Cybercrime on Twitter: Shifting the User Back into Focus

Vision Paper

Eva Zangerle
Databases and Information Systems
Institute of Computer Science
University of Innsbruck, Austria
eva.zangerle@uibk.ac.at

Günther Specht
Databases and Information Systems
Institute of Computer Science
University of Innsbruck, Austria
guenther.specht@uibk.ac.at

ABSTRACT

The microblogging platform Twitter has not only gained hundreds of millions of users throughout the last years, also cyber-criminals have been attracted to Twitter by the sheer volume of users engaging on the platform. This lead to multiple forms of fraud on Twitter, which in turn has also attracted academia and triggered a series of significant scientific contributions dedicated to multiple different aspects related to cybercrime on Twitter. However, we think that there are still open issues which remain to be tackled. This paper sets out to highlight missing pieces required to understand how cybercrime affects users on the Twitter platform and calls for shifting the user into the focus of research.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues—*Abuse and Crime Involving Computers*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Unauthorized access (e.g., hacking, phreaking)*; J.4 [**Computer Applications**]: Social and Behavioral Sciences

General Terms

Security, Human Factors, Legal Aspects

Keywords

Twitter, Social Media, Cybercrime, Cybersecurity, Hacking

1. INTRODUCTION

Online social networks have become important means of communication within the last decade, enabling users to reach out to other users and spread information. The microblogging platform Twitter is among the most popular online social networks, serving approximately 200 million users and issuing a total of 400 million tweets per day. Such a huge and active crowd has also attracted criminals who engage on the platform aiming at spreading spam. E.g., a significant number of fake accounts has been utilized by bots and cyborgs who try to mimic human users in order to distribute spam on Twitter in order to spread information or to influence opinions of targets. Such fake accounts are nowadays sold online for a price of approximately 30$ for 1,000 accounts [8]. Recent studies showed that the amount of spam messages on social networks (more specifically, Facebook, Twitter, Google+, YouTube and LinkedIn) has risen 355% in the first half of 2013 [6]. This is only one example of how criminals act fraudulently on Twitter, others include e.g., identity theft, compromising of accounts or trend hijacking.

In the following, we give a brief overview about current research related to crime on Twitter. Generally, we propose to categorize the research conducted on cybercrime on Twitter into the following three categories: (i) detection of spam and hacked accounts, (ii) analysis and observation of cyber-criminals and their behavior and (iii) analysis of user behavior. Due to reasons of brevity, we can only give examples of research conducted in these fields and can not provide a complete picture of the whole field. Generally, the first category has been the primary focus of researchers. This category contains research focused on methods enabling the detection of accounts which are abused for broadcasting spam tweets as e.g., in [2, 3]. The second category involves research which investigates how cybercrime is performed on Twitter. This ranges from behavioral analysis of the social dynamics between cyber-criminals [4] to the contents of the spam messages sent [5]. The third category is related to the analysis of Twitter users, their behavior and characteristics. This includes quantitative analyses of how users react after having had their account hacked and hijacked by cyber-criminals [12] or studying Twitter users and their susceptibility in regards to bots [9].

It is important to note that the research described above is highly valuable, of high quality and also of high relevance to the field. However, the vast majority the research previously described lays its focus on technical and quantitative aspects of cybercrime on Twitter and does not involve the user as a central element in this regard. E.g., to the best of our knowledge there is no work present on how a user's attitude changes once her/his account has been hacked and hijacked by cyber-criminals. Furthermore, the principle of the psychology of security states that due to the constant improvements in security mechanisms, the weak point in regards to security shifted from technology to the user her/himself [10].

International Web Science Cybercrime / Cyberwarfare Research Workshop (co-located with ACM Web Science 2014), June 23rd, 2014, Bloomington, Indiana, United States.

Hence, in order to reflect these changes, we propose to shift the actual user as the driving force for social media platforms back into the focus of research.

2. OPEN ISSUES

In the following, we briefly highlight the most important issues in regards to cybercrime on Twitter, which—to the best of our knowledge—have not been tackled by academia yet.

(i) Study User Behavior: generally, current Twitter research mostly treats users as a single, simple input factor to the cybercrime equation. However, in order to get a deeper understanding about a user's behavior, needs and attitude, we have to study the behavior of users on social networks—especially in the context of cybercrime as the user is one key factor for security (and crime) within online social networks. Hence, we call for more qualitative and empirical user studies in order to understand user behavior and attitude towards Twitter. Such empirical studies may cover the users' perceived risk of getting hacked, users' knowledge about the implications of such a hack in regards to privacy and the according actions taken. Also, the question of how user's trust into the Twitter platform (and social networks in general) in the case of such events changed remains to be answered. Such studies are the key-enabler for the development of user support mechanisms as described in the next point.

(ii) Support the User: based on the findings of research conducted as described in the previous chapter, we have to find ways to support the user in multivariate ways along the lifespan of a Twitter account ranging from the prevention of such crimes to support in recapturing a hacked account. Research on the psychology of security showed that security mechanisms are often difficult to understand for users and that users often fail to recognize risks [1, 7]. This can be lead back to the fact that security risks often seem too abstract for users, which makes such security risks less persuasive than risks with concrete consequences [10]. Therefore, it is important to strengthen a user's awareness of security risks and integrate the user into the design of applications by leveraging user-centered security design [11].

(iii) Get the Big Picture: in recent years, research on online social networks mostly has been focused on very specific aspects related to mostly technical details as pointed out in the previous chapter. However, aiming at shifting the user back into focus, we have to get the big picture in terms of user experience and perception in order to improve these aspects.

(iv) Get Interdisciplinary: many of the issues previously raised remain to be seen from different perspectives. Researchers from other sciences have to be invited and incorporated in order to get a full understanding of a user's needs and behavior and the social phenomena taking place in a social network setting. The interplay with psychology, social sciences, data mining experts and also human-computer-interaction specialists would reveal a whole new world of user-related aspects and lead to a more complete understanding of the user.

(v) Work Together: we also want to call for more cooperation between researchers in the field of cybercrime. This includes the sharing of source code and of data sets[1]. Especially the gathering of large and representative data sets is a tedious and long-term task. Making data sets and the applied algorithms available to other researchers would foster cooperative and interdisciplinary research and lead to more comparable findings.

[1]Please note that we are well-aware of the fact that Twitter is strict upon the sharing of data sets crawled via its API.

3. CONCLUSION

In this vision paper, we focus on research dedicated on cybercrime associated with Twitter. We give a brief overview about current research directions and observe that research is yet to be focused on the user him/herself. In order to tackle this problem, we present five main research objectives which aim at bringing the attention to the user and the according user experience. In a nutshell, we call for more qualitative studies of user behavior resp. user support and interdisciplinary research.

4. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida. Detecting Spammers on Twitter. In *Collaboration, Electronic Messaging, Anti-abuse and Spam Conference (CEAS)*, volume 6, 2010.

[3] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. COMPA: Detecting Compromised Accounts on Social Networks. In *ISOC Network and Distributed System Security Symposium (NDSS)*, 2013.

[4] S. Ghosh, B. Viswanath, F. Kooti, N. K. Sharma, G. Korlam, F. Benevenuto, N. Ganguly, and P. K. Gummadi. Understanding and Combating Link Farming in the Twitter Social Network. In *Proc. of the 21st Intl. Conference on WWW*, pages 61–70, 2012.

[5] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @ spam: the Underground on 140 Characters or Less. In *Proc. of the 17th ACM Conference on Computer and Communications Security*, pages 27–37, 2010.

[6] Nexgate. 2013 State of Social Media Spam. `http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf`, 2013.

[7] D. K. Smetters and R. E. Grinter. Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications. In *Proceedings of the 2002 workshop on New security paradigms*, pages 82–89. ACM, 2002.

[8] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson. Trafficking Fraudulent Accounts: the Role of the Underground Market in Twitter Spam and Abuse. In *USENIX Security Symposium*, 2013.

[9] C. Wagner, S. Mitter, C. Körner, and M. Strohmaier. When Social Bots Attack: Modeling Susceptibility of Users in Online Social Networks. In *2nd workshop on Making Sense of Microposts at WWW2012*, 2012.

[10] R. West. The Psychology of Security. *Communications of the ACM*, 51(4):34–40, Apr. 2008.

[11] K.-P. Yee. User Interaction Design for Secure Systems. *Information and Communications Security*, page 278.

[12] E. Zangerle and G. Specht. "Sorry, I was hacked"—A Classification of Compromised Twitter Accounts. In *Proc. of the 29th ACM Symposium on Applied Computing*, pages 587–593. ACM, 2014.