created. Consult a qualified professional for your specific situation. Full disclaimer at rexcalloway.com/disclaimer.