



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Social Engineering:

What is it, why is so little said about it, and what can be done about it?

John Palumbo

July 26, 2000

Social engineering: An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system.¹

“Hi Bev, this is Sam from the IS Department. We just got in a new corporate screensaver and since you’re the VP’s secretary you will get it first. It’s really cool wait ‘till you see it. All I need is your password so I can log on to your PC from the computer center and install it.
Oh Great!!!!!! My password is rover. I can’t wait to see that new screen saver!!!!!!”

In reality Sam does not work for the same company as Bev, and Bev is not going to be getting a new screen saver (at least not the one she was hoping for). Sam on the other hand just found himself a gold mine because he was able to Socially Engineer the password from the Vice President’s Secretary, and as many of us know, not many restrictions are put on the VP’s secretary’s login.

Social Engineering has existed in some form or another since the beginning of time, primarily because most of us are helpful and trusting people. It’s human nature. Take the “Love Bug” virus for instance, it played on the psychological need and/or want of human beings to be loved. Only after the person opened the e-mail did they discover that they were loved in a way they would hopefully never be loved again. Some Social Engineering methods include telephone – the method described above, e-mail – the I Love You virus, “Dumpster Diving” – hired guns for Oracle digging into Microsoft’s trash², in person – walking into a building and checking out all the post-it-notes with passwords on them that are stuck to monitors (come on, you know you do it), and snail mail – dropping a bogus survey in the mail offering a cash award for completion and asking some delicate questions.

So with the immeasurable security threat that Social Engineering brings to the computing community, why is very little ever said about it? The primary reason, I feel, for the lack of discussion about Social Engineering can be attributed to a statement made by said Sen. Fred Thompson, R-Tenn. about the lack of impact the Love Bug virus had on the Government.

“We in the government knew when we got an e-mail titled 'ILOVEYOU' that something was wrong”.³

People, for the most part, look at Social Engineering as an attack on their intelligence and no one wants to be considered “ignorant” enough to have opened such an e-mail. This is

why I feel that Social Engineering gets put in the closet as a “Taboo” subject. Let’s face it, there aren’t many “gurus” out there that would openly admit to being stung by a telephone call. The reality is that no matter who you are, you are susceptible to a Social Engineering attack, just ask Kevin Mitnick.⁴ Kevin Mitnick was arguably one of the most ingenious hackers of our time and he was definitely very gifted with his ability to Social Engineer just about anybody.⁵

So what can we do to combat the Social Engineer and keep our systems users and data safe and secure?

The first thing that absolutely needs to be accomplished is training, training, and more training. Users and all staff members must be aware that if anyone asks them for their passwords, or any other sensitive information, proceed with the greatest amount of caution possible. People must know that asking a question does not make them inferior or unintelligent and questioning a persons corporate ranking should be rewarded. Put the procedures into written policies and ensure that every user, manager and human being fully understands the methods listed in the policy. Assign a person to train new-hires on their start date so as not to leave that potential weak link available for even a day. When you show that person how to use their phone, explain to them your company policy on Social Engineering.

Ensure that your organization has the ability to shred sensitive documents and materials and implement policies on the usage of them. Do thorough background checks on cleaning companies, contractors, temporary employees, and permanent personnel.

And finally, keep in touch with the organizations that you can trust for current and dependable information dealing with security issues. Read advisories that are posted such as CERT Advisory CA-91.04⁶ and keep abreast of happenings in the news and on web sites.

Social Engineering is an exploit method that will only grow more dangerous as people continually “forget” to make its presence known. The advisory that was posted on the CERT Coordination Centers’ Website was dated 1991 and revised in 1997, a Network Magazine July 2000 article titled “Create Order with a Strong Security Policy” mentioned nothing about Social Engineering,⁷ and on the Computer Security Institutes’ Website⁸ there is nothing about Social Engineering. These are just to name a few. We need to train our users, peers, supervisors, managers, families, friends, and ourselves that a simple telephone conversation can cause more damage than we could know.

¹ Ryburn, Paul. COMP 1200, University of Memphis, January 1997. URL: http://www.msci.memphis.edu/%7Eryburnp/cl/glossary.html#social_engineering (26 July, 2000).

² Wolf, Jim. “Oracle’s Boardroom Spy Tricks” 29 June, 2000 URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2596401,00.html> (26 July, 2000).

³ Lemos, Robert. “Summit: Ban the Internet bad guys!” 9 May, 2000. URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2566543,00.html> (26 July, 2000).

⁴ “Kevin Mitnick: Timeline”. “Crypt Newsletter #30”. URL: <http://www.takedown.com/coverage/mitnick-timeline.html> (26 July, 2000).

⁵ Lemons, Robert. “Mitnick teaches ‘social engineering’” 17 July, 2000 URL:

<http://www.zdnet.com/zdnn/stories/news/0,4586,2604480,00.html> (26 July, 2000).

⁶ <http://www.cert.org/advisories/CA-91.04.social.engineering.html>

⁷ Blacharski, Dan. "Create Order with a Strong Security Policy". 14 July, 2000 URL: <http://www.networkmagazine.com/article/NMG20000710S0015> (29 July, 2000).

⁸ <http://www.goCSI.com> (29 July, 2000).

© SANS Institute 2000 - 2002, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor