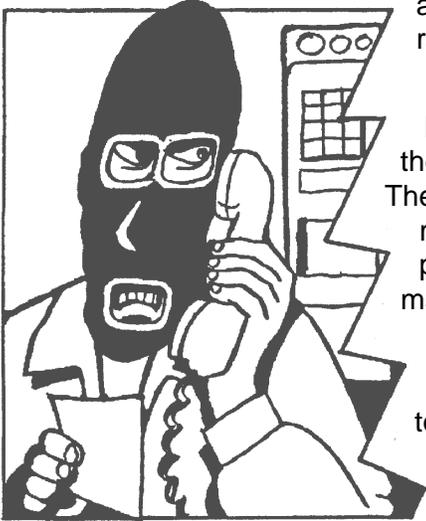


Are you sure it's an authorized request?

"Hello Chet. I was given your name by Roger Cherry and I need your assistance."

When you receive a message like this and the person is asking you to provide sensitive information, be cautious and ensure the request is legitimate. We want to be helpful, but with the use of phones, fax machines and e-mail, it is difficult to know whether the person is giving you his or her real identification.

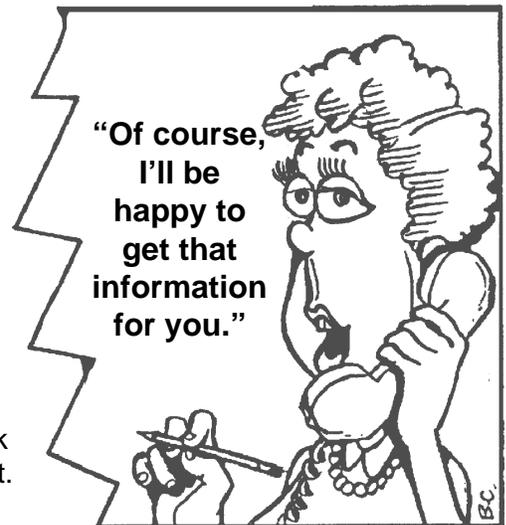


Hackers have coined the term "social engineering" to describe techniques they use to exploit weaknesses in people rather than in software or systems. The weakness they exploit is our trust. Surveys in the field of operations security, or OPSEC, show that we are susceptible to unsolicited requests from people who know enough about a subject to make the request appear legitimate.

For example, 13 days after the terrorist attacks on New York and Washington, an individual tried to gain access to a government building in Washington, D.C. The man was well dressed, well spoken and carrying a briefcase. He had no contractor or government identification badge. He stopped at the lobby guard desk and told the guard he had an appointment with an employee of a contractor on the fourth floor regarding employment opportunities. The employee he named had left for the day.

He then said he wanted to go to another contractor, but had no point of contact. When that failed, he named another employee on a different floor, but was not admitted and was asked to leave the building. He proceeded on foot to the parking garage, stopped the first person he met and told this person he was a journalist. He asked who the person worked for, where he worked, what the company did and where their customers were.

Unfortunately, the person gave this man a great deal of information. Later it was learned the man had taken mail (newspapers) from the rack in the lobby and used the names from the labels as his points of contact. The incident was reported to D.C. police, the Defense Security Service and the FBI.



If you receive an unsolicited request for sensitive or potentially sensitive information, use caution and verify the source. Contact your manager or security department if you think you've been targeted for information.

In order to protect sensitive matter, please remember that information released to the public must be approved. (See HNF Procedure HNF-PRO 184, "Standards for Controlled-Use Information.")

For information on operations security, contact your OPSEC manager or security specialist. ♦