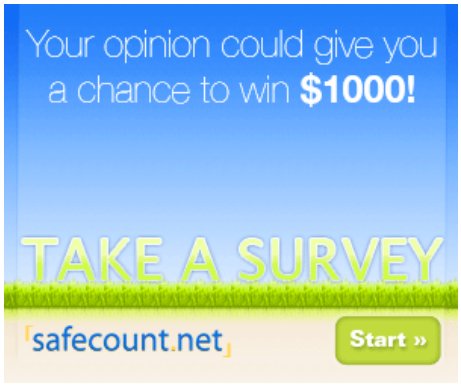

Social Engineering, White Hat Hackers Undercover - Redspin Finds 94% of Companies...

Mon Sep 14, 2009 7:30am EDT

Social Engineering, White Hat Hackers Undercover - Redspin Finds 94% of Companies Fail Email Test

CARPINTERIA, Calif., Sept. 14 /PRNewswire/ -- Redspin, Inc. is a computer information security assessment firm, which is usually the kind of cocktail party pick-up line guaranteed to send the girls home for a nap. But these white hat hackers get to do more than just sling code all day - they get to go undercover.
Social engineering is a security term used to describe the manipulation of people to get information, data, or system access; the classic con game updated for the Internet age. The most common form is phishing via email, although the phone is still a popular tool for hackers with a conman flair. Redspin has conducted hundreds of Social Engineering Assessments for corporations and financial institutions which included telephone based password acquisition, email phishing, and thumb drive drops.

As a result, Redspin found the following failure rates:

Employee failure rate:
Email: 22%
Phone: 53%

Organization failure rate (at least one employee failed):
Email: 94%
Phone: 72%

"It's one of the slickest parts of the job," says John Abraham, Redspin CEO. "Companies hire us to do social engineering assessments. We get paid to try to con people out of their data. Sometimes, it feels like we're in a movie."

One of the social engineering tests performed by Redspin involves thumb drives. "It's my favorite," says Abraham. "We put out a candy dish filled with brightly colored thumb drives, and a little post-it note that says FREE! Employees snap them all up and promptly plug them into their computers."

There's a simple little program that launches when the drive is plugged in, which would be malicious if designed by hackers. "If we were the bad guys, we would own that company's system. We still get hits from some of them months later. Good rule of thumb drives - don't use freebies."

A typical Redspin email test includes spoofing the IT department's email, then sending employees a link to a fake web page for a brand new web-based email system requesting the user's logon information. If the employee entered their name and password, then they failed. One employee wrote back to Redspin (thinking they were his IT department), "You ROCK! Thank you! I've been asking for webmail for years!"

One company had a failure rate greater than 100%; the employees were so helpful that they forwarded the spoofed emails to colleagues.

Redspin's typical phone test involves calling employees, claiming to be "Joe" from the IT department, and asking the employee to change their password to one chosen by the imposter. One customer-friendly employee offered, "As long as I'm here, would you like me to change the password on all the other

WATCHED

Red faces over top model gaff
Tue, Sep 28 2010

Mexican mayor stoned to death
Tue, Sep 28 2010

Glowing new fluorescent angelfish
Sun, Sep 26 2010

workstations?"

Yes, please.

"Employees are great," says Abraham. "They're trained to be helpful, which attackers take advantage of. We've found that it's not only our job to assess these companies, but also to ensure that the employees get awareness training. Trust, but verify."

"The best phone test we ever did was a follow-up audit a year after the first one. Our engineer started in on his script - 'Hi, I'm working with Jack over in IT, and. . .' - the person on the other end of the line said, 'Is this a social engineering call?' and hung up on us."

To prevent these attacks, a company must employ a solid security policy and employee education. To that end, one of the tools that Redspin uses is a new automated social engineering tool from its spin-off company Jetmetric: SocialPET (Policy Evaluation Tool). It automates the email test, and is available to information security and IT managers to test their own systems.

"We see the tool as having two primary functions," says Brian Hayes, Jetmetric CTO. "First, it lets you know whether or not your employees understand some basics about their security policy. Second, it's a great educational tool. After employees click through just one time, success rates shoot way up on subsequent assessments. It's so much better to learn about phishing and social engineering this way, than when it really counts."

Multimedia: A video demonstration of Jetmetric's SocialPET (Policy Evaluation Tool)

About Redspin - (www.redspin.com)

Redspin delivers the highest quality information security assessments through technical expertise, business acumen and objectivity. Redspin customers include leading companies in areas such as health care, financial services, hotels, casinos and resorts as well as retailers and technology providers. Some of the largest communications providers and commercial banks rely upon Redspin to provide an effective technical solution tailored to their business context, allowing them to reduce risk, maintain compliance and increase the value of their business unit and IT portfolios. Redspin, the objective third-party security assessment specialist, is the leader in penetration testing.

SOURCE Redspin

Deanna Grady, Redspin Inc., +1-805-684-6858 Ext 7158, dgrady@redspin.com, or
Deb Montner, Montner & Associates, +1-203-226-9290, dmontner@montner.com

MORE FROM REUTERS

HP names SAP ex-chief as its new CEO, shares slide

SAN FRANCISCO (Reuters) - Hewlett-Packard Co named Leo Apotheker, the former head of German software company SAP, its new chief executive in a surprise appointment. | **Video**

CONTINUE READING

HAPPENING NOW

JAMES PETHOKOUKIS:
China left out in the cold?
The China currency bill passed in the House helps brand this Congress as one of the more protectionist in years. Even if the next one switches gears, Beijing shouldn't expect a friendlier Washington.
Commentary

TODAY IN PICTURES

MARKETS

US Indices
DOW
-47.23
10,788.05
-0.44%

NASDAQ

CONTINUE READING

China says yuan bill could harm ties

Video: Buffett, Gates push China charity

CHINA

Editor's Choice

A selection of our best photos from the past 24 hours.

View Slideshow

TOP NEWS

Obama seeks to rally Dems to keep grip on Congress

Troops storm Ecuador hospital and free Correa | VIDEO

Report to say Waddell stoked flash crash: source

Fed's Bernanke, Pianalto say recovery disappointing

AIG and U.S. set faster, riskier exit path | VIDEO

Treasury to earn $2.25 billion on Citi securities

Data supports modest 3rd-quarter growth hopes

» More Top News

ANALYSIS & OPINION

Toxic waste is history but Superfund lives on
Gregg Easterbrook

Elizabeth Warren's principles
Felix Salmon

Gold as the "ultimate bubble"
John Kemp

» More Analysis & Opinion

TOP VIDEOS

Art's post-recession draw

The day ahead: October 1, 2010

AIG comes out ahead of taxpayers

» More Top Videos

	-7.94
	2,368.62
	-0.33%
S&P 500	
	-3.53
	1,141.20
	-0.31%
TR US INDEX	
	-0.29
	103.67
	-0.28%

Int'l Indices

NIKKEI	
	9,453.14
HANG SENG	
	22,358.17

» Markets