Protection Against Social Engineering

Updating security network and preventing data theft - anti-virus software, firewalls, and email and spam filters - is no doubt important. However, focus should be on the human element when it comes to social engineering. Education of your staff, teachers, students, etc. is your first line of defence against social engineering attacks. Organisations should increase security awareness among all employees by providing comprehensive training programs so that they are not tricked into revealing sensitive information.

Below are some tips that would help protect against attacks:

1. For any unrequested email you receive, make sure it came from a trusted source, even if it is from what looks like a trusted company you deal with. For example, you could check their phone number.
2. Before you click on that link or open/download attachment, make sure it is safe even if it comes from a sender you trust because it could be a Trojan. Call the phone number and ask about the attachment.
3. Never reply to unsolicited email messages with confidential or financial information. Remember legitimate organisations and companies do not contact you to provide help unless you request it.
4. Write policies or review existing ones related to outgoing transactions and make sure they are followed.

Security experts recommend the implement of social engineering penetration tests to help administrators identify assets most-at-risk and types of attacks. This would help provide focused security training to specific employees.

Author: Mariam Al Mahrooqi