Business Wire
A Berkshire Hathaway Company

September 15, 2010 01:00 PM Eastern Daylight Time

# Report Published: Social Engineering Contest Findings

OMAHA, Neb.--(BUSINESS WIRE)--Social-Engineer.Org, a website devoted to helping companies become more aware of the threat posed by social engineering techniques, announced the release of their report on the findings from a recent capture the flag (CTF) contest held at Defcon 18 in Las Vegas. A summary of that report is provided below.

Companies targeted in this year's CTF contest included BP, Shell, Apple, Google, Microsoft, Cisco Systems, Proctor and Gamble, Pepsi, Coca-Cola, Symantec, Phillip Morris, Walmart, Mcafee and Ford. The report published earlier today by Social-Engineer.Org reveals some interesting (even alarming) information.

One of the most alarming findings was that it doesn't take a seasoned expert in social engineering to successfully penetrate a company. Inexperienced attackers have easy access to free resources including Facebook, LinkedIn, Twitter, Google Search, and Google Street. These resources, coupled with call centers and customer service departments that are focused on customer satisfaction, were enough to gather valuable information from most targeted companies. For the more resistant targets, there were plenty of believable pretexts to choose from (e.g., employee satisfaction survey, helpless customer, recruitment agency interviewing a former employee who just posted a resume on a job-seeking website, etc.). As a last resort, any resistance encountered was easily overcome by simply hanging up and calling again until a more cooperative employee could be reached.

Sensitive information (e.g., financial, strategic, etc.) was off limits for the CTF, but fair game 'flags' included employee schedules, browser versions, and anti-virus software used. Contestants were also encouraged to fool targets into opening a fake url as a way of demonstrating a very common attack technique. Based on findings from this contest, the average entry-level and call center employee did not appear to have adequate security training. Due to this fact, they typically did not sense any danger in being as helpful as possible in sharing information that they perceived to be trivial. With the right information (i.e., the above-mentioned flags), social engineers can pretend to be an insider, essentially gaining the trust of key gatekeepers within any organization, which ultimately leads to the compromise of sensitive information.

The big challenge for any organization looking to defend itself from this threat will be to find a balance between their customer-centered training and their anti-social-engineer security training. Companies want to help their customers, but they don't want to share seemingly-trivial information that ends up sinking their ship. Savvy organizations have found that the best prevention naturally falls into place when they identify any security training gaps, include all employees in their security training program, and distribute anti-social-engineer tips on a regular basis.

Continuum Worldwide is a proud sponsor of Social-Engineer.Org's contest. Contests like this raise awareness about important (but too-often overlooked) issues such as the role that untrained employees can play in compromising otherwise secure data. The days of cut-and-paste network security are long gone. Businesses must take a holistic approach when considering the safety of their information.

For the full report, visit http://social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf

### About Social-Engineer.Org

Social-Engineer.Org is a website committed to improving the security of all organizations through education about the latest trends in social engineering. Their blog, newsletter, podcast, and other resources cover the hottest, newest, and most innovative social engineering information available.

For more information about Social-Engineer.Org, visit www.social-engineer.org.

**About Continuum Worldwide**

Continuum Worldwide Corporation (CWC), a subsidiary of Mutual of Omaha, is a risk management company focused on helping organizations protect their environment, people and sensitive information through evaluation and process controls.

For more information about Continuum, visit www.continuumww.com.

Contacts

**Continuum Worldwide**
Patrick O'Conner, 402-916-1841
patrick.oconner@continuumww.com

**Permalink:** http://www.businesswire.com/news/home/20100915006688/en/Report-Published-Social-Engineering-Contest-Findings