Journal of Information Security and Applications 42 (2018) 36–45

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

An exploratory study of cyber hygiene behaviors and knowledge

Ashley A. Cain*, Morgan E. Edwards, Jeremiah D. Still

Old Dominion University, Department of Psychology, Norfolk, VA 23529, USA

ARTICLE INFO

Article history:

Keywords:
Cyber hygiene
Cyber security
Age

ABSTRACT

End users' cyber hygiene often plays a large role in cybersecurity breaches. Therefore, we need a deeper understanding of the user differences that are associated with either good or bad hygiene and an updated perspective on what users do to promote good hygiene (e.g., employ firewall and anti-virus applications). Those individuals with good cyber hygiene follow best practices for security and protect their personal information. This exploratory study of cyber hygiene knowledge and behavior offers information that designers and researchers can employ to improve users' hygiene practices. We surveyed 268 participants about their knowledge of concepts, their knowledge of threats, and their behaviors related to cyber hygiene. Further, we asked participants about their previous training and experiences. Notably, the participants represent a large cross section from age 18 to 55+. We addressed inconsistencies in the literature, we provide up-to-date information on behaviors and on users' knowledge about password usage and phishing, and we explored the impact of age, gender, victim history, perceived expertise, and training on cyber hygiene.

1. Introduction

1.1. Statement of the problem

Ideally, users would have good cyber hygiene. They would appreciate the need for software updates and would take the time to develop unique passwords. However, it appears that many users have poor cyber hygiene. They freely share passwords and are quick to share private information over social networks. Attackers know that the easiest way into a system is to steal a user's information or find a technical vulnerability. We need to help users improve their cyber hygiene knowledge and their behavioral responses.

There is no doubt that weak cybersecurity is costing society. The Second Annual Cost of Cyber Crime Study, done by Ponemon Institute [50], showed that US organizations' average cost of cybercrimes ($17.36 million) is higher than that of Japan ($8.39 million), Germany ($7.84 million), the United Kingdom ($7.21 million), Brazil ($5.27 million), and Australia ($4.3 million). These averages have been on the rise since 2014. According to the report, 98% of organizations experienced attacks related to malware, 70% experienced attacks related to phishing and social engineering, 63% experienced web-based attacks, 61% experienced attacks related to malicious code, 55% experienced attacks related to botnets, 50% experienced attacks related to stolen devices, 49% experienced attacks related to denial of services, and 41% experienced attacks related to malicious insiders. It should be noted that the number of organizations that experienced phishing and social engineering related attacks had the largest increase from 2015 to 2016, rising by 8%.

Organizations are not only affected by cyber-attacks. Individual end users are also facing major losses from these security breaches. The FBI's [25] Internet Crime Complaints Center (IC3) provides some data on cybercrimes reported by Americans. During the year 2015, the FBI received 288,012 complaints of cybercrimes, and over 40% of those complaints resulted in monetary losses. The total dollar amount of losses reported for 2015 was $1,070,711,522, with the average report of a loss being $8421. Men and women of all ages can become victims in these types of crimes; however, males aged 50–59 had the highest victim count at 31,473 victims, and females had the highest victim count in the age bracket of 40–49 with 29,559 female victims reporting cybercrimes. There were 1648 men and women, across all age groups, who reported losses over $100,000.

End users are frequently characterized as the weakest link in cyber security [2,40,49,52]. This is especially true within personal computing environments, in which they are the target of 95% of the attacks [55]. This is probably because home and personal computing devices are not protected by information security staffs, which keep hardware and software up to date [3]. Increasing cyber threats make defensive behaviors from end users more important because, regardless of how secure a system is, the end user is often a critical backdoor into the network [11,22,38,55]. Attack-

* Corresponding author.
E-mail addresses: acain001@odu.edu (A.A. Cain), mthom122@odu.edu (M.E. Edwards), jstill@odu.edu (J.D. Still).

https://doi.org/10.1016/j.jisa.2018.08.002
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

ers look for vulnerabilities; these can come from users who are exhibiting poor cyber hygiene, such as by not following best practices or revealing too much personal information.

Cyber security breaches are highly publicized, so most end users are aware that they are at risk, but they do not know how to follow best practices, such as how to protect their passwords [27]. There are security options available, but end users frequently do not know how to find those options, understand them, and use them [27]. Users often lack understanding of the necessary cybersecurity actions and this can underlie inappropriate attitudes and behaviors [21,31,36,53]. However, good cyber hygiene can promote safe behaviors and can protect against threats [1,38]. The current research provides a survey to explore the cyber hygiene habits of end users to deepen our understanding of users, which will then facilitate the development of more effective practices.

1.2. Previous findings of cyber hygiene research

Security software, such as antivirus, firewalls, and Intrusion Detection Systems are available to end users, and are essential factors in secure computing [3,17,44]. The use of these requires some knowledge. A survey of 329 homes revealed that many users are not aware of the difference between antivirus software and firewalls [4]. 67% of survey participants did not have either updated antivirus software or, in some cases, any antivirus even installed. 72% did not have a correctly configured firewall. Another survey reported that 97% of respondents without training use antivirus at home, 72% use firewall protection, 38% use anti-phishing software, 75% use anti-spyware software, and 18% use an Intrusion Detection System [55]. Ovelgönne et al. [47] collected data longitudinally from users' computers about malware attacks on anti-virus software, and they found that software-developers were attacked most often, followed by gamers, professionals, and then normal users. It is important to update security software [29]. A survey of precautionary behavior and risk perception found that participants had more precautionary behavior for using anti-virus software and installing security-software updates than for using firewall software and anti-spyware software [57]. Risk perceptions that predicted good precautionary behavior were feelings of control and severity of consequences. A second survey found that gender was found to predict updating behavior intentions, with females updating software less often than males [29].

Authentication provides one of the crucial features of network security [3,59]. Dawson and Stinebaugh's [19] report of cyber security incidents in the Critical Infrastructure and Key Resources sectors explains that weak passwords are a major source of network vulnerability, along with other technical issues (e.g., vulnerabilities due to bypassing a firewall). Users are advised to select strong passwords to prevent guessing attacks [6,10,15,17,18,38,48]. Strong passwords are described as having at least eight characters [26]. The eight characters should include numbers, letters, and punctuation [59], or they should include upper and lower case letters, numbers, and special characters [56]. They should not include any personal information or dictionary words [10,15,56]. In addition to being complex, they should be memorable [35,39]; they should not be used for multiple accounts [6,10,35]; they should be changed often [10]; and they should not be shared with others [35]. Best practices for passwords are not practical, because long, complex alphanumeric passwords are not memorable [12], which will force users to use workarounds. Users put security at risk when they select weak passwords or leave their computers logged in [16]. 31% of participants use the same password for all accounts [23]. In separate studies, one-third of users report sharing their passwords with friends, loved ones, or coworkers [37], and users report reusing 50% of passwords [32]. Grawemeyer and Johnson found that users reuse passwords for up to four sites, although this number may be significantly higher with the increasing numbers of accounts of which users need to keep track. 43% of users never change their passwords [23]. Gender and age have been found to predict strength of passwords, with females creating weaker passwords than males, and young people studying humanities creating weaker passwords than other demographic groups [29]. Also, users who are consciousness or have propensities towards risk-taking create weaker passwords [29].

End users put security at risk when they fall for phishing scams [17,33,38,41]. Emails from unknown sources should be approached cautiously [3,18,48]. Phishing scams can result in the downloading of malware or the release of sensitive information, such as usernames, passwords, and credit card information [5,13,34]. Users need to be suspicious of email that has a mismatched name and address in the "From" field; that have spelling mistakes, incorrect grammar, or strange spacing; that encourage immediate action; that have a mismatch between the link text and the link addresses shown by hovering the mouse; or that intuitively seems like something is not right [13].

Previous research has found that the response rates for phishing emails are quite high. In 2004, 500 military cadets were phished, and 80% of them clicked an embedded link [9]. In 2005, 10,000 employees from New York State were phished, and 15% began entering personal information before they were warned not to [9]. Dodge and colleagues [22] trained participants from an organization about how not to respond to phishing emails. Later on, the researchers sent simulated phishing emails to participants to test their tendencies to respond. Simulated phishing emails included malicious embedded links, malicious attachments, and requests to send sensitive information. 50% of participants followed a link to a website, 38% opened the attachment, and 46% sent sensitive information. Caputo and colleagues [13] trained employees at an organization not to respond to suspicious emails. After training, the researchers measured rates of falling for phishing emails and rates of reporting them. The click rate for embedded links after training was 60%. Holm and colleagues [34] tested responses to simulated phishing emails in the electric power domain. The researchers sent an email with a malicious link. The email was in English or in Swedish, whichever was the employees' native language. 7.5% of participants clicked on the link for the email in English, and 30.2% clicked on the link in the email in Swedish. Europe [23] tested users' tendencies to respond to a phishing email that offered chocolate if users would supply their password. Shockingly, 21% of participants responded with their password. Spam protection can help protect against phishing attacks [14]. 75% of surveyed home users thought that they had spam protection, but only 42% actually did [46]. A separate survey reported that 66% of home users have a spam filter [55].

Personal information can also be stolen when users post this information on social networking sites [5,33]. 59% of surveyed participants reported using their real name on social networking sites, 62% reported disclosing their email address, and 45% reported disclosing their date of birth and full name [55]. 77% of users reported restricting their privacy settings [20]. Personal information can be used in social engineering attacks such as spear phishing, in which personal information is included in fraudulent emails to increase the chances of a response [13].

Browsing an infected website, using unsecured Wi-Fi hotspots, or using infected USB drives can compromise a network [17,41]. These behaviors can lead to problems, like the disclosure of a password or the downloading of malware. Most surveyed participants did not understand what it means when a web browser asks if they trust a website's credentials [4]. They proceeded to a site or not depending on how much they wanted to access the site.

In addition to protecting computers, end users need to protect other devices that connect to the internet. Markelj and Bernik