SECURITY
Smart™
BRIEFING

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Behind the Scenes of Social Engineering

When companies hire Nathan Drier, a consultant at computer security firm Trustwave, to test their workplace security, he borrows the tricks of social engineers, or criminals who prey on employees to infiltrate enterprises for nefarious purposes. Here are some common tactics:

Phone calls

The most direct way to get sensitive information is simply to call and ask, Drier says. "I like to pretend I’m interested in a technical job they posted, and use that guise to get additional information from HR or wherever I happen to land," Drier says. "I can usually get them to ask for a resume, which makes for an excellent prelude for sending in some phishing emails."

Email

Social engineers often get lucky via email. "One time we sent out emails telling all the employees that we upgraded them to a newer version of their external webmail service," says Drier. "Everyone started logging in, but instead of getting access to their email, we were collecting their usernames and passwords."

The lesson: When you click on a link or an attachment or follow instructions from an unknown source, an attacker can access your username and password, your workstation and possibly your employer’s network.

Free stuff

Hackers know people love a freebie. If you spot a shiny USB drive lying in the parking lot, resist the urge to pick it up—it could be loaded with malicious software that will take over your computer and give them remote access to it. From there, they can attack other internal systems.

"For even greater success, we put USBs in a trusted location," Drier says. "[We fill] up a small basket with the drives and write ‘free’ on it. [We] walk in the front door, schmooze with the receptionist, and drop off the basket somewhere in the lobby. A couple of hours later, all 30 drives are gone and beginning to phone home."

Face-to-face meetings

Having confidence and acting the part helps social engineers, Drier says. At one client site, he stumbled on an unlocked workstation. "I slid up to the keyboard and got to work escalating my privileges and installing a back door," he says. "A couple of minutes in, an employee walks over and ... says ‘Oh, they *finally* sent someone to fix my computer!’ I smile and agree I’m here to solve that problem for her."

Tailgating

People on their way to work are in a hurry, often too busy to notice someone walking in behind them.

"No, I don’t have a badge, and you haven’t seen me around before, but the office is large and I look like I belong," Drier says. "I’m dressed just like you. I’m typing an email or talking on my phone, and I seem to know where I’m going. I’ll smile and you’ll hold the door open for me. Once inside, I find an empty cubicle off in the corner. I crawl under the desk and plug in a wireless access point. My cohorts in the minivan outside see the wireless network pop-up and begin using it to map out the internal network."