# Combating Social Engineering

## A DoD Perspective

Nathaniel D. Amsden
Department of Computer Science
Sam Houston State University
Huntsville, TX

Lei Chen
Department of Computer Science
Sam Houston State University
Huntsville, TX

***Abstract*— Individuals and organizations are under increasing threats from social engineering attacks. The Department of Defense (DoD) is a lucrative target for malicious attackers, due to the sensitive nature of America's national security assets, tactics, techniques, and procedures. Attackers seek to access this information in whatever manner possible. The rise of social engineering attempts against DoD employees highlights the necessity of defeating social engineering attacks in order to maintain system integrity, thus protecting national security information. Good policies, education and awareness, and common sense defeat social engineering attacks. Formalizing and operationalizing social engineering benefits the DoD both offensively and defensively.**

***Keywords-social engineering; tailgating; social networking; security policy; authentication***

## I. INTRODUCTION

The Department of Defense (DoD) places heavy emphasis on the security of its installations, people, and information. Protection of classified information is of utmost importance, with heavy penalties levied against those who, unauthorized, disclose it to others. Social engineering is a threat that must be countered in order to ensure the security of DoD networks and information. Social engineers employ various tactics, techniques, and procedures (TTPs) in order to exploit unsuspecting victims. DoD security officers must understand the TTPs employed by social engineers in order to effectively defeat their attacks. Drafting and implementing policies designed to defeat social engineering attacks are crucial, but are only as effective as they are followed. If the DoD fully recognizes the threat of social engineering, it can operationalize it for offensive purposes. The DoD will gain a better understanding of how to defend against social engineering if it implements it offensively.

Employee education and training must be improved in order to effectively teach employees what social engineering is and how it can be prevented. Current social engineering resistance training is contained in a simple, short online Information Assurance (IA) training module. Social engineering is only briefly covered in the IA training. This training does not meet the needs to fully enable DoD employees to resist social engineering attacks. The difficulty with developing a plan to prevent social engineering lies in the fact that it deals with person-to-person communication. Malware can be blocked at firewalls or caught by anti-virus programs. How does an organization prevent spear-phishing emails, phone calls, or in-person conversations? This is why most social engineering defensive tactics rely heavily on organizational policies and employee education.

## II. SOCIAL ENGINEERING TACTICS

### A. *Psychological Triggers*

Various psychological triggers and traits of human nature, especially those ingrained into military and DoD culture, increase the likelihood of success when exploited by a skilled social engineer. These include strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility and moral duty, authority, and integrity and consistency [1]. The DoD is based on a very rigid command structure. Authority, integrity, and consistency are important to this structure. Commanders, directors, and superiors give instructions and orders to subordinates. Subordinates are expected to execute all tasks given to them. Social engineers exploit this structure through impersonation and name dropping. Impersonating the help desk can trick victims into disclosing a username and password. Social engineers, with minimal knowledge of the military rank structure, can impersonate a higher ranking member. The social engineer convinces the victim the social engineer has authority over them. By pretending to have authority, low ranking members are tricked into giving up information to the social engineer.

Name dropping strengthens the impersonation tactic. Social engineers mention the name of the commander or someone else of importance in the organization. The victim is led to believe the social engineer was asked by the mentioned person, who has authority, to complete whatever the social engineer is asking. The tendency to follow orders of higher ranking people is a military strength, yet a weakness that can be exploited by those with malicious intent. Pretending to be someone else or simply schmoozing are typical examples of how social engineers work to obtain the information they need. They will often contact the help desk and drop the names of other employees. Once they have what they need to gain further access, they will attack a more vulnerable person – someone who has information but not necessarily the clout to challenge anyone of "authority" [2].

### B. *Phishing*

Phishing seeks to trick users into giving up information such as usernames and passwords. Phishers often say an account is about to expire and the victim needs to confirm their account information. Anti-phishing services and toolbars

attempt to protect users from phishing attacks. Many users do not understand cues provided by anti-phishing tools or fraudulent websites indicating fake websites. Julie Downs et al recruited 20 people with computer experience, but without any computer security experience. The participants received information regarding a persona they were to portray and to read and react to several emails. Several emails were legitimate whereas the rest contained various forms of phishing attacks [3].

The participants were interviewed regarding their online behaviors and their perception of what made a website trustworthy. The participants reported having seen several cues that alert a user to be suspicious including spoofing "from" addresses (95%), broken images on web page (80%), unexpected or strange URL (55%) and https (35%). Participants identified three main strategies in making decisions about the emails. The strategies include "this email appears to be for me", "it's normal to hear from companies you do business with" and "reputable companies will send emails" [3].

All safety information presented by anti-phishing services and toolbars is relatively useless if the user does not know how to interpret it. Training employees to identify phishing emails is important and can protect the organization. For the DoD, this is often presented in the form of Computer Based Training (CBT). Information Assurance training is required annually, but employees often click through as quickly as possible in order to complete it and move on to "more important" work. Phishing is only briefly covered in the training.

### C. *Fradulent Websites*

Fake websites seek to lure DoD members into giving out usernames and passwords that can then be used on the real sites. Recently, a fake version of the Air Force Portal was launched. Air Force members seeking the Air Force Portal used Google to search for it. The fake Portal appeared among the top hits. Unsuspecting victims visited the fake Portal, entered their authentication information, and thus had their login information stolen [4]. Users must be careful and should avoid searching for specific websites and instead type in the link directly. An automatic method to detect fraudulent websites, much more than warning of invalid credentials, could be very beneficial to DoD users.

Malicious attackers, recognizing the fact the United States Automobile Association (USAA) banking institution is popular among military members, often create phishing schemes and fraudulent sites to lure military members into giving out login information. Not only do attackers gain access to their bank accounts, but also to military networks if the victims reuse passwords at work.

## III. SOCIAL NETWORKING

### A. *Social Networking Threats*

The use of social media by federal employees is growing tremendously, supported by initiatives from the administration, directives from government leaders and demands from the public. With social media come the threats of spear phishing, social engineering and web application attacks [5]. Spear phishers rely on personal pieces of information about their target. Often, this information is readily available on social media websites. Social media bypasses traditional email security controls and allows attackers alternative methods to send phishing messages and gather information. Federal employees may identify themselves as employees of their department either by using their .gov or .mil email address or by intentionally listing information in their profile.

As their "friends" grow, the network of federal employees expands. Attackers need only to establish a relationship of trust with one person in order to gain a foothold to "friend" other federal employees, harvest info and conduct social engineering attacks. Additionally, enticing victims to install malicious applications on social media websites, such as Facebook, can compromise their account or download unauthorized software to their computer. This is especially risky when victims use social media from their work computers.

Other social engineering websites seek a military audience. They claim to be military only, but have no ties to the military. One in particular is owned by a German company, with a server based in Nova Scotia [6].

### B. *The Robin Sage Experiment*

The Robin Sage experiment sought to exploit fundamental levels of information leakage stemming from people's haphazard and unquestioned trust. At the end of the month-long experiment, the young, attractive (yet fake) "Robin" accumulated hundreds of connections on social networking sites. These connections included executives at government entities including the National Security Agency (NSA), DoD and Military Intelligence Groups. Much of the revealed information violated Operations Security (OPSEC) procedures [7].

Based on her listed job, many of her "friends" assumed she was trustworthy, having passed trusted government background checks and security clearances. By successfully "friending" renowned security experts, Robin's credibility soared allowing her to create more connections. Close assessments of Robin's profile indicate the false identity. By analyzing profiles and using a little common sense, people can keep themselves safe and not be "friends" with someone who does not exist.

Social engineers build relationships of trust with their targets on social networking sites. The victim trusts the social engineer and opens opportunities for further exploitation when the social engineer begins asking for information. The rise of social networking is a big concern for DoD leaders, as it opens up new attack vectors for social engineers. Social networking adds additional security, OPSEC, and IA concerns. This experiment proves the need for enhanced training regarding the dangers of social networking. It also proves that security is for everyone at all levels of organizations. It is not just for the average employee.

## IV. Combating Social Engineering

### A. A Multi-layered Defense Begins with Policies

Defense against social engineering must be multi-layered. Should one layer be penetrated, other layers are available to halt the attack. Security policies must set the foundation of defense and address social engineering. Combat strategies require action on both the physical and psychological levels. Employee training is essential [8]. Policies such as 100% shredding, no tailgating, and challenging others not wearing identification (IDs) aid security measures and deter social engineers.

100% shred policies greatly decrease all potential printed pieces of information that a social engineer could use to research the organization (and any potential secrets he could find!). Social engineers will dumpster dive, given the opportunity, in order to find any and all information that could be used to exploit others into giving him access to unauthorized systems.

Security policies must address a number of areas in order to be a foundation for social engineering resistance. It should address information access controls, setting up accounts, access approval, and password changes. It should also deal with locks, IDs, paper shredding, and escorting of visitors. The policy must have discipline built in and, above all, it must be enforced [1]. Policies should be reviewed at least every five years, with at least 20% in review each year [9].

### B. Eliminate Tailgating

Badges raise another issue. Everyone, including visitors, should wear access badges indicating status [10]. This helps reduce the threat of people overstating their authority. Some DoD units allow tailgating, that is, following someone through a controlled access door. The first person swipes his/her card and inputs his/her Personal Identification Number (PIN), gaining access. He or she then holds the door for people following, only verifying that they have an appropriate badge. If they are careful, they will also verify the picture looks like the person owning the badge. A social engineer can print a fake ID card to look exactly like the organization's standard ID cards. By following someone entering a building or secure area, it is possible to gain entry after the first person enters the appropriate security measures simply by flashing one's badge. Occasionally, the person checking does not even look at the badge or make sure the picture on the badge looks like the holder. It is humorous to note that security personnel will occasionally wear badges with a Mickey Mouse picture and attempt to tailgate into secure areas. It is a quick way to test employees to ensure they verify the picture on the badge matches the owner.

DoD facilities have the added benefit of multiple entry control points. Individuals must show identification to even enter the perimeter of the installation. This ensures some manner of affiliation with the DoD prior to getting close to restricted areas. Restricted areas then further require additional credentials and access controls in order for an individual to gain access.

By eliminating tailgating, everyone must display valid credentials to the entry control points. This eliminates the possibility of anyone sneaking in without proper authorization. The fourth-factor authentication method allows tailgating, but only by someone who knows and can vouch for the tailgater's access rights. Employees should challenge people walking around without a proper badge, even those people they recognize. They may have had access suspended without other employees knowing.

### C. Employee Training and Education

Security awareness training for all users can also mitigate social engineering attacks [8]. Key personnel should also be resistance trained. Resistance training includes inoculation, forewarning and reality checks. These outline potential social engineering attacks so personnel can recognize and resist them in the future. Inoculation gives employees weak arguments used by social engineers in order to warn them of possible methods of social engineering. Forewarning takes inoculation one step further. Employees are warned of coming attacks and also about the persuasive content of the argument. Reality checks seek to trick the employees, in a controlled manner, into becoming a victim of a mock social engineering attack. This helps them realize they are vulnerable, and puts them at a heightened sense of security for future, real attacks [1]. Understanding the attack vectors and psychological triggers social engineers use can greatly reduce the likelihood of a successful attack.

Many security programs focus on technical security and leave information vulnerable to basic espionage methods. OPSEC addresses processes that could compromise information through non-technical means. "Need to Know" information access helps prevent unnecessary proliferation of information. Other policies restricting the use of open communication lines reduce the potential for the compromise of information. Reporting questionable circumstances and activity can protect information [10].

One of the best methods for educating employees to these risks is to take social engineering stories from current events and post them on an internal web site, or use email for safety tips and informational stories. The security officer can also incorporate these stories into security awareness training sessions held for employees. The stories work like fables of yore, imparting information with a purpose. Telling authentic stories of what happened to the 'other poor guy' increases resistance to these exploits in a non-threatening way, inoculating the employee against a vulnerability to social engineering [9].

### D. Four Authentication Factors

In addition to the three common authentication factors, something you know, something you have and something you are, a fourth authentication factor, someone you know, proves a person's access rights [11]. Social engineers can easily spoof the "something you have" factor by creating a fake ID card or similar. The "something you know" factor is difficult to spoof, since it usually is a password or PIN and thus must be physically given to the person by the organization.

Social engineers seek to circumvent the something you have, something you know, and something you are authentication factors in order to gain access to the desired system or information. When communicating via email or telephone, the something you have and something you are authentication factors cannot be utilized. Something you know, such as a passphrase, can be utilized. If suspicious, ask the caller for a callback number. If they refuse to give one, red warning flags and alarm bells should sound in your mind.

Social engineers often impersonate the help desk or administrators. They call employees claiming they need the potential victim's username and password in order to fix a network issue. By simply calling the organization the caller claims to be from, such as the help desk, the fourth authentication method, someone who knows you, can vouch for the caller and authenticate him. Of course, if the help desk says no one was authorized to call you, then something is obviously wrong. Report the situation immediately.

### *E. Ontological Semantic Technology*

Autonomous systems exist that analyze semantic information from casual and unsolicited verbal and written output of a person of interest. The technology analyzes how the target says things and looks for contradictions in normal patterns of life or from previous statements to detect lies, possible cover ups, setbacks or any other number of possible problems. It is difficult to employ to counteract social engineering due to the brevity of a hit and the relative small amount of conversation pulled during that time. However, since social engineers typically overload conversations with insider terms and name dropping, the system can detect that and alert to a potential social engineering threat [12]. The DoD's culture is full of insider terms and acronyms. A person using these terms and acronyms fits into the culture, whether they are a member of the DoD or not.

This technology is better suited to track potential insider threats rather than social engineering. Yet oftentimes, insiders attempt social engineering against coworkers in order to gain access to additional and/or restricted information. This technology can be deployed in order to track the insider and warn potential victims to be wary while the investigation proceeds. Stringent background checks all but eliminate insider threats.

A way to check if someone is lying is to ask questions about a fake person or situation. By casually asking if they heard about "Bob at the help desk's" accident, the social engineer can be tricked into answering a question about someone who does not exist. If they make up any answer, they are obviously lying. Other ways to detect lying is through contradictions. Do they contradict themselves in conversation by saying different things? Ontological semantic technology can analyze conversations over periods of time and flag potential contradictions for further analysis.

## V. Formalizing and Operationalizing Social Engineering

Formalizing social engineering in cyberspace enables security specialists to not only understand the myriad of different tactics, but also to infer good defenses to prevent social engineering. Lena Laribee et al developed a trust model showing how a social engineer establishes relationships of trust with a victim. The attacker first gathers info, usually freely available, about the victim. The attacker uses this info to exploit three key characteristics of trust: ability, benevolence and integrity. In this way, the attacker seeks to convince the victim that the attacker is a trustworthy person with a need to know or do. Their proposed attack model describes how social engineering attacks are performed. It includes tactics such as friendliness, confidence, persistence, quick-wittedness, impersonation, ingratiation, conformity, diffusion of responsibility and distraction [13].

These models can greatly improve the ability to create countermeasures to social engineering. However, with the rapidly changing nature of cyberspace, the models either need to be generic enough to apply to most situations, or be constantly updated. The DoD has many sub organizations dedicated to modeling and simulation. If cyber operators, information assurance officers, and security officers research, develop, study, and implement trust and attack models, the DoD will be better positioned to understand and combat social engineering attacks.

Operationalizing offensive social engineering will benefit military operations and aid defensive strategies against social engineering. Social engineering is compatible with existing Air Force and Joint military doctrine [6]. In a cyber sense, the DoD does not utilize the offensive capabilities of social engineering to its full potential. "Weaponizing" social engineering provides the benefit of increased US military gain in the cyber realm and a better understanding of ways to defeat social engineering attacks against our organizations. Operational units deployed in theater utilize minor forms of social engineering to build friendly relations with local citizens. Troops build trust with the locals in order to mutually benefit both sides. This aspect of social engineering has no malicious intent, unlike social engineers who lie in order to obtain something through deception.

In order to effectively operationalize social engineering, a framework must be developed for measuring social engineering's effectiveness in the operational realm, training plans must be created, and TTPs must be developed [6].

## VI. Conclusion and Future Work

This paper explained various aspects of social engineering and how they affect the DoD. The military culture of the DoD makes its employees more vulnerable to certain tactics implemented by social engineers. The increase in social networking use among DoD employees creates new attack vectors that must be properly guarded. The DoD must implement a multi-layered defense to protect itself from social engineering. Establishing strong policies, including 100% shred policies and no tailgating, form the foundation of any defense strategy. They are in place in some DoD units, but not all. Strong policies are useless when they are not followed, thus employee education is a key step.

The current social engineering awareness training, only briefly and ineffectively covered in the Information Assurance

CBT, does not adequately train users to identify or combat social engineering attacks. The DoD would do well to develop better education and training methods to protect against social engineering. It should invest in developing social engineering attack models in order to better understand incoming threats and how to counter them. By taking it one step further and operationalizing social engineering, the DoD will be able to exploit enemy systems and defend against similar attacks.

We are developing a multi-phased research plan with the end goal of developing a comprehensive social engineering training program. First, we will develop a detailed questionnaire to gather data on general knowledge of social engineering tactics, techniques, and defenses. We will send this survey to members of various DoD units we have contacts at in order to get a broad variety of responses. Ideally, the organizational responsibility of each unit will be different, such as a communications unit, a test and engineering unit, a surveillance unit, a network security unit, etc. The different unit types will provide a breadth of experience and responsibilities, in order to get a diverse feel of the knowledge of the topic. Gathering enough data may pose a challenge, as the average response rate to surveys, at least within the Air Force, is about 10%. Those surveys are also shorter than we are planning. To help motivate those surveyed, we will inform them that the questionnaire is for a master's degree project. Also, we will send it to units where we have contacts, who can assist us in distributing and explaining the purpose of the questionnaire. Hopefully this will help increase the response rate.

Second, we will analyze the responses to determine the strengths and weaknesses of the general knowledge of those surveyed with regards to social engineering. This analysis will enable us to determine which social engineering tactics the average user is more susceptible to.

Third, we will develop a social engineering attack model and a social engineering defense model. These models will be specific to nuances of the DoD organization.

Fourth, we will create a comprehensive social engineering defense training program. Information gleaned from the questionnaire will enable us to determine how best to develop the training program.

## REFERENCES


[1] D. Gragg, (2002, Dec.). *A multi-level defense against social engineering* [Online]. Available: http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920

[2] T. R. Peltier, "Social engineering: concepts and solutions," *EDPACS*, vol. 33, pp. 1-13, 2006.

[3] J. S. Downs, M. B. Holbrook and L. F. Cranor, "Decision strategies and susceptibility to phishing," in Proc. *Symp. Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, 2006, pp. 1-12.

[4] R. Boland, (2011, Dec.). *Military website spoofing is no laughing matter* [Online]. Available: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2814&zoneid=254

[5] E. Crane, (2009, Sept.). *Guidelines for secure use of social media by federal departments and agencies* [Online]. Available: http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

[6] B. E. Skarda, "Operationalizing offensive social engineering for the Air Force," M.S. thesis, Dept. Elect. and Comp. Eng., AFIT, WPAFB, OH, 2008.

[7] T. Ryan, "Getting in bed with Robin Sage," in *Blackhat USA 2010*, Las Vegas, NV, 2010.

[8] S. Granger, (2002, Jan 9). *Social engineering fundamentals, part II: combat strategies* [Online]. Available: http://www.securityfocus.com/infocus/1533

[9] W. Arthurs, (2001, Aug. 12). *A proactive defense to social engineering* [Online]. Available: http://www.sans.org/reading_room/whitepapers/engineering/proactive-defence-social-engineering_511

[10] I. S. Winkler, (2009, May 13). *Case study of industrial espionage through social engineering* [Online]. Available: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF

[11] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung., "Fourth-factor authentication: someone you know," in *Conf. Comput. and Commun. Security*, Alexandria, VA. 2006, pp. 168-178.

[12] V. Raskin, J.M. Taylor and C. F. Hempelmann, "Ontological semantic technology for detecting insider threat and social engineering," in *Proc. 2010 Workshop New Security Paradigms*, 2010 © ACM. doi: 10.1145/1900546.1900563.

[13] L. Laribee, D. S. Barnes, N. C. Rowe and C. H. Martell, "Analysis and defensive tools for social-engineering attacks on computer systems," in *Information Assurance Workshop, 2006 IEEE*, West Point, NY, 2006, pp. 388-389.