

SOLUTIONS

The Weakest Link

Even the best-protected networks are vulnerable if employees unwittingly divulge sensitive information. **BY LEON ERLANGER**

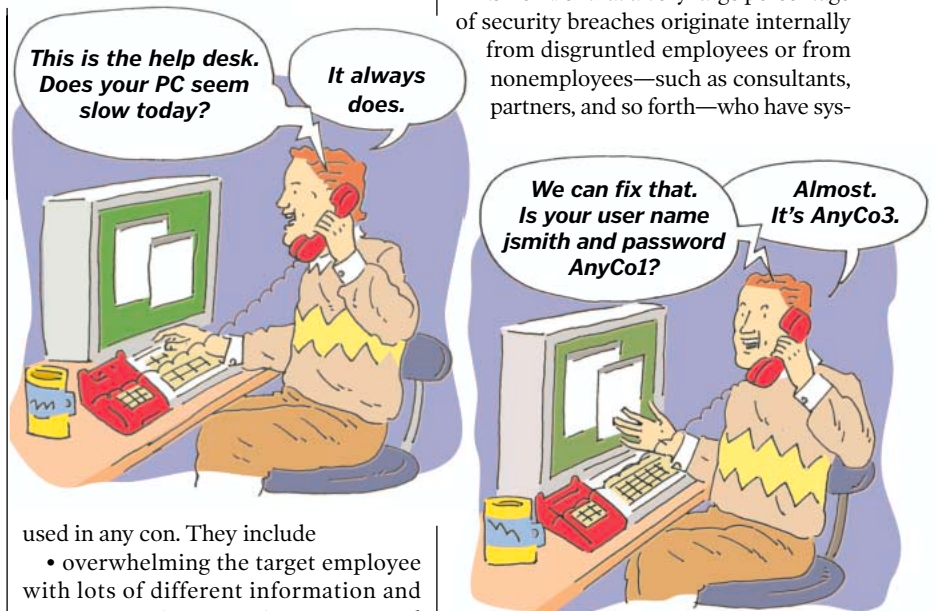
What's the weakest link in your network security infrastructure: your firewalls, antivirus systems, telecommuter PC, road-warrior notebooks? Here's a hint: Go look in the mirror. Most security experts agree that a clever hacker can penetrate almost any network simply by asking the right users for the right information. Using a variety of manipulative techniques—together known as

social engineering—that exploit a human being's natural desire to trust and help others, or to gain something for nothing, hackers can learn user names, passwords, and other information that allows them to penetrate networks—even those secured with the most advanced technology.

If you find this hard to believe, take a look at the sidebar "Five Tricks Hackers Use on You" and consider how you might respond in such situations. But the techniques explained there are only a few of the hundreds hackers use to gain valuable information.

In fact, hackers can gain a lot of information without talking to anyone, simply by surfing company Web sites for executive titles, financial information, organizational charts, and employee e-mail addresses and phone numbers. They can also sift through company trash for org charts, employee directories, system and application manuals, marketing plans, memos, company letterhead, human resources manuals, financial printouts, and procedure/policy manuals. Hackers use this information to gain the trust of others through phone calls and e-mails, often masquerading as an employee, customer, or consultant and convincing employees to provide information that can, little by little, get them into company LANs.

The techniques for eliciting information from staffers are similar to those



used in any con. They include

- overwhelming the target employee with lots of different information and strange questions or using strange and confusing arguments that make it difficult to process what is happening;
- helping the target with some technical problem, possibly one that the hacker has created. This is often called *reverse social engineering*;
- making statements that elicit strong emotions or using intimidation tactics;
- in the case of resistance, yielding on one or more small points. After a while the target often feels he must yield to other requests in return;

- sharing information and technology over time without asking for anything in return—at least not at the moment. When it comes time for the hacker to request information, the target feels he must reciprocate;

- pretending to have the same interests as the target, perhaps through information gained in user groups;

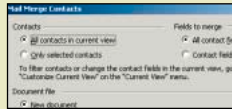
- pretending that the target can help a fellow employee fulfill an important commitment that employee has made;

- maintaining a seemingly innocent, friendly relationship with the target during which the hacker learns, bit by bit, company jargon and the names of key employees, servers, and applications.

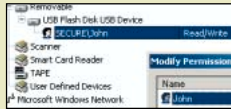
Remember that a very large percentage of security breaches originate internally from disgruntled employees or from nonemployees—such as consultants, partners, and so forth—who have sys-

tem access. People rarely question the actions of insiders.

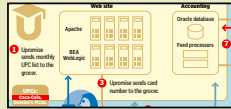
Of course, social engineering doesn't target only companies. The same techniques are also used against individuals to gain personal information such as credit card numbers, user names, and passwords for accessing popular e-commerce sites. One common technique is *phishing*, which uses a combination of e-mail messages and fake Web sites to convince users



60 Office: Use Outlook to launch a mail merge.



62 Security Watch: USB drives aid data thieves.



64 Internet Business: U-promise college funds



66 Internet Professional: Parked domains.



69 User to User: Tips and tricks.

MAKING TECHNOLOGY WORK FOR YOU

they are dealing with a major company.

If you still have doubts about the efficacy of social engineering, take a lesson from the best. Kevin Mitnick, the notorious late-20th-century hacking superstar has said again and again that he penetrated networks much more easily by manipulating people than by technology.

The truth is that most companies spend a lot more money and resources tackling security with technology than with people. But most products and technologies are not designed to protect against social engineering. So what do you do?

You should approach the problem from two angles: protecting the physical spaces that are commonly penetrated, such as offices, dumpsters, and Web sites, and protecting users through clear policies and ongoing education.

Physical security is the easier part. Here are some important tips, many of which overlap physical security and policy.

- Make sure all employees and visitors wear identification badges. Require that visitors be escorted to their destinations.



- Determine which documents must be kept locked away at all times and which require shredding on disposal.

- Keep your dumpsters in secure, locked, and monitored locations.

- Make sure that all systems, including client PCs, are protected by strong passwords that change frequently. Implement and enforce screensaver passwords that

take effect after a few minutes of idle time.

- Encrypt files stored on hard drives that contain confidential information.
- Avoid posting too much information on your public Web site.

Policy and training are harder. Employees may not understand the value of the information they give away. They must be educated continually on how to respond to unknown people requesting information, and they need to be aware of how easily they can be manipulated.

One of the best ways to give employees insight is to hold a training session and before it begins, use social engineering techniques to elicit confidential information from them. Then have the teacher amuse the class by telling them what she or he learned and from whom.

You need to draw up clear policies on what type of information should not be divulged under any circumstances. Seemingly simple tidbits, such as a server name, organizational structure info, or company jargon, can be invaluable to a hacker. Your policies should spell out clear rules for information access, setting up the physical security and safeguards outlined above. Make sure there are clear penalties for violating those policies. It's much easier for employees to refuse to divulge information if the policy is clearly spelled out.

Tools for fighting social engineering are rare, but content filtering and anti-spam products, such as MailFrontier Matador, can be configured to detect signs of fraudulent e-mails or to prevent employees from giving away sensitive information. Matador in particular uses a number of patented techniques to detect phishing and other suspicious e-mails.

Fighting social engineering is a continuous battle in which the attackers find clever ways around existing safeguards. It's important to keep up with the new tactics social engineers use and to implement policies to stop them quickly. And keep reminding employees that they are the true corporate firewall.

Leon Erlanger is a freelance author and consultant.

FIVE TRICKS HACKERS USE ON YOU

1. You receive an e-mail promising a chance at a prize of thousands or millions of dollars. All you have to do is fill in a form with your user names and passwords. You'd be amazed at how many people answer such e-mails and use the same user name and password they use on the company LAN. By sending such e-mails to tens or hundreds of employees, hackers are likely to learn at least a couple of users' network log-on information.

2. A dialog box pops up with a message that says you've lost your network connection and asks you to type in your user name and password to regain network access. Or you get an e-mail message from Microsoft, telling you to run the attached security update. Do you trust that the dialog box and the e-mail are legitimate?

3. You go out for a smoke and join a group chatting about trouble with the company's messaging servers, during which server names, as well as network and system quirks, are discussed. You don't know everyone, but, hey, it's a large company. After a while, everyone heads inside. Or you discuss the same subjects at your company's favorite local pub and a hacker just happens to be hanging out at the bar.

4. Someone shows up saying that the boss, who is on vacation, asked him to come by to fix "that Outlook problem." That sounds believable. Doesn't everyone have an Outlook problem?

5. You get a call from a woman claiming to be the president's executive assistant, who says the president asked her to obtain certain personal and user information from you. She dispels your doubts by rattling off the names and nicknames of cooperative colleagues and casually mentions some facts that only an insider is likely to know.—LE