Avoiding Social Engineering and Phishing Attacks

Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a web site's security (see Protecting Your Privacy for more information).
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org/phishing_archive.html).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information).

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

Author: Mindi McDowell
