Computers in Human Behavior 29 (2013) 2090–2099

Contents lists available at SciVerse ScienceDirect

Computers in Human Behavior

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

# Coding behavior of authentication code on the internet

Shu-Chiung Lin [a,1], David C. Yen [b,*], Patrick S. Chen [c,2], Wei-Kuo Lin [d]

[a] Department of Information Management, College of Management, Tatung University, No. 40, Sec. 3, Zhongshan N. Road, Taipei 104, Taiwan, ROC
[b] Department of Information Systems and Analytics, Miami University Oxford, OH 45056, United States
[c] Department of Information Management,College of Management, Tatung University, No. 40, Sec. 3, Zhongshan N. Road, Taipei 104, Taiwan, ROC
[d] Department of Information Management,College of Management, Tatung University, No. 40, Sec. 3, Chungshan N. Road, Taipei 104, Taiwan, ROC

ARTICLE INFO

*Article history:*
Available online 11 May 2013

*Keywords:*
Authentication code
Coding behavior
Password
Account
Focus group

ABSTRACT

With the rapid growth of Internet services, virtual world has witnessed an increasingly large number of online users who have a variety of needs such as accessing various websites to gather information, easing business transactions, and sharing updates. As a result, information security has become a major concern among online users, and the verification of access codes is now the main practice used to keep information systems safe. However, some issues arise as the result of coding and managing behavior, and this research seeks to address these issues. After following the *Focus Group* method and interviewing 13 college students, this research finds that forgetting the access code is one of the biggest challenges to most online users simply because of the longer duration and the time when the users have a need to access the websites again, their memory will eclipse. In addition, online users usually develop self-constructed rules to cope with elusive code. These rules include: creating some sets of code that may not be meaningful to outsiders; taking different degrees of complex measures to register authentication codes, dependent upon the importance of the websites to the online users; writing the authentication codes on a scratch-pad and sticking it on the computer screen; and keeping the codes in a notebook or computer file. The above practices nevertheless run the risk of being usurped by hackers, and it is found that hacking frequently takes place among closest friends, as they are quite familiar with the coding behavior of the victims. While assisting coding management does not help in this regard, as it is generally too expensive, online users troubled by the forgetting of access codes often end up with re-applying for a new set of authentication codes after unsuccessfully trying to login. All these self-constructed rules, nevertheless, constitute threat to information security. The research, in conclusion, calls for an education campaign to promote healthy coding behavior and effective coding management. The obtained findings provide valuable references for both academicians and practitioners to understand the online users' coding behaviors and to effectively manage them accordingly to improve the resulting information security.



## 1. Introduction

With the entrance into the second decade of rapid development of information technology and booming of the online information business, people in every walk of life are found gradually transplanting their *modus operandi* from conventional platforms into informational vehicles. Given the frequent activities (e.g. playing online game, participating in virtual communities) performed through the Internet, one of the important tasks for many businesses that rely on information technology is to ensure the security of their information systems (Cox, 2012; Huang, Rau, & Salvendy, 2010). As a result, the identification of accessing users has now become a first priority in the effort to tighten security (Lin, Tzeng, & Chou, 2007; Zviran & Haga, 1999). However, a consensus has also arisen: to sustain a website as an income source and to ensure continual access of visitors, online information and shop business websites need to be immune to hackers' purposeful attacks. For those surfing the Internet and making access to varied websites, personal identification has become the first step to have access to information systems of websites through which either the users are to receive e-mails, engage in online games or to communicate through Skype (Yang & Liu, 2004; Mulligan & Elbirt, 2005; Arslan, 2012).

The major approach to filter legitimate users making access to businesses' websites is through a control mechanism that consists of users' name (i.e., account) and password (Ranalli, 2003; Zviran & Haga, 1999). It is not until both accounts and passwords successfully go through the verification process that the user can have access to the information on this website (Landwehr et al., 1994).

* Corresponding author. Tel.: +1 513 529 4827; fax: +1 513 529 9689.
*E-mail addresses:* sclin@ttu.edu.tw (S.-C. Lin), yendc@miamioh.edu (D.C. Yen), chenps@ttu.edu.tw (P.S. Chen), ufpa0303@ms6.hinet.net (W.-K. Lin).
[1] Tel.: +886 2 25925252x3614; fax: +886 2 25853966.
[2] Tel.: +886 2 25925252x3609; fax: +886 2 25853966.

0747-5632/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chb.2013.04.005

Therefore, developing the security authentication code is such an important work for controlling webmaster's management and supervising online users' usage to prevent initially hackers' attack (Singh & Thakur, 2012). In other words, authentication and verification are not only taken as the critical step to make legal access to the informational system but also a basic means to provide information security (Campbell, Ma, & Kleeman, 2011). Although accounts and passwords have become a necessity nowadays, many of online users establish their authentication code in a random manner for ease memory while never take the associated information security problems into account (Campbell et al., 2011; Weber, Guster, & Safonov, 2008). Meanwhile, a problem to arise here is that many website users often register different accounts and passwords in their applying for membership, and this it will end up with a notorious memory challenge to them (Bunnell, Podd, Henderson, Napier, & Kennedy-Moffat, 1997). It is admitted that written notes at hand may help solve this embarrassing moment, but these notes are also in danger of being misplaced or stolen. The setting process of authentication code not only represents online users' coding behavior, but also results in s potential code management and information security problems. Good managing practice will no doubt bring forth positive utilities both to online users and website masters (Cox, 2012). Zviran and Haga (1999) point out that sound information systems will help the business make profits. This is mainly because the coding management and related practices will create a positive effect onto the business operation. It can also be used to explain why a clear understanding about coding behavior becomes such a concern of/to this study. The coding behavior of authentication code in this study actually means how online users set and manage their account and password when they apply or start to use a new Internet service.

Previous researches on the users' accounts and passwords have been limited to works seen from the perspectives of systematic management and focused on security and algorithm descriptions (Agarwal & Agarwal, 2012; Bishop & Klein, 1995; Engebretson, 2004; Gao, Ma, Jia, & Ye, 2012; Metz, 2005; Mulligan & Elbirt, 2005; Wakefield, 2004; Yao & Yin, 2005). These aforementioned studies regarding coding management place more emphasis on the technical parts such as the means to strengthen protection of authentication codes. Stantona, Stama, Mastrangelo, and Joiton (2005) have correctly pointed out, prior researches rarely touch upon the inconveniences caused by issues of verification from the users' perspective, and they leave some derivative issues intact. With more and more sets of authentication code in demand, forgetting and mismatching different sets of code become a notoriously frequent and bothersome problem to the extent that many users consider it to be inconvenient (Singh & Thakur, 2012). But, fewer, past studies have been focused on issues related to users' password typing behavior (Singh & Thakur, 2012), secure practices of creating password (Cazier & Medlin, 2006; Zhang & McDowell, 2009), and/or enforcing password composition rules (Campbell, Kleeman, & Ma, 2007). With rapid growth of online users, their complaints as the result of inconveniences caused by verification and authentication are sure to emerge. Nonetheless, researchers should not overlook the disturbing part of authentication and verification existing between the users that are emphatic of convenience and website masters that highlight information security (Tam, Glassman, & Vandenwauver, 2010). This study seeks to understand, first, what is the online users' attitude toward the authentication currently in use? Second, how do the online users cope with the inconveniences as a result of authentication? To meet the two goals—understanding what inconveniences are caused by authentication and verification and what the users' expedients are to cope with them—this paper applies the *Focus Group* as a study method to acquire interviewees' feedback as an answer to the above questions. From the discussion above, the purpose of this study is to provide an in depth understanding of some emerging problems associated with coding behavior- mainly editing and applying accounts and passwords—from the perspective of online users.

The remainder of this study is organized as follows. Section 2 discusses perceived risks related to password, Internet users' coding features and the managing behavior of authentication code. Section 3 mainly describes the focus group method and the related research procedures. Section 4 presents the findings of usage and management of authentication code and Section 5 is composed of the comprehensive analysis and the research contributions. Conclusion, management implications and future researches are discussed in the final section.

## 2. Literature review

The literature review made by this paper will explore four parts. This literature review intends not only to justify the value of the research itself but reflect a necessity to highlight coding management as a vital part of Internet behavior.

### 2.1. Coding process and feature

A coding procedure is an indispensable part of membership application. There are two kinds of coding process. One is a set of authentication code given by the information system. The other coding measure is basically set by the applicants but with some restraints (Campbell et al., 2007). The applicants follow the rules set by the information system as they set their authentication code (Campbell et al., 2007). Given the flexibility, the chosen accounts and passwords reflect certain meaning that is significant to the users. This set of coding procedure will be seen as one that consists of special referents to people, matter, fact, location, things, and words that are either psychologically related to the applicants or can be commonly found in the dictionary (Campbell et al., 2011). Its initial intention is nothing but to help memorize the sometimes elusive accounts and passwords with the assistance of something referential to the users. But this arrangement remains controversial. On the one hand, as Bunnell et al. (1997) and Mulligan & Elbirt (2005) point out, we will see that putting real matters into coding does help arouse the cognitive associates. It is indeed to the benefits of the online users. On the other hand, however, Pond, Podd, Bunnell, and Henderson (2000) counter that a coding procedure assisted by personal referents risks the danger of being rightly guessed by outsiders. Despite the fact that the code has been randomly set, information security concern remains (Weber et al., 2008). Zviran and Haga (1999) echoed, observing that authentication code set up by personal referents has a lower level of security, because these accounts and passwords are relatively easier targets for guessing, and the researchers recommend online users to seek the assistance of information systems to enhance data security. Does the security assistance tool really help? Does it constitute another barrier to the Internet users? These are questions that this research will discuss later.

### 2.2. Perceived risks of coding

The original purpose of various information systems to process verification through accounts and passwords is to maintain an information security with minimum costs (Tam et al., 2010; Zhang & McDowell, 2009). Under the standard condition that accounts and passwords have to be verified before users are given certain access to information posted on the websites, personal coding either set up by the users or granted by website masters becomes one of the most important authentication data for verification (Cox,