Social engineering attacks: What we can learn from Kevin Mitnick

by Mark T. Edmead

This article provides examples of how to strengthen your organization against social engineering.

THIS ARTICLE COVERS
Spam, phishing and social engineering attacks »

LOOKING FOR SOMETHING ELSE?
How to protect your financial organization from malware
How to integrate social engineering into an information security assessment
Phone phishing: The role of VoIP in phishing attacks

+ Show More

This tip examines what Kevin Mitnick can teach us about social engineering attacks.

Last week I had the opportunity to hear Kevin Mitnick speak at the local technical bookstore in San Diego. He was there to talk about his new book, *The Art of Deception*. Most people know (or should know) who Kevin Mitnick is. I remember reading so many wild stories about Mitnck's hacker exploits. Did he really hack into the NSA and steal the address book? Did he also break into NORAD? Well, you'll have to read his book to find the answers to those questions.

What Mitnick is most famous for are his social engineering skills. In his book, Mitnick states, "Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology." While the ILOVEYOU attack was a virus attack, it also used social engineering -- exploiting the weakness that curious people that would click on an e-mail attachment.

According to Mitnick, all of the firewalls and encryption in the world will never stop a gifted social engineer from rifling a corporate database or an irate employee from crashing a system. If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link -- not operating systems, firewalls or encryption algorithms -- but people. For instance, if you wanted to illegally capture and use someone's credit card number, forget about stealing his or her wallet or purse. A social engineer would call the person on the phone and pretend to work for the bank or company that

issued the card. With the right persuasion, the person might give them the card number, billing address, social security number and mother's maiden name. If the goal were to steal sensitive information from a corporate database, the social engineer would find an employee with access to data, call them and con them into divulging the information. For the social engineer, this is much safer, much faster and can be done without leaving their house.

Security consulting firm VIGILANTe (www.vigilante.com) describes other examples of social engineering exploits:

- A confused and befuddled person will call a clerk and meekly request a password change.
- Seemingly powerful and hurried people, identifying themselves as executives, will telephone a new system administrator and demand access to their account IMMEDIATELY!
- At an airport, somebody will look over a shoulder ("shoulder surfing") as telephone credit card numbers or ATM PINs (sometimes even using binoculars or camcorders) are keyed.
- A visitor, incognito, will watch as you enter a login-ID and password at your keyboard.
- Somebody will call and confidently instruct a computer operator to type in a few lines of instruction at the console.
- An attacker will sift through your paper trash (also known as "dumpster diving"), looking for clues to unlock your IT treasures or financial life.

Preventing social engineering attacks

The best social engineering security strategy is user awareness that these attacks do happen. Here are some good business practices:

- Train employees never to give out passwords or confidential information over the phone.
- Update your security policy to address social engineering attacks.
- Update your incident-handling procedures to include social engineering attacks.
- Don't type in passwords with anyone else looking.
- Require all guests to be escorted. (Once they're inside, they have full access!)
- Keep all trash in secured, monitored areas.
- Shred important and sensitive data.
- Conduct periodic security awareness training programs.

I suspect that as better hardware and software security controls are developed and implemented, attackers will be resorting to social engineering attacks to compromise systems or steal information. Why? Companies aren't providing security awareness training for their employees. Companies spend a lot of money buying the latest and greatest security hardware but forget that some of the most sensitive information is stored in their employees' minds. And human weaknesses are the easiest ones to exploit.

Resources:

Defensive Thinking: Kevin Mitnick's new company that focuses on security awareness training.

http://www.defensivethinking.com

Ameritech Consumer Information, "Social Engineering Fraud."
http://www.ameritech.com/content/0,3086,92,00.html

Anonymous, "Social engineering: examples and countermeasures from the real-world," Computer Security Institute.
http://www.gocsi.com/soceng.htm

Arthurs, Wendy: "A Proactive Defense to Social Engineering," SANS Institute, August 2, 2001.
http://www.sans.org/infosecFAQ/social/defence.htm

Berg, Al: "Al Berg Cracking a Social Engineer," by LAN Times, Nov. 6, 1995.
http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

About the author: Mark Edmead, CISSP, SSCP, TICSA, is president of MTE Software, Inc. (www.mtesoft.com), and has more than 25 years of experience in software development, product development and network systems security.

This was first published in January 2008

Dig deeper on Spam, phishing and social engineering attacks

ALL | NEWS | PROBLEM SOLVE

- **Phishers turn to smishing and vishing scams to trick bank customers**
- **Increase in phishing attacks against nationwide banks reported**
- **Research reveals success rate of phishing attacks**
- **Notorious spammer sentenced in stock fraud scam**

Load More

0 comments

Oldest

Share your comment

Register or Login

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy

Latest TechTarget resources

SECURITY

CLOUD SECURITY

NETWORKING

CIO

CONSUMERIZATION

ENTERPRISE DESKTOP

COMPUTER WEEKLY

SearchSecurity

Report: Chick-Fil-A data breach affects locations nationwide

The popular fast-food chain has suffered what may be a massive, months-long payment card data breach that likely dates back as ...

As PCI DSS 3.0 deadline looms, QSAs urge 'continuous compliance'

As PCI DSS 3.0 becomes mandatory on Jan. 1, QSAs say struggling merchants will find that a continuous approach to PCI compliance ...