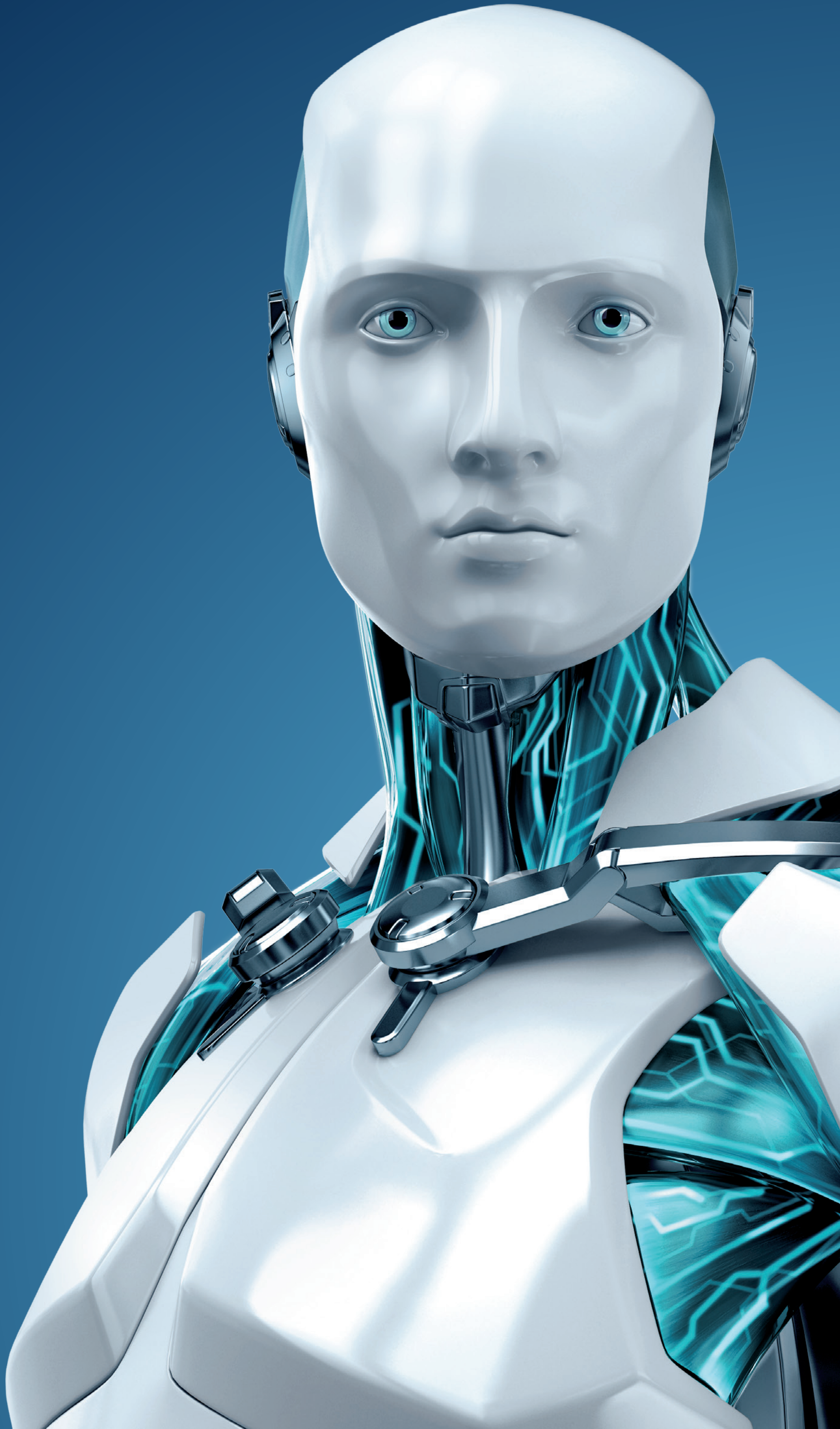
TECH BRIEF

Big companies still fall for social engineering “hacks” by phone – and it’s not getting better



ESET®

ENJOY SAFER TECHNOLOGY™

BIG COMPANIES STILL FALL FOR SOCIAL ENGINEERING "HACKS" BY PHONE – AND IT'S NOT GETTING BETTER

By Rob Waugh, We Live Security

Major companies such as Disney, Boeing and General Electric are still handing out information to "hackers" using the most basic tool of all – the human voice.

The Social Engineer Capture the Flag competition held at the Defcon security conference issued its full report – and it's grim reading, as major companies continue to "leak" crucial information in basic social engineering attacks via the telephone. Ten major US companies were targeted – and most handed out information to the attackers.

Major hacks such as the recent defacement of the New York Times home page rely on "social engineering" – fooling people into handing over information, before sending targeted emails to penetrate networks.

This year's test found that even huge companies such as the 10 under test were not immune – and the "hackers" were also untrained, using only publicly available information (such as Facebook pages) to select targets and "craft" their phone calls, according to a report by Computerworld.[1]

The attackers were available to capture information such as which operating system was used on company systems, whether wireless access was available, whether a company used a virtual private network – and information such as who supplied vending machines and catering services. All of this could be used by hackers as the basis of an attack.

"Social engineering has played some role in nearly every major hack you have read about over the last few years, yet this year's competition clearly illustrates how poorly prepared companies are to defend against socially engineered attacks," stated Chris Hadnagy, Chief Human Hacker, Social-Engineer, Inc.

"While there continues to be improvements in the quality and preparation of the contestants, there have not been any significant improvements by companies to secure information available on the Internet and educate and prepare employees against a disciplined social engineer.

"For example, one contestant was able to find an improperly secured help desk document that provided log in credentials for the target company's employee-only online portal. It's disheartening to note that after years of attacks and years of warnings, these valuable pieces of information are still so easily found and exploited."

The contest organizers selected 20 untrained contestants (10 men, 10 women), and chose brands who US customers rely on – as these would have access to their personal and financial information.

All too recently, Adobe revealed that details for 38 million users had been leaked in an attack on their systems.

[1] Computerworld. http://blogs.computerworld.com/cybercrime-and-hacking/23048/free-candy-social-engineer-tricks-company-secret-treats

"The bottom line is the firms did really poorly," says Michele Fincher of Social-Engineer.inc, which stages the contest each year, according to a report by CIO magazine.[2]

"The companies who happened to do well did so accidentally or out of ignorance in they either couldn't answer the question or didn't know how, so the call shut down. Very few said, 'I am not allowed to give out this information.'"

The organizers noted that the untrained "attackers" crafted cleverer cover stories – i.e., rather than being students or researchers – and stuck to them better, taking laptops with them and using notes on the "victim" companies. They also voiced surprise at the amount of information available during the "research" phase – where callers were able to pick who to target within each company, using the data collection tool Maltego as well as Google, LinkedIn, Bing, Facebook and other sites such as BlogSpot.

"This was an excellent competition," the organizers said. "One thing we do not see, however, are any significant improvements on the part of companies to educate and prepare themselves against social engineering attacks."

[2] We Live Security. http://www.cio.com/article/742147/Social_Engineers_Demonstrate_the_Damage_That_Could_Be_Caused_By_Information