Ascertaining Trust Indicators in Social Networking Sites

N. Veerasamy, Defense, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa

W. A. Labuschagne, Defense, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa

ABSTRACT

The use of social network sites has exploded with its multitude of functions which include posting pictures, interests, activities and establishing contacts. However, users may be unaware of the lurking dangers of threats originating from Social Networking Sites (SNS) which include malware or fake profiles. This paper investigates the indicators to arouse suspicion that a social networking account is invalid with a specific focus on Facebook as an illustrative example. The results from a survey on users’ opinions on social networks, is presented in the paper. This helps reveal some of the trust indicators that leads users to ascertaining whether a social networking profile is valid or not. Finally, indicators of potentially deceptive agents and profiles are given as a guideline to help users decide whether they should proceed with interaction with certain contacts.

Keywords: Infection, Malware, Profile, Social Networking Sites (SNS), Trust Indicator

INTRODUCTION

Social networks are increasingly popular due their wide range of communication capabilities like sharing photos, interests and even contacts. In social networks, individuals or groups with similar values, visions, goals, interests, or friendships can establish contact and start communicating. Online social networks have helped encouraged such interactions due to their ability to rapidly share information and support communications. Online social networks allow users to create profiles that can be shared with fellow contacts.

Social networking profile serves as an opportunity to grow a user’s connections and thus expand one’s contact circle which enhances their social currency. Increasingly people may use their profile to enhance their social status by gathering more contacts and posting more

DOI: 10.4018/ijcwt.2013040102
messages or updates. People may be attracted to those with strong social statuses and influential roles.

Social networks have grown tremendously in popularity due to a number of useful features. These features include:

- Profile pages showing details and interests;
- Ability to connect to like-minded individuals;
- Lists of contacts;
- Photo albums;
- Messages;
- Status updates;
- Comments;
- Games;
- Applications;
- Quizzes;
- Advertising;
- Links to other social networks;
- Ability to make new contacts;
- Contact lookup.

These features, to a large extent are attractive functions of social networks, with many users posting updates of their status, as well as establishing contacts and sharing content within social groups. Since social network provide the ability to make new contacts, users may be eager to accept friend requests and posted links. Users can receive multiple invitations to accept contacts and due to the implicit trust on social networks these invitations may be easily accepted without any consideration of the consequences.

Social networks provide for many functions. However, both malicious and beneficial activities be carried out using these platforms. Social engineering attacks may take advantage of users that are eager to interact and engage with a new contact made on a social networking site. Social engineering attacks occur when an attacker convinces a user to divulge sensitive information like passwords or system settings. Fake contacts may entice a user into believing they are real through compliments and gentle persuasion. However, the user remains in the dark completely unaware that the profile they are engaging with is invalid. Furthermore, social networking malware can be propagated from fake accounts or reposted messages.

These dangers raise important issues about understanding why users inherently trust these platforms. Understanding on why users trust social networks can help create security awareness to protect users from being attacked with social engineering techniques. It is, therefore, becoming vitally important that users be educated on the dangers of malware dispersal and fake personas.

Social engineering makes use of trust as a component to influence users to perform actions detrimental to themselves and others. Thus, social networking sites and the dangers of implicit trust have become a very important issue. Users need to be made aware of the signs that perhaps they are not dealing with a legitimate user and educated on how to evaluate the various components of a social network account. Also when users seek information, it is often overlooked that people may turn to social networks of individuals for recommendations to make trust decisions about these sources (Thomas, Enrico & Marian, 2006). By assessing various components of a social networking, users will be better empowered to determine whether they are dealing with an authentic person or an automated account that may have malicious intent. This paper commences with description of how terrorists may use social networking sites to recruit members. This is an area of concern as unsuspecting users may be drawn into an organisation. Thereafter, the paper continues with a brief explanation of how trust in social networks is built. The paper mainly focuses on Facebook but the principles are applicable to all social networking sites. The paper then presents results from a survey polling users on their trust levels of social networks to determine whether users are aware of these potential malicious objectives. It concludes with a model that summarises critical indicators that should arouse suspicion in users that they may be dealing with an invalid profile.

An important goal of this paper is to show users the dangers of social networking malware
14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/ascertaining-trust-indicators-in-social-networking-sites/101938?camid=4v1


Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

Emergent Issues in the World War Against Global Terrorism
www.igi-global.com/chapter/emergent-issues-in-the-world-war-against-global-terrorism/213320?camid=4v1a

Monkey See - Monkey Take Photo: The Risk of Mobile Information Leakage
www.igi-global.com/article/monkey-see-monkey-take-photo/105191?camid=4v1a

Securing America Against Cyber War
www.igi-global.com/article/securing-america-against-cyber-war/75764?camid=4v1a
Threats, Vulnerability, Uncertainty and Information Risk

www.igi-global.com/chapter/threats-vulnerability-uncertainty-information-risk/72168?camid=4v1a