Social Engineering

1. 'Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.

2. Some emails entice the recipient into opening an attachment that activates a virus or malicious program in to your computer.

3. Be suspicious of unsolicited phone calls, visits, or email messages frohl 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.

4. 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.

5. 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.

6. Don't send sensitive information over the Internet before checking a websites security. Pay attention to the URL of a website. Malicious websites 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).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account.