

SOCIAL ENGINEERING



Email Phishing

Used to steal passwords, credit card numbers, user data, etc. This occurs when an attacker - disguised as a trusted entity - fools their victim into opening an email, sms message, etc. They are tricked into clicking a malicious link that installs malware.

Phone Phishing

Most common social engineering attack. This is done by the attacker calling a company and imitating someone, like a computer technician or employee, to get information out of the user.

Physical Security Testing

Testing corporate network vulnerabilities. A pen tester would attempt a security breach using tactics of a malicious hacker. Some may seek employment at the target organization. Once employed, their goal is to obtain information.

An attacker will frequently take advantage of an end user's lack of knowledge (security awareness) of proper security procedures - along with the innate desire of most people to be helpful - in order to gain illicit access to protected resources. This type of manipulation is referred to as a "Social Engineering" attack. Foresite can help you identify vulnerabilities and find risks as they apply to those with direct access to your systems, then put processes in place to mitigate internal threat.

»»FORESITE



7311 W 132nd St, Suite 305
Overland Park, KS 66213



1 Hartfield Blvd, Suite 300
East Windsor, CT 06088



A8 Ively Rd, Farnborough
Hampshire, GU14 0LX UK