

Social Engineering Contest To Target Financial Institutions and Businesses

7/15/10 Notice from EPCOR

Highlight:

An upcoming Hackers conference has challenged attendees to legally social engineer organizations, including Financial Institutions, during a contest they call "Capture the Flag". Conference Hackers / participants are restricted from gathering confidential information during the contest. This alert is intended to inform EPCOR Members of this upcoming event, alert Members that Hackers are currently searching websites to find useable information, and to encourage all Members to evaluate their Social Engineering Identification Plan.

What is DEFCON?

DEFCON is one of the largest annual Hacker conventions in the world, held every year in Las Vegas, Nevada. The first DEFCON took place in June 1993, and in 2008 over 8,500 people attended DEFCON 16. Many of the attendees at DEFCON include computer security professionals, journalists, lawyers, federal government employees, crackers, and hackers with a general interest in computer code and computer architecture.

Each year DEFCON hosts several contests; Capture the Flag (CTF) is perhaps the best known. It is a hacking competition where teams of Hackers attempt to attack and defend computers and networks.

DEFCON 18 will take place July 30-August 1, 2010.

Details:

Social Engineering remains a high concern of all organizations. In order to demonstrate tactics used to social engineer organizations, this year's CTF contest aims to test participants' social engineering skills.

This contest encourages conference Hackers to legally social engineer their way into a target company; this includes Financial Institutions. The Hackers are not allowed try to gain credit card numbers, social security numbers, passwords or make the target feel "at risk." Participants cannot use government agencies, law enforcement or legal entities as a ruse to get inside, nor can they contact relatives of the targeted firm's employees.

Hackers are already searching company and Financial Institution websites to build dossiers of potential targets. Hackers in the contest are not allowed to phone or email the potential target prior to the contest.

Be Prepared:

Financial Institutions should be aware of this upcoming event, and should brief their personnel, especially call centers and legal departments. We also encourage Members to review their social engineering incident and identification response processes with legal teams and appropriate state and local statutes before the exercise starts.

This is a good time to review your procedures and make updates to thwart all forms of social engineering.

The Do Not List of CTF:

One of the requirements of CTF is that no one actually gets victimized during the contest. Social engineering skills can be demonstrated without engaging in unethical activities. The contest focuses on the skills of the contestant, not who does the most damage.

Items that are not allowed to be targeted at any point of the contest, include:

- 1) No confidential data. (i.e. SS#, Credit Card Numbers, etc)
- 2) Nothing that can get Social-Engineer.org, DEFCON or the participants in the contest sued.
- 3) No porn.
- 4) At no point are any techniques allowed to be used that would make a target feel as if they are "at risk" in any manner. (ie. "We have reason to believe that your account has been compromised.")
- 5) No targeting information such as passwords.
- 6) No pretexts that would appear to be any manner of government agency, law enforcement or legally liable entity.
- 7) The social engineer must only call the target company, not relatives or family of any employee.
- 8) Nothing unethical.