SECURITY darkREADING
Protect The Business Enable Access

New Social Networking, Security Awareness Training Gets 'In Your Face'

Defcon social engineering contest organizers launch security awareness training for non-technical and technical users

By Kelly Jackson Higgins, DarkReading
Aug. 19, 2010
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=226800075

Security training for users often gets a bad rap for too much multiple-choice and lecturing and not enough reality-check, so the organizers behind the Defcon Social Engineering Capture the Flag contest have now launched a more "in your face" type-training for end users.

Chris Hadnagy, operations manager for Offensive-Security.com and founder of social-engineer.org, which sponsored the Social Engineering Capture The Flag contest in Las Vegas earlier this month, says his company is now offering security awareness training that's more "hardcore and hands-on."

He says he and his colleagues got inspired to take a new twist on user training after the Defcon social engineering contest proved so successful: All of the contestants in the live event were able to social-engineer information out of their targeted companies, with some posing as journalists, IT survey-takers, and businessmen, for instance.

"After Defcon, we decided it was a good idea for this security awareness program. This is something completely different from what's out there: you don't just learn how to be secure, we show live attacks and demonstrations of social engineering, and what actually happens [to you] when you click on a malicious PDF," for example, he says. The idea is to make it personal to the user so they can understand what an attack means for them, as well as for their company.

Other firms, such as tiger-team type experts offer penetration testing, social engineering, and other security services for firms that want a third party to pinpoint their logical and physical security weaknesses for them, and there are a handful of phishing-training packages and services available.

Hadnagy says his firm's new offering is about "real-world, in-your-face" security training courses for all types of users, technical and non-technical, "executives, IT, security, and everything in between," he says. The courses don't emphasize showing how an attack works, but rather what happens if you click on a malicious link. "Most classes show statistics about why phishing is bad," he says. "But people are saying 'why should I care, it's not my data.' That scares us," he says. So making it personal is more effective, he says.

"If someone hacks your computer at work, like most people you use it for checking personal email and you have pictures of your kids on it, so your personal life can also be in danger and at risk," Hadnagy says.

Offensive Security and Social-Engineering.org's courses also include more in-the-trenches social engineering awareness training. Some companies are having Hadnagy's firm call their organizations to see just what they can social-engineer out of their employees. "We're not gathering any serious data, but we'll record it and use it as part of their training," Hadnagy says.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors