3.3.2 Countermeasures and Prevention Facts

Implementing and teaching strong security policies and procedures is a critical component of security management. The most effective countermeasure for social engineering is employee awareness training. Teach employees at all levels how to recognize social engineering schemes and how to respond to them appropriately.

This lesson covers the following topics:

- Hiring and termination process
- Help desk
- Employee identification
- Physical prevention
- User awareness
- Paper shredding
- Backups

Hiring and Termination Process

One of the most important policies any company should have in place is a hiring and termination process for employees. The following table describes both processes.

Process	Description
Hiring	The HR department should perform the following tasks: - Check the background and contact the references of every candidate who applies for a job with the company. - Verify the candidate's educational records. - Have all employees sign a nondisclosure agreement (NDA). - Have all employees sign acceptable use policies (AUPs).
Termination	When an employee leaves the company, the HR department should be responsible for: - Ensuring that an exit interview is conducted. - Reviewing the NDA with the employee during the exit interview. - Verifying that all the equipment belonging to the company and used by the employee during employment is returned. The equipment could include keys, ID cards, cell phones, credit cards, laptops, and software. - Verify that the employee's network access is suspended.

Help Desk

The two most basic procedures to be followed by the help desk are caller ID and employee callback. These two procedures ensure a safer employee verification. A second form of employee authentication also strengthens security. For example, the help desk could request a cognitive password before sharing an account password or other sensitive information.

If the company is highly concerned about security, it could implement a policy that prohibits passwords and other sensitive information to be given over the phone under any circumstances. Every employee should be taught to forward any call requesting a password or the name of an employee to the help desk. In most cases, a caller attempting to gather information through social engineering will mostly likely hang up when directed to the help desk.

Employee Identification

Implement policies and procedures that require employee identification. ID badges are a great and easy way to identify who is authorized to be in a given area. Employees should be trained to:

- Wear their badge at all times.
- Respond appropriately if they encounter a person without a badge.
- Prevent piggybacking and tailgating.
- Never share their ID badge with anyone.

Physical Prevention

Bollards are an easy physical barrier that deters aggressive intruders. Bollards can be small straight concrete pillars, flat barricades, ball-shaped pieces of concrete, large flowerpots, or even cement picnic tables, as long as they prevent attackers from forcing themselves in by driving through an exterior wall or door.

User Awareness

The table below describes different areas in which employees should be trained.

Area	Description
Phishing	Many browsers have phishing detection software. Require employees to enable the phishing detection feature and restrict employees from using browsers without that feature. Train employees to: ▪ Check the link destination within emails to verify that it points to the correct URL. ▪ Never click on links in emails. ▪ Use the different types of HTTPS appropriately: ▪ Sites secured with a regular certificate will display a lock in the address bar of most browsers. This means that the connection is encrypted using HTTPS. However, it doesn't necessarily mean the identity of the person running the site is verified. ▪ Sites that display either a green lock or green bar in the address bar indicate that the site is secure and the identity of the site has been verified.
Guests	Ensure that any guest who visits the facility is escorted. This will help prevent attackers from trying to gather information from within the facility. Also, implement a policy that prohibits guests from connecting to the organization's wired or wireless network.
Passwords	Password protection is a vital part of securing a network. Teach users to: ▪ Never write down or share passwords under any circumstances. It's not uncommon for users to write down their passwords. Sometimes, they write their passwords on a sticky note and attach it to the monitor, hide their password under the keyboard, or put the password inside a desk drawer. Strong passwords can be very difficult to remember, which tempts the user to write the password down to remember it. This practice should be prohibited. ▪ Never store passwords in cell phones. Phones are easily lost or stolen, potentially exposing the passwords. ▪ Never give out passwords to anyone. Many social engineering attacks attempt to leverage sympathy, bullying, or coercion to get the user to reveal a password. Train users not to give their passwords to anyone, even if that person claims to be the CEO or a help desk administrator. ▪ Never email passwords. Most email systems are relatively secure as they transmit email messages, but not all of them are. If an email system uses clear text, such as POP3, IMAP, or SMTP, without also using encrypting protocols, incoming and outgoing messages are transmitted in clear text. An attacker running a sniffer could capture email messages and read the contents. ▪ Never use personally associated passwords. For convenience, users tend to set passwords that contain personally associated information, such as their name, birthday, spouse's name, child's name, pet's name, anniversary date, and hometown. This is an unsecure practice. A simple social media search can reveal a great deal of personal information about a user, making it possible to guess a password. In fact, many attackers prefer this approach to a technological password attack because it is easier and faster and has a very high success rate.

Paper Shredding

Procure shredders that discourage or make it impossible to reassembled shredded documents. It's important to teach employees to safely shred all sensitive information before disposal. This is one of the best ways to prevent information from being leaked through a physical copy. There are two basic types of shredders, strip-cut and crosscut. The table below describes each type in more detail.

Type	Description
Strip-cut	Strip-cut shredders cut paper into long, thin strips. They usually handle a larger volume of paper than the crosscut shredders, and they're also lower maintenance. They usually shred paper into 1/8 to 1/2 inch thick strips. The downside of this type shredder is that dumpster divers can put the strips back together and reassemble documents.
Crosscut	Crosscut shredders are more secure because they cut the paper both vertically and horizontally, turning the paper into confetti. This makes it a lot more difficult for dumpster divers to reassemble the document.

Backups

Most organizations back up data once a day, usually at night. A backup can be full, incremental, or differential. The table below describes each type of backup.

Backup Type	Description
Full backup	A full backup is exactly what it sounds like; it backs up everything. All data on the system is backed up each time the backup runs. It's the most complete backup you can choose. Most organizations run full backups at least weekly.
Incremental backup	An incremental backup backs up every file that's changed since the last full or incremental backup. This goes a lot faster than a full backup, allowing you to back up files daily. Incremental backups have one drawback: restoring data from incremental backups takes a long time. The first thing you must do is restore the first full backup. Then you have to restore every incremental backup in the order they were created. This could take hours.

Differential backup	A differential backup backs every file that's changed since the last full backup. This has advantages and disadvantages. The advantage is that when a system crashes, data can be restored quickly. Only the last full backup and the last differential backup are restored. The disadvantage is that, by the end of the work week, the differential backup may contain a week's worth of data instead of a day's worth.