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/

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

[42] examined awareness of and behaviors towards security threats specific to mobile phones. A questionnaire revealed that 75% of participants were aware of the threat of theft. Fewer were aware of other threats. 39.1% were aware of the threat of malware, 39.7% were aware of spyware threats, and 45.3% were aware of rootkit threats. The most common form of protection used on mobile phones was authentication. Many participants used a PIN password. However, 56.8% of participants did not use authentication. 40% of participants were aware that they could erase data remotely if their phone was stolen but did not use this option.

There are individual differences among users' cyber hygiene habits. Older age has been found to be a main predictor of not following best practices for cyber hygiene [30,58], even though 43% of adults have reported having had security training [45], and only 19% of college age users report having had security training [7]. Older users' deficiencies in following standard practices and their greater likelihood of sharing personal information, such as passwords, may be due to less use, familiarity, and knowledge about technology [30].

1.3. Deficiencies in previous studies

While there have been multiple studies involving various users and aspects of cyber hygiene, there currently is not a comprehensive up-to-date survey which explores cyber hygiene by considering individual differences and the users' level of knowledge. Results from past surveys have been inconsistent in their findings; this current study aims to address those issues. Previously, a survey by America Online and the National Cyber Security Alliance found that 67% of surveyed home users did not have any antivirus software [4]. However, Talib et al. [55] found that 97% of users did have antivirus software at home. AOL said that 72% of users did not correctly configure their firewall protection (2004), and Talib et al. [55] reported that 72% of people who are not trained on the topic did use firewall protection. There are also discrepancies in the data that describes the use of Spam protection. NCSA [46] says that 42% of home users had spam protection, while Talib et al. [55] reported that 66% of non-trained home users had a spam filter. Previous surveys do cover several topics regarding cyber hygiene, but there are currently no comprehensive surveys on cyber hygiene as a whole. For example, van Schaik and colleagues [57] examined how risk perceptions (e.g., severity of risk) lead to protective behaviors. Also, Gratian and colleagues [29] examined how characteristics of risk-taking, conscientiousness, decision-making styles, and gender predicted security behavior intentions, but many demographic and descriptive factors have yet to be explored in a comprehensive survey. Furthermore, the majority of previous surveys only examine some of the many behaviors that would compose good cyber hygiene. For example, Gratian and colleagues [29] examined only the security behavior intentions of device securement, password generation, proactive awareness, and updating. Van Schaik and colleagues [57] examined only the protective behaviors of using antivirus and firewall and installing updates.

1.4. Needs addressed by the current study

This survey study will explore the cyber hygiene knowledge of concepts, the knowledge of threats, and the behaviors of end users in an extensive and updated approach that will include topics of security software, authentication, phishing scams, social networking, web browsing, Wi-Fi hotspot usage, and USB drive use. Context for the survey was developed based on topics brought up in previous literature and topics discussed on government websites that describe good cyber hygiene (see Table 1; Cyber hygiene Practices). We will address the inconsistencies in the results of previous studies done by AOL [4], NCSA [46], Talib et al. [55], and Kaye [37], we will provide up-to-date findings about behaviors and knowledge about password usage and phishing, and we will investigate possible user characteristics (i.e. the impacts of age, gender, attack history, expertise, and training) that might indicate good or poor cyber hygiene. The current study will provide comprehensive data about the cyber hygiene of end users in today's cyber threatening world.

Table 1
Topics found on government websites.

Cyber Hygiene Practices
Update your applications, software, and operating systems
Secure your browser and add-ons
Back up your data and files
Secure your wireless network
Use firewalls
Use anti-virus and separate anti-spyware software
Do not open emails or attachments from unknown sources
Use hard-to-guess passwords and keep them private
Password protect your Wi-Fi
If in doubt, do not visit the website
Turn off router when not in use
Encrypt sensitive files the computer
Perform weekly anti-virus scans

Table 2
Gender and technology use.

Age range	Females (%)	Mean hours spent using technology per day (SD)
18–24	48.39	10.48 (3.79)
25–29	54.55	8.64 (2.97)
30–34	43.18	11.23 (8.23)
35–44	54.72	8.94 (5.47)
45–54	54.35	8.78 (2.79)
55+	60.00	7.32 (3.298)

Table 3
Age ranges.

Age	Mean age	SD
18–24	21.61	1.75
25–29	26.98	1.39
30–34	31.73	1.52
35–44	38.7	2.97
45–54	50	3.12
55+	62.02	5.46

2. Methods

2.1. Participants

A total of 312 participants (females = 144) were recruited through Mechanical Turk and were compensated $1.40 for their efforts. There were 52 participants in each age range. The age ranges established by Mechanical Turk were 18–25, 25–30, 30–35, 35–45, 45–55, and 55+. These ranges were adjusted to offset the ranges by a year, in order to eliminate overlap. These new age ranges are 18–24 ($N = 31$), 25–29 ($N = 44$), 30–34 ($N = 44$), 35–44 ($N = 53$), 45–54 ($N = 46$), and 55+ ($N = 50$). After examination of the attention check question, data from 44 participants were omitted, giving a new total of 268 participants (females = 142; country of origin: 92% US). See Tables 2–4 for additional demographics.

2.2. Stimuli and procedure

Self-report was found to be a valid measure for this subject area. Reports of non-secure behaviors have resulted in honest reporting of when they do not behave securely [51]. There have

Table 4
Level of education.

Level of education	*N*	%
Less than High School	1	0.37
High School Graduate	24	8.96
Some College	66	24.63
Professional Degree	33	12.31
2 Year Degree	37	13.18
4 Year Degree	102	38.06
Doctorate	5	1.87

been many useful studies about cyber hygiene that have relied on self-report, the current study included. The survey was implemented using Qualtrics. Participants were recruited through Mechanical Turk. The survey consisted of four sections of questions: demographics, knowledge of concepts, knowledge of threats, and behaviors. Questions fell into one of ten cyber hygiene categories believed to be of importance based on previous research: security software, authentication, phishing scams, social networking, browsing infected websites, using unsecured Wi-Fi hotspots, using an infected USB drive, mobile phones, and miscellaneous practices.

The Knowledge of Concepts section consisted of 16 multiple choice test-like questions which measured participants' knowledge of specific cyber hygiene concepts. Participants were given a statement or a question and had to choose the correct answer from among four choices. An example of a concept question is, "What are over-the-shoulder attacks/ shoulder surfing?" Knowledge of Concepts questions had a Cronbach's alpha of 0.50.

In the Knowledge of Threats section, participants were given 18 statements that involved threats or outcomes associated with cyber hygiene. Participants were asked to report the degree to which they agreed with the given threat statement on a Likert scale, with the options being Strongly Agree, Somewhat Agree, Neither Agree Nor Disagree, Somewhat Agree, and Strongly Disagree. The Threats and Concepts scores were combined to create an overall knowledge score. In order to combine the Threats and Concepts, we changed the score of Threats from a 5-point Likert scale to a binary score by deeming answers marked Neither Agree Nor Disagree, Somewhat Disagree, and Strongly Disagree as incorrect or correct responses and answers of Strongly Agree and Somewhat Agree as incorrect or correct responses. An example of a Threats question is "Accessing sensitive information on an unsecured public Wi-Fi hotspot makes the user vulnerable to an intruder gaining access to all of the user's activity occurring over the network." Knowledge of Threats and Concepts had a Cronbach's alpha of 0.78.

The Behavior section consisted of 57 diverse behavior statements in which participants reported their frequency of engagement on a 5-point Likert scale ranging from Always to Never. Participants were given a specific behavior that was either cyber hygienic or not and were asked to disclose their level of frequency, reporting that they do the given behavior Always, Most of the Time, Half of the Time, Sometimes, or Never. We also changed this measurement to a binary scale in order to form correct and incorrect answers. An example of a Behavior questions is, "Do you disable browser plug-ins while not in use?" Cronbach's alpha for Behaviors questions was 0.88.

3. Results

Initially, participants were surveyed on their knowledge of cyber hygiene concepts, their knowledge of cyber hygiene threats, and their behaviors related to cyber hygiene. All of the figure error bars represent standard deviation.

In the following results section, we first present, in text and in tables, the findings about participants' behaviors and their knowledge of concepts and threats as they relate to cyber hygiene. These findings can resolve discrepancies in previous research about knowledge about and usage of passwords, phishing scams, antivirus, firewall, anti-spyware, and social media. Next, we present findings about characteristics that may or may not predict good or poor cyber hygiene, including age, attack history, expertise, and training.

Table 5
Primary uses of home computer.

	N	%
Email	247	92.16
Banking	216	80.6
Paying bills	203	75.75
Web browsing	250	93.28
Gaming	127	47.39
Social media	220	82.1
Work-related tasks	202	75.37
School work	53	19.78
Other	14	5.22

Note: Percentage represents the proportion of users who agreed with this question. Participants checked all that applied.

Table 6
Types of devices in household.

	N	%
Desktop	168	62.69
Laptop	220	82.1
Smart phone	207	77.24
Tablet	112	41.79
Other	3	1.12

Note: Percentage represents proportion of users who agreed with this question.

Table 7
Antivirus general use.

Do you use antivirus?	*N*	%
18–24	23	74.19
25–29	34	77.27
30–34	38	86.36
35–44	43	81.13
45–54	41	89.13
55+	44	88.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

We determined the percentage of users who, more than half the time, followed best practices for password usage and in response to phishing scams. 91% of users create passwords that were at least eight characters long. 84% of users use upper and lowercase letters. Only 71% of users use special characters. 85% of users use personal information when creating passwords. Only 54% of users avoid the use of dictionary words. 50% of users use the same password for multiple accounts. Only 41% of users change their passwords. Only 5% of users do not share their passwords with others. 81% of users are mindful of over-the-shoulder attacks in public places. Also, good cyber hygiene was not demonstrated for phishing attacks. 96% of users click on embedded links from unknown senders. 98% of users download attachments from unknown senders. 94% of users send sensitive information over email when a sender requests it. 84% of users use a spam filter. For more complete reports on demographic cyber hygiene, see Tables 5 and 6 and Fig. 1. For reports on cyber hygiene behaviors, see Tables 7–20. The dataset has been shared [12].

Below, we report results about participants' age and cyber hygiene, gender and cyber hygiene, their reporting of having been attacked in the past and their current cyber hygiene, expertise and cyber hygiene, and training and cyber hygiene.

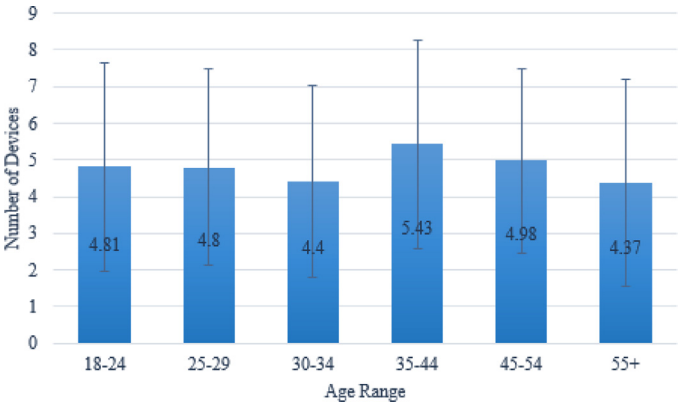


Fig. 1. Mean number of computing devices per household.

Table 8
Antivirus updates.

Do you keep your antivirus software up to date?	*N*	%
18–24	21	67.74
25–29	29	65.91
30–34	40	90.91
35–44	40	75.47
45–54	41	89.13
55+	44	88.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 9
Antivirus specific use.

How often do you run antivirus scans?	*N*	%
18–24	8	25.81
25–29	18	40.91
30–34	22	50.00
35–44	21	39.62
45–54	30	65.22
55+	30	60.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 10
Firewall general use.

Do you use firewalls on your home computer?	*N*	%
18–24	21	67.74
25–29	36	81.82
30–34	33	75.00
35–44	41	77.36
45–54	39	84.78
55+	46	92.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 11
Firewall settings.

Do you change your firewall settings to the strictest level when needed?	*N*	%
18–24	12	38.71
25–29	19	43.18
30–34	19	43.18
35–44	23	43.40
45–54	39	84.78
55+	21	42.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 12
Anti-spyware general use.

Do you use anti-spyware software?	*N*	%
18–24	15	48.39
25–29	28	63.64
30–34	29	65.91
35–44	34	64.15
45–54	34	73.91
55+	39	78.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 13
Anti-spyware specific use.

How often do you run anti-spyware scans?	*N*	%
18–24	7	22.58
25–29	17	38.6
30–34	21	47.73%
35–44	22	41.51
45–54	27	58.70
55+	28	56.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 14
Pop up blocker use.

Do you use a pop-up blocker?	*N*	%
18–24	27	87.10
25–29	39	88.64
30–34	39	88.64
35–44	44	83.02
45–54	37	80.43
55+	35	70.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 15
Providing name on social media.

Do you use your real name on social media sites?	*N*	%
18–24	15	48.39
25–29	15	34.09
30–34	20	45.45
35–44	19	35.85
45–54	28	60.87
55+	27	54.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 16
Providing date of birth on social media.

Do you provide your real date of birth on social media sites?	*N*	%
18–24	9	29.03
25–29	20	45.45
30–34	25	56.82
35–44	31	58.49
45–54	33	71.74
55+	36	72.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

3.1. Age and behaviors

An independent samples ANOVA (age groups: 18–24, 25–29, 30–34, 35–44, 45–54, and 55+) was conducted to explore specific behaviors related to cyber hygiene behaviors. See Fig. 2 for descriptive statistics. Differences were found among behaviors, $F(5,$

Table 17
Providing address on social media.

Do you provide your mailing address on social media sites?	*N*	%
18–24	24	77.42
25–29	40	90.91
30–34	41	93.18
35–44	46	86.79
45–54	42	91.30
55+	47	94.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 18
Providing phone number on social media.

Do you provide your phone number on social media sites?	*N*	%
18–24	22	70.97
25–29	40	90.91
30–34	38	86.36
35–44	48	90.57
45–54	43	93.48
55+	48	96.00

Note: Percentage the represents the proportion of users within each age group who selected "always" or "almost always."

Table 19
Providing email on social media.

Do you provide your email address on social media sites?	*N*	%
18–24	15	48.39
25–29	33	75.00
30–34	27	61.36
35–44	38	71.70
45–54	37	80.43
55+	42	84.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

Table 20
Privacy setting use on social media.

Do you check your privacy settings on your social media accounts?	*N*	%
18–24	24	77.42
25–29	32	72.73
30–34	36	81.82
35–44	33	62.26
45–54	26	56.52
55+	26	52.00

Note: Percentage represents the proportion of users within each age group who selected "always" or "almost always."

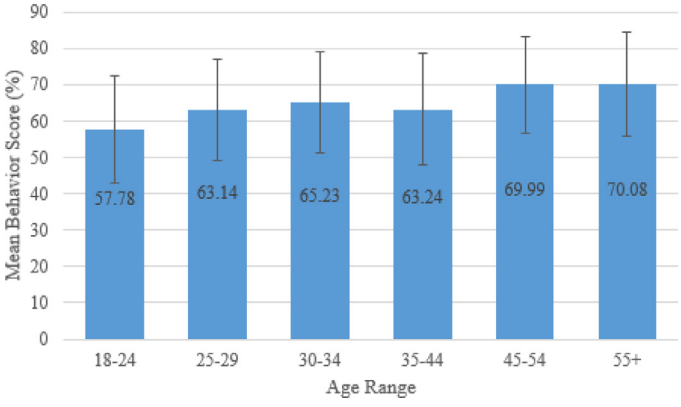


Fig. 2. Mean behavior score by age.

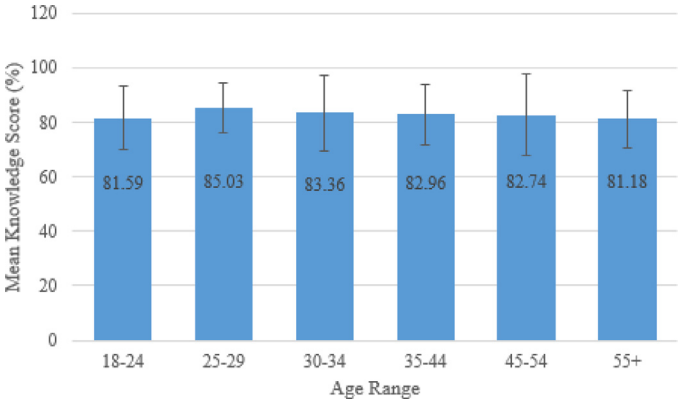


Fig. 3. Mean knowledge score by age.

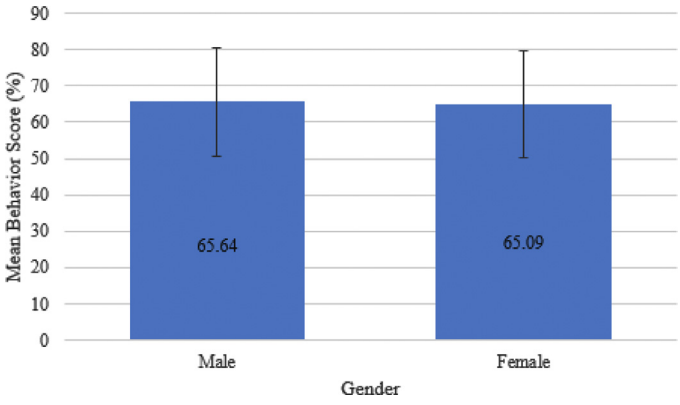


Fig. 4. Mean behavior score by gender.

262) = 4.25, $p < .001$, partial $\eta^2 = 0.075$. Post hoc comparisons revealed that the oldest age groups, 45 to 54 and 55 and above, had more secure behaviors than the youngest age group, 18 to 24, $p < .05$ for both comparisons. No differences were found between behaviors for other age group comparisons.

3.2. Age and knowledge

An independent samples ANOVA (age groups: 18–24, 25–29, 30–34, 35–44, 45–54, and 55 and above) was conducted to explore cyber hygiene knowledge. See Fig. 3 for descriptive statistics. No differences were found among knowledge, $F(5, 262) = 0.56$, $p = .727$, partial $\eta^2 = 0.011$.

3.3. Gender and behaviors

An independent sample *t*-test (gender: male, female) was conducted to explore cyber hygiene behavior. See Fig. 4 for descriptive statistics. No differences were found among behaviors, $t(266) = 0.31$, $p = .761$, $d = 0.037$.

3.4. Gender and knowledge

An independent sample *t*-test (gender: male, female) was conducted to explore cyber hygiene knowledge. See Fig. 5 for descriptive statistics. Significant differences were found among behaviors, $t(266) = 3.09$, $p = .002$, $d = 0.378$.

3.5. Having been attacked and behaviors

An independent sample *t*-test (attacked: yes, no) was conducted to explore cyber hygiene behavior. See Table 21 and Fig. 6 for de-

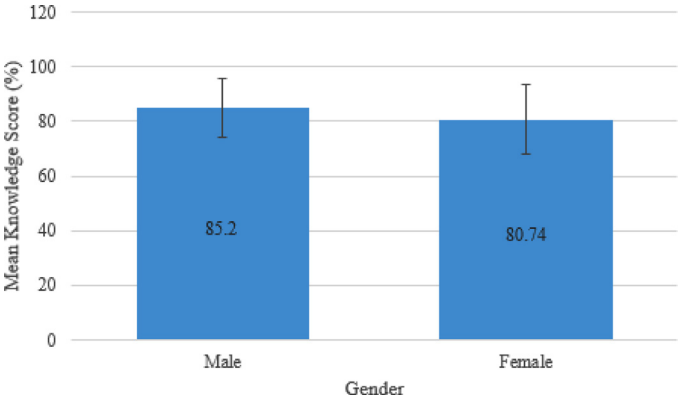


Fig. 5. Mean knowledge score by gender.

Table 21
Attack history and home computer use.

	N	%
Do you access sensitive information on your home computer?	230	85.82
Are you in charge of your household's security?	199	74.25
Have you ever been the target of a cyber security attack in the past?	48	17.91

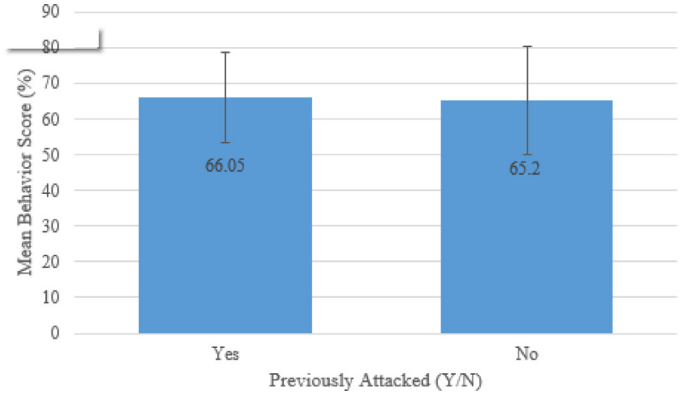


Fig. 6. Mean behavior score by attacks.

Table 22
Expertise and training.

	N	%
Major in a technical field?	66	24.63
Received training?	55	20.52
Taken classes?	48	17.91
Expert?	15	5.6

scriptive statistics. No differences were found among behaviors, $t(266) = 0.36$, $p = .719$, $d = 0.057$.

3.6. Having been attacked and knowledge

An independent sample *t*-test (attacked: yes, no) was conducted to explore knowledge related to cyber hygiene. See Table 21 and Fig. 7 for descriptive statistics. No differences were found among knowledge, $t(1, 266) = 0.66$, $p = .505$, $d = 0.106$.

3.7. Experts and behavior

An independent sample *t*-test (expert: yes, no) was conducted to explore cyber hygiene behaviors. See Table 22 and Fig. 8 for descriptive statistics. Differences were found among behaviors,

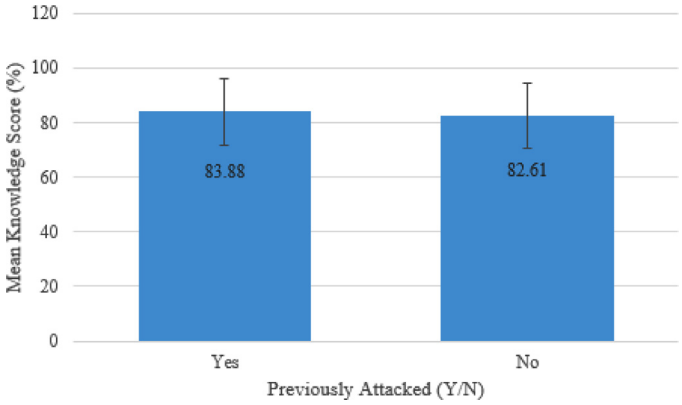


Fig. 7. Mean knowledge score by attacks.

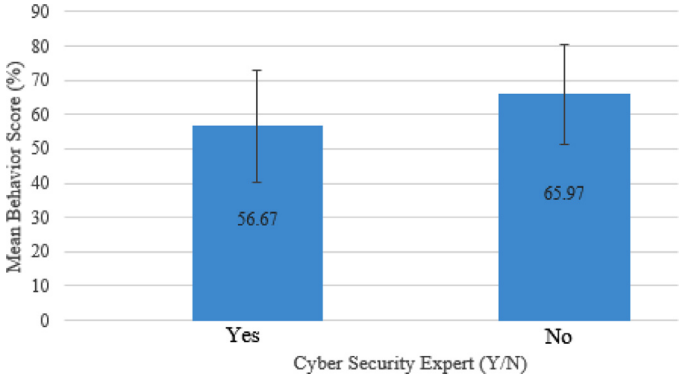


Fig. 8. Mean behavior scores for experts.

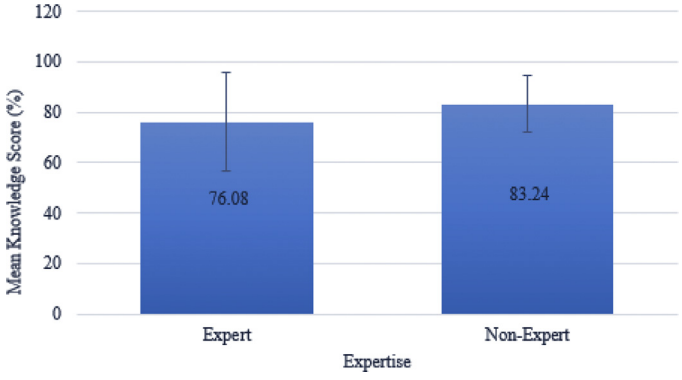


Fig. 9. Mean knowledge score for experts.

$t(266) = 2.37$, $p = .018$, $d = 0.630$, such that self-identified experts had less secure behaviors than self-identified non-experts.

3.8. Experts and knowledge

An independent sample *t*-test (expert: yes, no) was conducted to explore cyber hygiene knowledge. See Table 22 and Fig. 9 for descriptive statistics. Differences were found among knowledge, $t(266) = 2.26$, $p = .025$, $d = 0.601$, such that self-identified experts had less knowledge about cyber hygiene than self-identified non-experts.

3.9. Trained and behavior

An independent sample *t*-test (trained: yes, no) was conducted to explore cyber hygiene behavior. See Fig. 10 for descriptive statis-

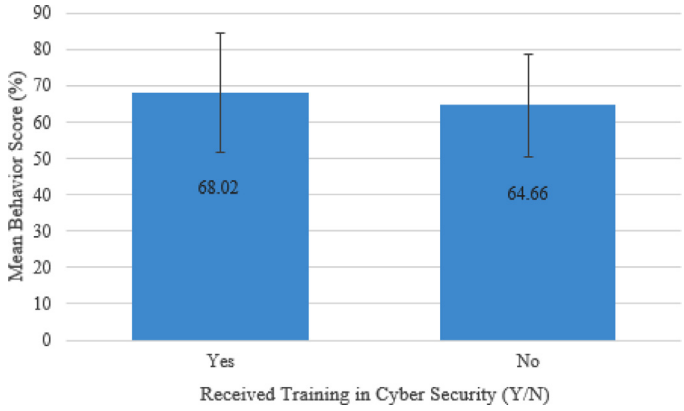


Fig. 10. Mean behavior score by training.

Fig. 11. Mean knowledge score by training.

tics. No differences were found among behaviors, $t(266) = 1.51$, $p = .131$, $d = 0.229$.

3.10. Trained and knowledge

An independent sample *t*-test (trained: yes, no) was conducted to explore cyber hygiene knowledge. See Table 22 and Fig. 11 for descriptive statistics. No differences were found among knowledge, $t(266) = 0.93$, $p = .355$, $d = 0.140$.

4. Discussion and conclusion

We explored the impact of age on cyber hygiene knowledge and behaviors. Also, we presented descriptive findings about what users know and do with respect to cyber hygiene. We found that most users have antivirus software and update it regularly, but also that most users do not run frequent-enough scans. Our findings showed that 47% to 78% of users employ antivirus software. This is in line with the previous finding of 67% from AOL [4] and disagreed with Talib and colleagues' previous finding of 97%. Most users employ a firewall, but most users do not change the firewall settings when needed. Our finding, that 68% to 92% of participants used a firewall, agreed with Talib and colleagues' previous finding that 72% of users use firewall. Our findings that four out of five age groups had a majority of participants who did not change firewall settings when needed did not concur with previous findings from AOL that 72% of users did not have a correctly configured firewall (2004). And our findings did not concur with van Schaik and colleague's [57] finding that participants have more protective behavior in terms of using anti-virus software than firewall. We learned that anti-spyware software is more often used by older participants than by younger participants. Many older and younger users share too much personal information on social media, such as their address and their phone numbers, and most do not check their privacy settings.

We also examined what characteristics of participants could impact good cyber hygiene knowledge and behavior. Our findings about these characteristics were insightful. It is commonly believed that age has an impact on cyber hygiene behaviors [30,58]. However, older users tended to behave more securely than younger users. This finding was counterintuitive because younger people are believed to have the most know-how about technology [30]. Also, surprisingly, there was no difference in cyber hygiene knowledge among age groups. When it comes to cyber hygiene, older users, who are often described as having less familiarity with technology, are not at a disadvantage. In fact, they are the least susceptible to attacks. Our findings agree with McGill and Thompson's [43] finding that there was no difference due to age on security perceptions and behaviors.

We found that males had more knowledge about cyber hygiene than females. This finding agrees with Gratian and colleagues' [29] previous finding that females created weaker passwords and updated software less often than males. However, the current survey showed that despite having more knowledge, males did not differ on cyber hygiene behavior from females.

We examined whether having been attacked in the past would impact cyber hygiene. Presumably, after users have been attacked, they will behave more securely in the future and perhaps will know more about how to avoid attacks. Another possibility is that users who have been victims of attacks have worse cyber hygiene and will have less secure behaviors and knowledge about security. Surprisingly, neither of these positions was supported. Whether or not a user had been attacked in the past had no impact on their current cyber hygiene.

Another surprising finding came from our examination of self-identified experts' cyber hygiene. We would expect users who describe themselves as "cyber security experts" to behave more securely and to have more knowledge about cyber hygiene than other users. However, our self-described experts reported less secure behaviors and had less knowledge about cyber hygiene than did other participants.

Finally, we reported our findings about training and cyber hygiene. We found that 81% of users had some security training, which was more than the findings of 43% for adults [45] and 19% for college age users found in previous studies [7]. We would expect that users who have had some training in cyber hygiene (e.g., a tutorial at work) would behave more securely and would know more about cyber hygiene. However, training did not increase users' cyber hygiene behaviors or knowledge. Surprisingly, current training programs seemed to have no impact.

The current study described cyber hygiene knowledge and behaviors for a large, diverse sample of users. We found, consistent with previous research, that users are not using best practices to protect passwords or to defend against phishing attacks. Our findings provide some additional insight. Hopefully, future research studies will focus on developing more effective training programs and on ways to encourage younger users to behave more securely.

5. Future directions

Our findings can be used by designers when they create systems that need to be used securely. Clearly, we need to provide explicit security clues and better training to all age groups equally regardless of their experience. And, we need to investigate further the types of training users are receiving to determine why training cyber hygiene does not appear to be effective. Users report they most commonly get information about behaving securely

from public information websites, IT professionals, friends or relatives [28], or at a local computer store [54]. Researchers should investigate whether these sources of information are reliable and their degree of effectiveness. Fagan and Khan [24] found that users tend to follow safe practices more when they perceive more benefits to those behaviors, and tend to not follow safe practices more when they perceive more costs to following the safe behaviors. Thus, future research needs to focus on how training can better communicate benefits and costs. Aytes and Conolly [7] identified that users behave more protectively when they have an awareness of what constitutes safe practices and awareness of consequences of not behaving securely. However, the current study showed that having had training or being an expert does not lead to more protective behaviors. Our findings that training has been ineffective is in line with previous findings that cyber security awareness campaigns have been ineffective [8]. Providing users with knowledge is the first step, but we need to determine how to improve users' cyber hygiene attitudes and behaviors.

Acknowledgments

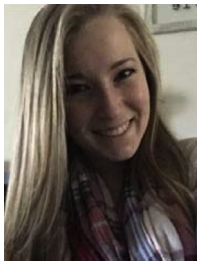
This research was supported in part by NSF under grant CNS-1659795. M.E. Edwards and J. D. Still developed the study concept. M. E. Edwards collected and analyzed the survey data. A. A. Cain drafted the manuscript and interpreted the data. All authors revised drafts of the manuscript.

References

[1] Almeida VA, Doneda D, de Souza Abreu J. Cyberwarfare and digital governance. IEEE Internet Comput 2017;21(2):68–71. doi:10.1109/MIC.2017.23.
[2] Aloul FA. The need for effective information security awareness. J Adv Inf Technol 2012;3(3):176–83. doi:10.4304/jait.3.3.
[3] Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. Mis Q 2010;34(3):613–43.
[4] AOL/NCSA. AOL/NCSA online safety study. America Online and National Cyber Security Alliance; 2004. Retrieved from http://www.staysafeonline.info/news/safety_study_v04.pdfO.
[5] Arachchilage NAG, Love S. Security awareness of computer users: a phishing threat avoidance perspective. Comput Hum Behav 2014;38:304–12. doi:10.1016/j.chb.2014.05.046.
[6] Ashford W. Millions of web users at risk from weak passwords. ComputerWeekly; 2009. Retrieved from http://www.computerweekly.com/Articles/2009/09/07/237569/Millions-of-web-users-at-risk-from-weak-passwords.htm?printerfriendly=true 07.
[7] Aytes K, Conolly T. A research model for investigating human behavior related to computer security. In: Proceedings of the AMCIS; 2003. p. 260.
[8] Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? UK: Oxford. Retreived from http://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf.
[9] Bank D. Spear phishing tests educate people about online scams. Wall Street J 2005. Retrieved from http://online.wsj.com/public/article/0,SB112424042313 615131-z_8jLB2WkfcVtgdAWf6LRh733sg_20060817,00.html?mod=blogs.
[10] Barton B, Barton M. User-friendly password methods for computer-mediated information systems. Comput. Secur. 1984;3(3):186–95. doi:10.1016/0167-4048(84)90040-3.
[11] Bulgurcu B, Cavusoglu H, Benbasat I. Roles of information security awareness and perceived fairness in information security policy compliance. In: Proceedings of the AMCIS; 2009. p. 419–30.
[12] Cain AA, Still JD. Usability comparison of over-the-shoulder attack resistant authentication schemes. Cyber hygiene data. Cain AA, Edwards ME, Still JD, editors. Mendeley Data.; 2018.
[13] Caputo DD, Pfleeger SL, Freeman JD, Johnson ME. Going spear phishing: Exploring embedded training and awareness. IEEE Sec Priv 2014;12(1):28–38. doi:10.1109/MSP.2013.106.
[14] Chaudhry JA, Rittenhouse RG. Phishing: classification and countermeasures. In: Proceedings of the 7th international conference on multimedia, computer graphics and broadcasting; 2015. p. 28–31. doi:10.1109/MulGraB.2015.17.
[15] Choong Y, Greene K. What'sa special character anyway? effects of ambiguous terminology in password rules. In: Proceedings of the human factors and ergonomics society annual meeting, 60; 2016. p. 760–4.
[16] Cone BD, Thompson MF, Irvine CE, Nguyen TD. Cyber security training and awareness through game play. In: Proceedings of IFIP international information security conference; 2006. p. 431–6. doi:10.1007/0-387-33406-8_37.
[17] Coventry L, Briggs P, Jeske D, van Moorsel A. Scene: a structured means for creating and evaluating behavioral nudges in a cyber security environment. In: Proceedings of the international conference of design, user experience, and usability; 2014. p. 229–39. doi:10.1007/978-3-319-07668-3_23.
[18] Cox A, Connolly S, Currall J. Raising information security awareness in the academic setting. Vine 2001;31(2):11–16. doi:10.1108/03055720010803961.
[19] Dawson LA, Stinebaugh J. Methodology for prioritizing cyber-vulnerable critical infrastructure equipment and mitigation strategies. Sandia National Laboratories; 2010. *(No. SAND2010-1845).*
[20] Debatin B, Lovejoy JP, Horn AK, Hughes BN. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J Comput Med Commun 2009;15(1):83–108. doi:10.1111/j.1083-6101.2009.01494.x.
[21] Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Inf Syst J 2001;11(2):127–53. doi:10.1046/j.1365-2575.2001.00099.x.
[22] Dodge RC, Carver C, Ferguson AJ. Phishing for user security awareness. Comput Secur 2007;26(1):73–80. doi:10.1016/j.cose.2006.10.009.
[23] Europe I. Woman 4 times more likely than men to give passwords for chocolate. Press Rel 2008. Retrieved from http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071.
[24] Fagan M, Khan MMH. Why do they do what they do? A study of what motivates users to (not) follow computer security advice. In: Proceedings of the twelfth symposium on usable privacy and security (SOUPS); 2016. p. 59–75.
[25] FBI. 2015 internet crime report. Federal Bureau of Investigation Internet Crime Complaint Center (ICE3); 2015. Retrieved from https://www.ic3.gov/media/annualreports.aspx.
[26] Florêncio D, Herley C, Coskun B. Do strong web passwords accomplish anything. HotSec 2007;7(6).
[27] Furnell S. Why users cannot use security. Comput Secur 2005;24(4):274–9. doi:10.1016/j.cose.2005.04.003.
[28] Furnell SM, Bryant P, Phippen AD. Assessing the security perceptions of personal Internet users. Comput Secur 2007;26(5):410–17. doi:10.1016/j.cose.2007.03.001.
[29] Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Comput Secur 2018;73:345–58. doi:10.1016/j.cose.2017.11.015.
[30] Grimes GA, Hough MG, Mazur E, Signorella ML. Older adults' knowledge of internet hazards. Educ Gerontol 2010;36(3):173–92.
[31] Goodhue D, Straub D. Security concerns of system users: A study of perceptions of the adequacy of security. Inf Manag 1991;20:13–27. doi:10.1016/0378-7206(91)90024-V.
[32] Grawemeyer B, Johnson H. Using and managing multiple passwords: a week to a view. Interact Comput 2011;23(3):256–67. doi:10.1016/j.intcom.2011.03.007.
[33] Halevi T, Lewis J, Memon N. A pilot study of cyber security and privacy related behavior and personality traits. In: Proceedings of the 22nd international conference on World Wide Web; 2013. p. 737–44.
[34] Holm H, Flores WR, Ericsson G. Cyber security for a smart grid-what about phishing?. In: Proceedings of innovative smart grid technologies Europe; 2013. p. 1–5. doi:10.1109/ISGTEurope.2013.6695407.
[35] Hoonakker P, Bornoe N, Carayon P. Password authentication from a human factors perspective: Results of a survey among end-users. In: Proceedings of the human factors and ergonomics society annual meeting, 53; 2009. p. 459–63.
[36] Hu Q, Hart P, Cooke D. The role of external influences on organizational information security practices: An institutional perspective. In: Proceedings of the 39th annual Hawaii international conference on system sciences, 6; 2006 127a-127a.
[37] Kaye J. Self-reported password sharing strategies. In: Proceedings of the SIGCHI conference on human factors in computing systems; 2011. p. 2619–22. doi:10.1145/1978942.1979324.
[38] Konieczny F, USAFR NJT. SEADE: Countering the futility of network security. Air Space Power J 2015;29(5):4.
[39] Labuschagne WA, Veerasamy N, Burke I, Eloff MM. Design of cyber security awareness game utilizing a social media framework. In: Proceedings of information security South Africa; 2011. p. 1–9. doi:10.1109/ISSA.2011.6027538.
[40] Long RM. Using phishing to test social engineering awareness of financial employees. Eastern Washington University; 2013. Doctoral dissertation.
[41] Loukas G, Patrikakis C. Cyber and physical threats to the internet of everything. Cutter IT J 2016;29(7):5–11.
[42] Markelj B, Bernik I. Safe use of mobile devices arises from knowing the threats. J Inf Sec Appl 2015;20:84–9. doi:10.1016/j.jisa.2014.11.001.
[43] McGill T, Thompson N. Old risks, new challenges: exploring differences in security between home computer and mobile device use. Behav Inf Technol 2017;36(11):1111–24. doi:10.1080/0144929X.2017.1352028.
[44] Mills JR. Counterinsurgency in cyberspace. Georgetown J Int Affairs 2011:157–62.
[45] National Cyber Security Alliance and Norton by Symantec. 2010 NCSA/Norton by Symantec online safety study. National Cyber Security Alliance and Norton by Symantec; 2010.
[46] NCSA and Symantec. NCSA-Symantec national cyber security awareness study newsworthy analysis. NCSA and Symantec; 2008. Retrieved from https://und.edu/it-security/awareness/_files/docs/2008-ncsa-symantec-study-analysis.pdf .
[47] Ovelgönne M, Dumitras T, Prakash BA, Subrahmanian VS, Wang B. Understanding the relationship between human behavior and susceptibility to cyber

attacks: a data-driven approach. ACM Trans Intel Syst Technol 2017;8(4):51. doi:10.1145/2890509.
[48] Pelgrin W. A model for positive change: influencing positive change in cyber security strategy, human factor, and leadership. Best practices in computer network defense: incident detection and response; 2014. doi:10.3233/978-1-61499-372-8-107.
[49] Pike M. The magazine for the IT professional. The Charted Institute for IT; 2011. British Computer Society.
[50] Ponemon Institute. 2016 cost of cyber crime study & the risk of business innovation. Ponemon Institute; 2016. Retrieved from: http://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation .
[51] Russell JD, Weems CF, Ahmed I, Richard GG III. Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. J Cyber Sec Technol 2017:1–12. doi:10.1080/23742917.2017.1345271.
[52] Seidenberger S. A new role for human resource managers: social engineering defense. Cornell HR Review; 2016. Retrieved June 2017 from Cornell University, ILR School site: http://digitalcommons.ilr.cornell.edu/chrr/95 .
[53] Straub D, Welke R. Coping with systems risk: security planning models for management decision making. MIS Q 1998;22(4):441–69. doi:10.2307/249551.
[54] Szewczyk P, Furnell S. Assessing the online security awareness of Australian Internet users. In: Proceedings of the 8th Annual Security Conference: Discourses in Security Assurance & Privacy. Las Vegas, NV, USA; 2009.
[55] Talib S, Clarke NL, Furnell SM. An analysis of information security awareness within home and work environments. In: Proceedings of the International Conference on Availability, Reliability, and Security; 2010. p. 196–203. doi:10.1109/ARES.2010.27.
[56] US-CERT. Choosing and protecting passwords. US-CERT; 2009. National Cyber Alert System Cyber Security Tip ST04-002. Retrieved from http://www.us-cert.gov/cas/tips/ST04-002.html .
[57] van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P. Risk perceptions of cyber-security and precautionary behaviour. Comput Hum Behav 2017;75:547–59. doi:10.1016/j.chb.2017.05.038.
[58] Whitty M, Doodson J, Creese S, Hodges D. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychol Behav Soc Netw 2015;18(1):3–7.
[59] Yale University. HIPAA security compliance—system administrator reference guide. Yale University; 2005. Retrieved from http://hipaa.yale.edu/security/sysadmin/referenceguide.html.

Ashley Cain is a Ph.D. student in human factors psychology at Old Dominion University where she focuses on the human side of cyber security. She received her master's degree from San Jose State University in experimental and research psychology.



Morgan Edwards is a human factors psychology research assistant at Old Dominion University where she focuses on Cyber Security from the human error aspect. She received her Bachelor's degree in Psychology from Old Dominion University.

Dr. Jeremiah Still is an Assistant Professor at Old Dominion University. His Psychology of Design laboratory explores the relationship between human cognition and technology; specifically, he is focusing on: usable cybersecurity, visual attention, and intuitive design. He earned a Ph.D. in Human-Computer Interaction from Iowa State University.