

Social Test

Is Your Workforce Prepared To Defend Against An Attack?

Social engineering is one of the key ways attackers can gain access to or information about your organization. People are the weakest link in the daily management of network security. To mitigate this, Digital Defense offers an examination into the security awareness and practices of your employees and suppliers through Digital Defense's Social Test.

Digital Defense offers several Social Test social engineering options, depending on your organization's needs, preferences, and resources.

Remote Social Engineering

Remote Social Engineering is ideally performed on a semi-annual basis to provide an accurate representation of your employees' security awareness. It includes a wide range of attacks, each specially designed to give important information on employee reactions. There are several options for remote social engineering:

Option 1: Phone-based Phishing

Digital Defense will place calls to your internal staff members and, upon request, to your suppliers in an effort to assess their security awareness. We specifically attempt to obtain information that could be used to gain unauthorized or falsely authorized access to your network resources or data.

Option 2: Vishing

Digital Defense will send targeted emails with an action request for the user to call a local number for more information. Digital Defense answers the call and conducts social engineering (i.e. "vishing"). We specifically attempt to obtain information that could be used to gain unauthorized or falsely authorized access to your network resources or data.

Option 3: Web-based Phishing

Digital Defense will send targeted emails with an action request for the user to visit a website which is designed to elicit sensitive information (i.e. phishing). This involves creating a custom webpage which has the look and feel of your intranet or public site, and then capturing the input involved.

RESULTS ARE KEY

Many benefits to clients can be gleaned from Digital Defense's Social Test, such as:

- Identification of gaps in security policies and personnel awareness
- Balancing of investments in security technology versus personnel training
- Identification of the absence of necessary physical safeguards

Digital Defense will provide a formal softcopy report of all evaluation findings, which can be used for internal review, planning purposes, and regulatory examinations.

Our social engineering solutions support organizations in achieving compliance with the following regulatory guidelines:

- GLBA
- NCUA
- HIPAA
- SARBOX

"To thwart a hacker, you must be able to think like one."

Option 4: Email-based Phishing

Digital Defense will send employees targeted emails with an action request for the user to reply back to the message with information (i.e. phishing). Data is then captured at Digital Defense, and analyzed for sensitivity.

Option 5: USB Drops (physical based)

Digital Defense will obtain USB drives and load them with custom-developed software that, when the USB key is plugged into a computer, will auto run and transmit the username, hostname, and IP address in a secure fashion to Digital Defense. The intent is to determine how susceptible staff are to opening these USB drives. Digital Defense will report on the number of incidents of users running this software, the associated username, system name and IP address.

Onsite Social Engineering

Onsite Social Engineering is ideally performed annually to provide an accurate and more thorough representation of your employees' security awareness. DDI uses several onsite testing methods, including:

- Attempts to gain physical access to the premises
- Obtaining records, files, equipment, sensitive information, network access, etc.
- Attempts to garner information to permit unauthorized network access

With both forms of testing, Digital Defense provides a detailed report with all methods employed and weaknesses discovered.

Let Us Help Identify Your Weaknesses

Contact us at sales@digitaldefense.com. Or, for more information visit www.digitaldefense.com/contact-us.



Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.