

System and Network Security Best Practices Contest

TWNCERT Social Engineering Drill: The Best Practice to Protect against Social Engineering Attacks in E-mail Form

**Pei-Wen Liu, Jia-Chyi Wu, Pei-Ching Liu
TWNCERT**

Abstract

In spite of sophisticated technology, cyber criminals started using a simpler and more insidious technique: social engineering to access computers and obtain information. Social engineering concentrates on the weakest link of the computer security chain, which is also the most essential part of the security component: human. This paper will explain the basics of social engineering by giving a general overview. Next, it will share TWNCERT's main effort in protecting its clients against social engineering attacks through security awareness and training programs and will then review the TWNCERT Social Engineering Drill, which significantly prevents and mitigates system and network security attacks. Finally, this paper will emphasize the result and impact of implementing this low-cost and high-efficacy drill program. The appendix contains samples of actual data developed using the methods discussed in the paper.

1. TWNCERT and Social Engineering

TWNCERT, also domestically known as ICST¹, is a public sector CSIRT established in 2001 to protect national Internet infrastructures and to defend against and respond to cyber attacks. TWNCERT has helped RDEC² form a network of 13,000 government agencies and developed NSOC³ to coordinate prevention and mitigation of its clients' security threats. Furthermore, TWNCERT is responsible for

¹ ICST: Information & Communication Security Technology Center; <http://www.icst.org.tw>

² RDEC: Research, Development, Evaluation Commission

³ NSOC: National Security Operation Center

publishing cyber security alerts and vulnerability advisories, responding to incidents, and sharing and distributing information. In 2003, TWNCERT was affiliated with APCERT and FIRST as a full member.

In 2004, TWNCERT experienced and handled the first social engineering attacks, in phishing form, targeted toward its clients. Since that time, a specific team, EXAMINER, was formed in 2004 in response to this problem. In the past two years, EXAMINER has manually analyzed 417 suspected e-mails collected from clients and has considered 287 malicious (almost 69%). By the end of 2004, work on social engineering continued to grow and evolve in response to the changing needs of TWNCERT. As it analyzed and reduced social engineering attacks, TWNCERT then designed an integrant scheme to protect its clients: central and local governments.

2. TWNCERT Contributes to Prevention and Mitigation of Social Engineering Attacks

There are two main categories under which all social engineering attempts could be classified—computer or technology-based deception, and human-based deception. TWNCERT provides enough methods to prevent and mitigate social engineering attacks for its clients.

2.1 Technology:

- HoneyBear⁴: Acts as a detection system for malicious e-mail attacks. It was initially designed by TWNCERT to take the place of EXAMINER and began to function in 2006. With its web-based interface, HoneyBear allows users to submit suspect e-mail attachments in most formats to examine backdoors, viruses, Trojans, and other threats to protect clients' networks.
- TWNCERT is disseminating timely upgrades, patches, vulnerability and other technical cyber security alerts, and also provides cyber threat warning information and advisories to both governmental agencies and the general public.

2.2 Non- Technology:

TWNCERT designs a series of awareness and training programs for clients to defend against social engineering attacks.

⁴ HoneyBear: Behavior-based Email Anomaly Reconnaissance; <https://honeybear.icst.org.tw/>

- **E-learning, workshops and e-mail security guidelines.** TWNCERT has developed forty-one cyber security e-learning courses (totaling fifty hours) and designed e-mail security guidelines. TWNCERT had the honor of getting E-Learning Courseware Certification in 2007.
- **Social Engineering Drill System.** In 2005, TWNCERT created a new framework to simulate social engineering attacks (mainly phishing) and examined the role and value of information security awareness efforts in its clients. This framework includes one simulation system, one incident response team, and non-periodical exercises (TWNCERT Social Engineering Drill).

3. TWNCERT Social Engineering Drill System

Phishing and spear phishing are the most common types of social engineering encountered by TWNCERT's clients. These attacks use e-mail or malicious websites to solicit sensitive information. The concept of the TWNCERT Social Engineering Drill is as a form of security awareness program that makes clients suspicious of unsolicited e-mail. Security awareness is more complicated than just telling people not to give sensitive information away. Besides videos, newsletters, brochures, and other materials that discuss social engineering, the TWNCERT Social Engineering Drill can serve to inform clients about information security policy, to sensitize them to risks and potential losses, and to train them to recognize social engineering techniques.

The TWNCERT Social Engineering Drill, initially created by TWNCERT in 2005, is continuing development toward the newest social engineering trends. Further, TWNCERT has continued to modify and improve the techniques and methods in each exercise. The TWNCERT Social Engineering Drill is essentially resulted from cooperation between the Incident Response Team and Social Engineering Simulation System, and, as described later in this paper, is designed to do more than just prevent a social engineering. It is designed to act as a social engineer.

3.1 The Social Engineering Simulation System

The Social Engineering Simulation System was built as a defense against social engineering attacks but actually acts as both phisher and spear phisher. It is composed of three main parts: Web-Based Interface, Sample E-mail Generator, and Behavior Recorder.

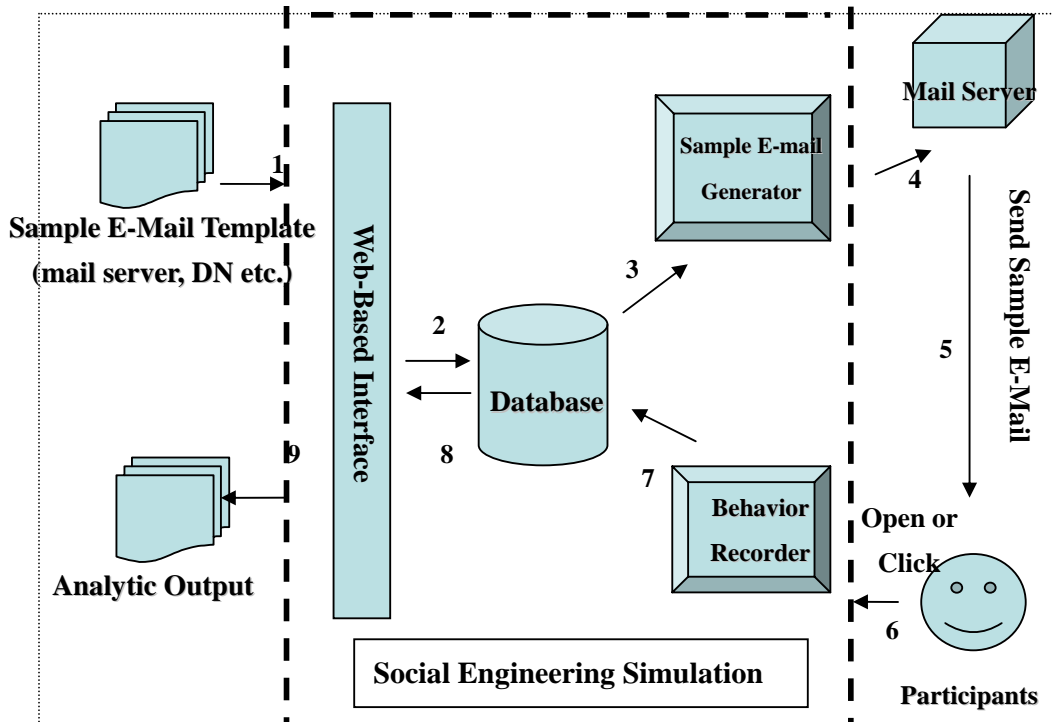


Figure 1: Overview of TWNCERT Social Engineering Drill

3.1.1 Web-Based Interface. The facility enables drillers (administrators) to launch and configure the method of the drill. The administrators are able to set up the mail server, website DN, email topics, attachment format, e-mail receivers, and sender schedule.

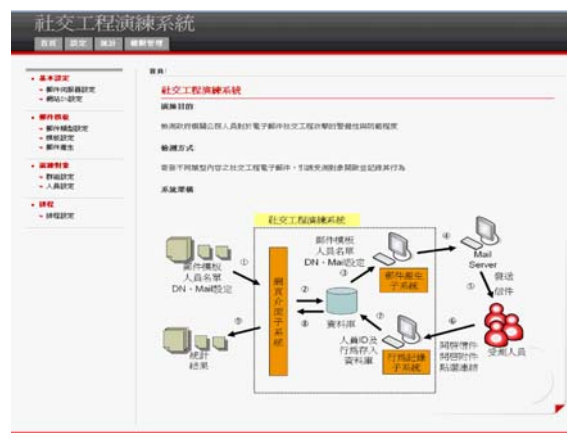


Figure 2: Web-Based Interface of the Social Engineering System

3.1.2 Sample E-mail Generator. In 2007, the TWNCERT Social Engineering Drill Sample E-mail Generator automatically produced specific “sample e-mail” that covers six types of topics, and each type contains several different contents

and texts. The categories of malicious e-mail topics include the following:

- Tech
- Health
- Travel
- Entertainment
- Sports
- Pornography

And each topic category may come with couple formats:

- Malicious attachment in MS Word format
- Malicious pictures
- Malicious links



Figure 3: Sample E-mail Generator in the Social Engineering Simulation System



Figure 4: Sample E-mail—Malicious attachment in MS Word format



Figure 5: Sample E-mail—Malicious Link



Figure 6: Sample E-mail—Malicious picture

3.1.3 Behavior Recorder. Once the sample e-mail or malicious attachment is opened or the link is clicked by the participant, Behavior Recorder would act as a behavioral surveillance to keep track of the following activities and subsequent behaviors:

- if a participant opens the sample e-mail
- if a participant opens both the sample e-mail and the malicious attachment
- if a participant opens the sample e-mail and clicks the malicious link

Behavior Recorder is simulated by certain syntax embeded in the sample e-mail. For example:

```
;
<a href="replaceURL" target="_blank"> [text]</a>; and

```



Figure 7: Behavior Recorder in the Social Engineering Simulation System

The reminder of this simulation system is organized as follows:

- Since the TWNCERT Social Engineering Simulation System is only a web application, it adopted a Low Observable technique to hide sample e-mail's IP address and domain name to accomplish the mission.
- TWNCERT Social Engineering Simulation System needs to be operated with JDK, Derby, Tomcat, TWNCERT Social Engineering System's program, and its database.

3.2 TWNCERT Social Engineering Drill

TWNCERT performed four Social Engineering Drills in 2006 and 2007. The first two drills focused on the format of e-mail attachment based upon the current threat tendency. As time went on, varied skills were used in social engineering, so the last two drills focus on e-mail topic. We will review the latest drill materials and explain the techniques used in this drill. The latest Social Engineering Drill was held in December 2007, and its details are below.

Time	December 2007
Participant (Ptp.)	62 Gov. Agencies (31,094 pers.)
Ptp. Opened Sample e-mail	7,515 (24.17%)
Ptp. Clicked Sample e-mail	5,064 (16.29%)
Sample e-mail (S-email) Sent	186,564
S-email Opened	15,484 (8.30%)
S-email Clicked	7,836 (4.20%)

Figure 8: TWNCERT Social Engineering Drill in Dec. 2007

Note: Reopen and re-click is not counted

In the 2007 TWNCERT Social Engineering Drill, each participant was sent a total of six sample e-mails (one sample e-mail in each topic) by the Social Engineering Simulation System’s randomizer with a variable schedule. For example, Participant A may have received two sample e-mails (one Sports related; another Tech related) in the first day of the drill. A couple days later, Participant A may have received four more sample e-mails on Health, Travel, Entertainment, and Pornography topics. All participants received six sample e-mails, and each sample e-mail had a particular topic. Once the sample e-mail was sent, the Social Engineering Simulation System’s Behavior Recorder logged every interaction that the sample e-mail made with the receiver (the participant).

	Sample E-mail Sent	Sample E-mail Opened	Sample E-mail Clicked
Tech	31,094	12.74%	7.44%
Health	31,094	9.81%	4.61%
Travel	31,094	8.85%	4.41%
Entertainment	31,094	7.41%	0.51%
Sports	31,094	5.52%	1.63%
Pornography	31,094	5.50%	2.03%

Figure 9:

Topics of Sample E-mail Sent in TWNCERT Social Engineering Drill in Dec. 2007

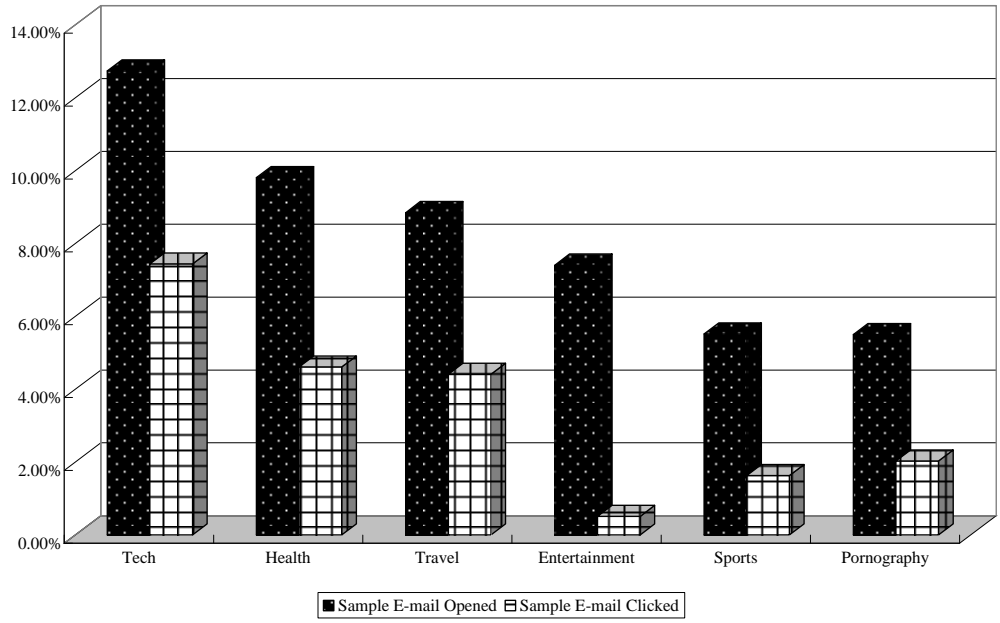


Figure 10:
Topics of Sample E-mail Sent in TWNCERT Social Engineering Drill in Dec. 2007

	Dec. 2007	June 2007	Nov. 2006	June 2006
Participant (Ptp.)	62 Gov. Agcy. (31,094 pers.)	18 Gov. Agcy. (10,799 pers.)	16 Gov. Agcy. (8,550 pers.)	6,630 Gov. Agcy. (13,575 pers.)
Ptp. Opened S-email	21.20%		33.45%	
Ptp. Clicked S-email	13.02%		18.35%	
S-email Sent	186,564	64,794	51,300	81,450
S-email Opened	6.84%		13.35%	
S-email Clicked	3.25%		4.75%	

Figure 11: TWNCERT Social Engineering Drill in Dec. 2007 Data

Note: Reopen and re-click is not counted

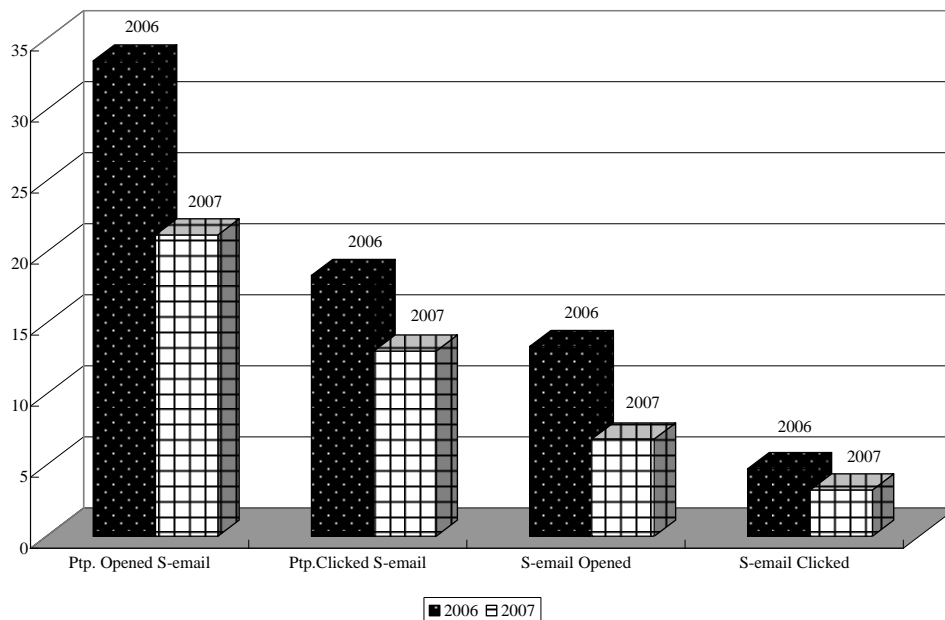


Figure 12: Output of TWNCERT Social Engineering Drill in 2006 and 2007

3.3 Incident Response Team

It should be noted, the sample e-mail is intended to be harmless. Although a participant may open a sample e-mail or click the sample e-mail attachment, no malicious activity happens to the participant’s computer. The “victim participant” will be security-clueless and will only be notified at the end of the drill. The role of Incident Response Team in the drill is to preside over, manage, and operate the exercise. Moreover, the Incident Response Team collects and analyzes all data and consequences for further implementing and employing.

4. How is the TWNCERT Social Engineering Drill related to Social Engineering Attacks?

The purpose of social engineering is usually to secretly install spyware or malicious software or to trick the user into handing over sensitive information. Since hackers find it easier to exploit human nature than to exploit holes in software, at some point, the strategy must be more than a defense so that users’ behavior is not a formidable threat to most secured networks. From the noticeable outcome (a significant decrease in the number of successful attacks), the TWNCERT Social Engineering Drill highlights the need for network and system protection in two areas:

- **Prevention.** The TWNCERT Social Engineering Drill prevents social engineering attacks from happening. By implementing the TWNCERT

Social Engineering Drill, users are adept at identifying and addressing the weaknesses or exposure before being exploited. Additionally, by implementing the TWNCERT Social Engineering Drill, users are able to collect information and evaluate the impact.

- **Migration.** The TWNCERT Social Engineering Drill mitigates the impact of social engineering attacks that have already occurred through lessons learned from the drill. By implementing the TWNCERT Social Engineering Drill, users are able to review the incident and are capable of making changes to prevent reoccurrence of the same or similar attacks.

5. Conclusion

As this paper discussed earlier, the simplest and most popular method of social engineering is still human-based. Not only do current studies show that security awareness training is usually offered as the primary defense against social engineering, but the TWNCERT Social Engineering Drill demonstrated a good security awareness program that is multi-pronged and low cost with high efficiency. Since social engineering is diverse and complex, a user's behavior is the most effective method to protecting the security. Because one of the major points of vulnerability is people, the TWNCERT Social Engineering Drill is a well measured and developed practice to reduce social engineering attacks and improve and maintain a high standard of information security for clients in other system and network threats.

According to the results of the TWNCERT Social Engineering Drills in 2006 and 2007, presumably the TWNCERT Social Engineering Drill is effective. The drill results suggest more reason to emphasize users' behavior against social engineering attacks. In addition, TWNCERT has assisted and cooperated with Microsoft on zero-day vulnerabilities and attacks for years on the strength of malicious e-mail analysis. Further, it should be noted that TWNCERT has released systems/schemes to fifty governmental agencies so far. Again, the TWNCERT Social Engineering Drill highlights the importance of experience in winning the battle.

Appendix

Since the participants of TWNCERT Social Engineering Drill are all governmental agencies, the following data is expressed in a fragmented form.

Participant Governmental Agencies	Sample E-mail Sent	Sample E-mail Opened	Percentage (%)
Public Sector 1	3,708	762	20.55%
Public Sector 2	3,114	433	13.90%
Public Sector 3	7,386	929	12.58%
Public Sector 4	2,208	183	8.29%
Public Sector 5	6,024	433	7.19%
Public Sector 6	1,464	80	5.46%
Public Sector 7	2,466	113	4.58%
Public Sector 8	5,154	205	3.98%
Public Sector 9	1,854	53	2.86%
Public Sector 10	5,934	116	1.96%
Public Sector 11	1,248	24	1.92%
Public Sector 12	1,632	30	1.84%
Public Sector 13	8,136	61	0.75%
Public Sector 14	4,968	29	0.58%
Public Sector 15	2,136	12	0.56%
Public Sector 16	2,244	11	0.49%
Public Sector 17	2,718	6	0.22%
Public Sector 18	2,400	4	0.17%

Appendix Figure 1: Sample of TWNCERT Social Engineering Drill in 2006

Participant Governmental Agencies	Sample E-mail Sent	Sample E-mail Opened	Percentage (%)
Public Sector 1	3,708	425	11.46%
Public Sector 2	3,114	243	7.80%
Public Sector 3	7,386	344	4.66%
Public Sector 4	1,464	35	2.39%
Public Sector 5	2,466	54	2.19%
Public Sector 6	1,854	39	2.10%
Public Sector 7	5,154	81	1.57%
Public Sector 8	6,024	91	1.51%
Public Sector 9	5,934	74	1.25%
Public Sector 10	2,208	25	1.13%
Public Sector 11	1,248	6	0.48%
Public Sector 12	2,136	10	0.47%
Public Sector 13	1,632	6	0.37%
Public Sector 14	8,136	29	0.36%
Public Sector 15	4,968	13	0.26%
Public Sector 16	2,244	3	0.13%
Public Sector 17	2,400	3	0.13%
Public Sector 18	2,718	3	0.11%

Appendix Figure 2: Sample of TWNCERT Social Engineering Drill in 2007