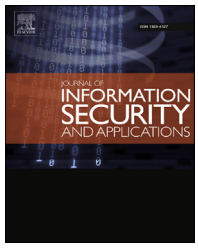
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



Advanced social engineering attacks☆

*Katharina Krombholz**, *Heidelinde Hobel*, *Markus Huber*, *Edgar Weippl*

SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria

ARTICLE INFO

Article history:
Available online 24 October 2014

Keywords:
Security
Privacy
Social engineering
Attack scenarios
Knowledge worker
Bring your own device

ABSTRACT

Social engineering has emerged as a serious threat in virtual communities and is an effective means to attack information systems. The services used by today's knowledge workers prepare the ground for sophisticated social engineering attacks. The growing trend towards *BYOD* (bring your own device) policies and the use of online communication and collaboration tools in private and business environments aggravate the problem. In globally acting companies, teams are no longer geographically co-located, but staffed just-in-time. The decrease in personal interaction combined with a plethora of tools used for communication (e-mail, IM, Skype, Dropbox, LinkedIn, Lync, etc.) create new attack vectors for social engineering attacks. Recent attacks on companies such as the New York Times and RSA have shown that targeted spear-phishing attacks are an effective, evolutionary step of social engineering attacks. Combined with zero-day-exploits, they become a dangerous weapon that is often used by advanced persistent threats. This paper provides a taxonomy of well-known social engineering attacks as well as a comprehensive overview of advanced social engineering attacks on the knowledge worker.

1. Introduction

The Internet has become the largest communication and information exchange medium. In our everyday life, communication has become distributed over a variety of online communication channels. In addition to e-mail and IM communication, Web 2.0 services such as Twitter, Facebook, and other social networking sites have become a part of our daily routine in private and business communication. Companies expect their employees to be highly mobile and flexible concerning their workspace (Ballagas et al., 2004) and there is an increasing trend towards expecting employees and knowledge workers to use their own devices for work, both in the office and elsewhere. This increase in flexibility and, conversely, reduction in face-to-face communication and shared office space means that increasing amounts of data need to be made available to co-workers through online channels. The development of decentralized data access and cloud services has brought about a paradigm shift in file sharing as well as communication, which today is mostly conducted over a third party, be it a social network or any other type of platform. In this world of ubiquitous communication, people freely publish information in online communication and collaboration tools, such as cloud services and social networks, with very little thought of security and privacy. They share highly sensitive documents and information in cloud services with other virtual users around the globe. Most of the time, users consider their interaction partners as trusted, even though the only identification is an e-mail address or a virtual profile. In recent years, security vulnerabilities in online communication and data sharing channels have often been

☆ This paper is an extended version of the conference paper (Krombholz et al., 2013).

* *Corresponding author.*
E-mail address: kkrombholz@sba-research.org (K. Krombholz).

http://dx.doi.org/10.1016/j.jisa.2014.09.005

misused to leak sensitive information. Such vulnerabilities can be fixed and the security of the channels can be strengthened. However, even security-enhancing methods are powerless when users are manipulated by social engineers. The term *knowledge worker* was coined by Peter Drucker more than 50 years ago and still describes the basic characteristics of a worker whose main capital is knowledge (Drucker, 1959). The most powerful tool an attacker can use to access this knowledge is *Social Engineering*: manipulating a person into giving information to the social engineer. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users themselves are the most vulnerable part of the system. Research has shown that social engineering is easy to automate in many cases and can therefore be performed on a large scale. Social engineering has become an emerging threat in virtual communities. Multinational corporations and news agencies have fallen victim to sophisticated targeted attacks on their information systems. Google's internal system was compromised in 2009 (Google Hack Attack), the RSA security token system was broken in 2011 (Anatomy of an Attack), Facebook was compromised in 2013 (Microsoft Hacked), as was the New York Times (Perlroth, 2013). Many *PayPal* costumers have received phishing e-mails (SocialEngineer) and many have given the attackers private information such as credit card numbers. These recent attacks on high-value assets are commonly referred to as Advanced Persistent Threats (APTs). APTs often rely on a common initial attack vector: social engineering such as spear-phishing and water-holing. The awareness for software security issues and privacy-enhancing methods has increased as serious incidents have been reported in the media. For example, the awareness for social engineering attacks over e-mail, which is without doubt the most frequently used communication channel on the Internet and is flooded by scammers and social engineers every day, has increased among users. However, the awareness for social engineering in cloud services and social networks is still comparatively low.

The main contributions of this article are the following:

- We discuss social engineering with regards to knowledge workers.
- We provide a taxonomy of social engineering attacks.
- We give an overview of current attack vectors for social engineering attacks.
- We discuss real-world incidents of successful social engineering attacks.

The goal of this paper is to provide a comprehensive and complete overview of social engineering attacks on the knowledge worker, to monitor the state of the art of research in this field, and to provide a comprehensive taxonomy to categorize social engineering attacks and measure their impact. Our paper significantly extends the state of the art by including novel, non-traditional attacks such as APTs. Our taxonomy extends and combines already existing work in this field, e.g., by Ivaturi and Janczewski (2011) and Mohd Foozy et al. (2011). Furthermore, our taxonomy systemizes operators, channels, types and attack vectors as well. The remainder of this paper is structured as follows: Section 2 contains a brief introduction to social engineering. In Section 3, we provide a detailed classification of social engineering attacks. In Section 4, we describe advanced social engineering attacks in online social networks, cloud services and mobile applications. Before concluding our work in Section 6, we discuss recent real-world social engineering attacks in Section 5.

2. Background

This section discusses the state of the art of social engineering and computer-supported collaborative work (CSCW). Attacks are divided into four different categories: physical, technical, social and socio-technical approaches.

2.1. Social engineering (SE)

Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion. Technical protection measures are usually ineffective against this kind of attack. In addition to that, people generally believe that they are good at detecting such attacks. Research, however, indicates that people perform poorly on detecting lies and deception (Qin and Burgoon, 2007; Marett et al., 2004). The infamous attacks of Kevin Mitnick (Mitnick and Simon, 2002) showed how devastating sophisticated social engineering attacks are for the information security of both companies and governmental organizations. When social engineering is discussed in the information and computer security field, it is usually by way of examples and stories (such as Mitnick's). However, at a more fundamental level, important findings have been made in social psychology on the principles of persuasion. Particularly the work of Cialdini (2001), an expert in the field of persuasion, is frequently cited in contributions to social engineering research. Although Cialdini's examples focus on persuasion in marketing, the fundamental principles are crucial for anyone seeking to understand how deception works.

2.2. Types of social engineering attacks

Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used in different stages of the actual attack. This subsection aims to explain the different approaches attackers use.

2.2.1. Physical approaches

As the name implies, physical approaches are those where the attacker performs some form of physical action in order to gather information on a future victim. This can range from personal information (such as social security number, date of birth) to valid credentials for a computer system. An often-used method is *dumpster diving* (Granger, 2001), i.e., searching through an organization's trash. A dumpster can be a valuable source of information for attackers, who may find personal data about employees, manuals, memos and even print-outs of sensitive information, such as user credentials. If an