Cybersecurity Behavior: Current Trends in the Use of Protective Measures and Reasons Why They Aren't Used

Marc Dupuis
marcjd@uw.edu
University of Washington
Bothell, Washington

Marshelle Slayton
Tamara Geiger
marshelle.slayton@gmail.com
tamara.isaura@gmail.com
University of Washington
Seattle, Washington

Frances Dewing
frances@rubica.com
Rubica, Inc.
Seattle, Washington

Abstract – Cybersecurity behavior changes over time, as do the recommendations for how one may best protect themselves from cybersecurity threats. This paper examines current trends in what protective measures people take, such as using a password manager, virtual private network (VPN), or anti-malware software. The reasons why people employ these protective measures is explored, including why some choose not to. The evidence indicates that there is an important place for security education, training, and awareness (SETA) programs to help those that do not use such measures.

Keywords: ***cybersecurity, privacy, education, training, awareness, protective measures, threats, behavior***

1. INTRODUCTION

Cybersecurity threats remain a significant concern for individuals, organizations, and nation-states. Cybersecurity behavior changes over time, as do the recommendations for how one may best protect themselves from cybersecurity threats (Dupuis, Crossler, & Endicott-Popovsky, 2016). This paper examines current trends in what protective measures people take, such as using a password manager, virtual private network (VPN), anti-malware software, two-factor authentication, and backing up data. The reasons why people employ these protective measures is explored, including why some choose not to.

A large-scale survey was conducted to explore these issues. We breakdown the results based on gender and age (18-34 and 35+). The evidence indicates that there is an important place for security education, training, and awareness (SETA) programs to help those that do not use such measures.

This paper is organized as follows. We begin by introducing some of the protective measures explores in this research. This includes an examination of why they are deemed important and how they have traditionally been used. Next, we discuss the methods employed in this study. We follow this with some analysis of the results obtained. Some concluding remarks are made related to what the data tells us, what it perhaps does not tell us, and how security education, training, and awareness (SETA) programs may have a role to play to help close the gap in the usage of various protective measures.

2. BACKGROUND

Anti-malware software is an all-encompassing term used to describe software that detects and prevents infections from various types of malicious software, including viruses, Trojan horses, worms, etc. It is used by individuals and organizations alike. Sometimes individuals may acquire anti-malware software for free through their organization or Internet Service Provider (ISP), while other times they may pay for the software.

Malicious software remains a significant threat to individuals and its success may vary based on age and gender. A study using data collected from Microsoft's Windows Defender on a sample of three million devices running Windows 10 found that both age and gender are contributing factors for malware victimization. Males were found to be 1.24 times more likely to encounter malware than females. This gender difference was most marked in the population under the age of 25, but was also evident among older users. Results suggest that age is a significant independent risk factor for malware victimization. Young users (under 25) were the most likely to encounter malware. In contrast, older users (50+) were found to be the less susceptible to encounter malware, supporting findings from earlier studies (Lévesque, Fernandez, & Batchelder, 2017).

Another study from the emerging field of neurosecurity (cognitive neuroscience applied to studying cybersecurity to gain a deeper understanding of users' unconscious security behaviors), found women exhibit higher brain activity than men when viewing malware warnings. This finding is consistent with previous research that women may be less trusting of online sites than men, and more likely to pay attention to detailed characteristics of a site when forming impressions of initial trust (Anderson, Kirwan, Eargle, Jensen, & Vance, 2015).

Beyond malware and software to protect systems from it, a virtual private network (VPN) service is a method of connecting to the internet and is used to add another layer of security and privacy to either private or public networks, such as your home or WiFi Hotspots like the local coffee shop. It creates an encrypted channel between two end points so that certain types of attacks or privacy intrusions are not successful.

A VPN reduces the likelihood that your data will be intercepted as it moves between your device and the server. Pavlicek and Sudzina (2018) found that certain factors such as gender, job type, and work experience impact the use of a VPN and proxy server. The also highlighted that where VPN's used to be used for big companies and governments, home users are increasingly employing the service for added security and privacy.

Another tool that acts in concert with these other tools to provide as much complete protection as possible is a password manager. A password manager stores all of an individual's passwords into a vault that can only be accessed with knowledge of the master password (and a second factor, if so employed). The goal behind a password manager is to exchange one long and complex password for many shorter, repeated, and less complex passwords. By doing so, security is increased significantly. No longer do individuals have to reuse the same password at multiple sites, write them down on a post-it note, or some other insecure means of information retrieval. Password managers are arguably the most effective way of mitigating the security versus usability challenge prevalent with passwords (Dupuis & Khan, 2018).

While these tools are effective, bad things still happen to the data people store. It may be due to hardware failure, losing a flash drive, or perhaps through malicious software, such as ransomware (Al-rimy, Maarof, & Shaid, 2018). Although using several tools in concert with one another (e.g., anti-malware software, password managers, VPNs, etc.) may mitigate the threat of data loss, it does not eliminate it (Dupuis et al., 2016).

Thus, it is essential that individuals have some means to backup their data on a regular basis. This may include storing it in the cloud through an automated software-based backup solution, or copying your important files to a flash drive or some other external storage device. Having proper (and redundant) backs up data is one of the most effective protective measures an individual can take to mitigate almost any kind of attack, hardware failure, or theft. Our interest here is in determining the prevalence of individuals backing up their data and the reasons why they choose to do so and why many do not.

Finally, we also examine the use of two-factor authentication. Many individuals are familiar with two-factor authentication as they may use it at their place of employment, to access online bank accounts, or perhaps even for their personal email. Thus, individuals are not strangers to two-factor authentication. Nonetheless, it remains an important protective measure in mitigating the chance that their account is accessed in an unauthorized manner. Some individuals may also be forced to use two-factor authentication rather than making an intentional decision to do so for security reasons. We assess this in this study as well since many of them may not be using two-factor authentication otherwise.

Next, we discuss the methods employed in this study.

3. METHODS

In order to explore cybersecurity behavior, the use of protective measures, and the reasons why they are used and also not used, a large-scale survey was employed. Amazon's Mechanical Turk (MTurk) was used to recruit survey participants. MTurk provides researchers with a relatively low-cost and quick turnaround platform for participant recruitment (Dupuis, Endicott-Popovsky, & Crossler, 2013; Steelman, Hammer, & Limayem, 2014). Participants generally represent a broader cross-section of the population than other methods often employed, such as college sophomores in an introductory psychology class (Sears, 1986).

IRB approval was on file prior to collecting data. Participants were compensated with $2 for their participation in the study. Two quality control questions were used. If participants failed either quality control question, the survey would conclude with an explanation of why it has concluded.

We used the Qualtrics survey platform. Logic was employed in various places within the survey to make the completing of the survey as efficient as possible for participants. For example, if a participant did not use a VPN then they were asked why later in the survey. Likewise, if a participant indicated that she did use a VPN, we would ask her why she was using this protective measure.

A total of 1,002 responses were collected. Participants are asked at the end of the survey how the effort and time required to complete the survey compared to similar work offered through the MTurk platform. Most participants indicated that it was either easier (21.5%) or comparable (69.1%) to other projects with a small number indicated more effort was required (9.4%). Of note, a pilot study consisting of 50 participants was employed beforehand to check for any issues with the survey, including survey logic and question wording problems, as well as the same question noted above. The compensation was subsequently adjusted from the pilot study ($1.50) to better reflect a comparable amount of time and effort for research participants. Thus, we believe we accomplished this given the above results from this question in the final survey.

Some of the demographic data collected during the survey are presented in Table 1.

Table 1. Demographics

	Number	**Percentage**
Gender		
Female	514	51.3%
Male	480	48.0%
Other	7	0.7%
Age		
18-34	525	52.4%
35+	476	47.6%
Ethnicity		

Asian / Pacific Islander	88	8.8%
Black / African-American	97	9.7%
White / Caucasian	692	69.1%
Hispanic / Latinx	77	7.7%
Native American / Alaskan Native	22	2.2%
Other / Multi-Racial	25	2.5%
Household Income		
Less than $50,000	438	43.8%
$50,000 - $99,999	417	41.7%
$100,000 - $199,999	127	12.7%
$200,000 - $299,999	17	1.7%
$300,000 or more	2	0.2%

In the next section, we provide some of the data from the survey. While other data was collected, our focus is on the use of five protective measures: anti-malware software, password managers, data backups, VPNs, and two-factor authentication.

4. ANALYSIS

Several different types of protective measures may be used by individuals to help mitigate a number of cybersecurity threats. We focus here on five protective measures and include a breakdown by age (18-34 and 35+), as well as gender (female, male, other).

Table 2 provides us with information on the use of anti-malware software. While most people do use anti-malware software for their laptops and desktops (82.4%), significantly fewer choose to use it on their tablets and smartphones (37.1%). Gender and age do not appear to make much of a difference with respect to the use of anti-malware software.

Table 2. Anti-Malware Usage

Tablet SmartPhone	**Totals**	**Female**	**Male**	**Other**	**18-34**	**35+**
Yes	37.1%	37.4%	36.8%	28.6%	34.9%	39.4%
No	51.6%	47.6%	55.6%	71.4%	55.2%	47.6%
Not Sure	9.2%	13.3%	4.8%	0.0%	7.9%	10.5%
Laptop Desktop						
Yes	82.4%	81.6%	83.4%	71.4%	79.0%	86.1%
No	12.5%	11.4%	13.7%	14.3%	16.2%	8.4%
Not Sure	4.1%	6.3%	1.9%	0.0%	4.1%	4.2%

The primary reason why individuals use anti-malware software is that they believe it is effective (32.5%), which is closely followed by it providing peace of mind (32.0%). Younger people (15.5%) seem to use it primarily because of how easy it is to use more so than older individuals (8.0%).

Table 3. Anti-Malware Primary Usage Reasons (N=837)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Inexpensive	5.3%	5.2%	5.2%	20.0%	6.4%	4.1%
Easy	11.8%	10.4%	13.5%	0.0%	15.5%	8.0%
Professional or Someone I Trust	7.5%	9.4%	5.7%	0.0%	8.2%	6.8%
Someone Did It For Me	7.8%	10.8%	4.7%	0.0%	8.9%	6.6%
Effective	32.5%	29.4%	36.1%	0.0%	30.4%	34.7%
I'm a Target	1.1%	0.9%	1.2%	0.0%	0.5%	1.7%
Peace of Mind	32.0%	31.8%	31.9%	60.0%	29.4%	34.7%

Risky Behavior	2.0%	2.1%	1.7%	20.0%	0.7%	3.4%

The cost of anti-malware software appears to be a significant impediment to its usage. This is a larger issue for females (43.4%) compared to males (28.6%). In contrast, males indicate that they believe it is not effective (26.4%), which is much higher than that of females (10.1%). Finally, twice as many females (20.9%) plan on implementing anti-malware software when compared to males (9.9%), but have not had the time yet.

Table 4. Anti-Malware Primary Non-Usage Reasons (N=222)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Expensive	37.4%	43.4%	28.6%	50.0%	39.7%	34.4%
Too Complicated	7.7%	7.0%	8.8%	0.0%	5.6%	10.4%
Don't Know How	4.1%	4.7%	3.3%	0.0%	4.8%	3.1%
Not Effective	16.7%	10.1%	26.4%	0.0%	20.6%	11.5%
Time Consuming	8.6%	7.0%	9.9%	50.0%	9.5%	7.3%
Interfere with Other Activities	9.5%	7.0%	13.2%	0.0%	7.9%	11.5%
Plan on Doing It	16.2%	20.9%	9.9%	0.0%	11.9%	21.9%

Password managers are not commonly used by individuals, whether on a smartphone or tablet (28.7%), or a laptop or desktop (33.3%).

Younger individuals use password managers at a higher rate than older individuals across various platform types.

Table 5. Password Manager Usage

Tablet SmartPhone	Totals	Female	Male	Other	18-34	35+
Yes	28.7%	27.5%	29.9%	28.6%	34.3%	22.5%
No	66.5%	66.8%	66.1%	71.4%	59.8%	73.9%
Not Sure	2.3%	3.3%	1.3%	0.0%	3.3%	1.3%
Laptop Desktop						
Yes	33.3%	32.0%	34.3%	57.1%	37.4%	28.8%
No	62.3%	62.5%	62.6%	28.6%	57.7%	67.4%
Not Sure	2.4%	3.3%	1.5%	0.0%	3.1%	1.7%

The primary reason why individuals use password managers is because they believe they are easy to use (34.7%), while others do so based on their belief that they are effective (21.7%). Females tend to value the peace of mind (22.0%) it brings them more than males (16.5%).

Table 6. Password Manager Primary Usage Reasons (N=369)

	Totals	Female	Male	Other	18-34	35+
Inexpensive	6.2%	6.2%	6.4%	0.0%	7.1%	4.9%
Easy	34.7%	35.6%	34.0%	25.0%	33.6%	36.4%
Professional or Someone I Trust	9.8%	7.3%	11.7%	25.0%	10.6%	8.4%
Someone Did It For Me	2.7%	3.4%	1.6%	25.0%	4.0%	0.7%
Effective	21.7%	20.3%	23.4%	0.0%	19.9%	24.5%

I’m a Target	3.0%	2.8%	3.2%	0.0%	2.2%	4.2%
Peace of Mind	19.2%	22.0%	16.5%	25.0%	20.4%	17.5%
Risky Behavior	2.7%	2.3%	3.2%	0.0%	2.2%	3.5%

The reasons why individuals do not use a password manager vary significantly across the answer choices they were provided with. Many thought that a password manager was not effective (19.5%) or too time consuming (18.4%), while others simple do not know how (14.9%) or believe it is too complicated (11.2%). Females indicated in far greater numbers (22.7%) than males (6.2%) that not knowing how was the primary reason they are not using a password manager.

A plurality of individuals (20.0%) plan on using a password manager someday, but have not had the time yet to do so. This is not too surprising given the effort required to initially begin using a password manager, which may involve setting up multiple accounts on the software and understanding how to use it.

Table 7. Password Manager Primary Non-Usage Reasons (N=625)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Expensive	6.7%	6.3%	7.2%	0.0%	7.4%	6.1%
Too Complicated	11.2%	11.8%	10.7%	0.0%	11.1%	11.2%
Don’t Know How	14.9%	22.7%	6.2%	0.0%	11.5%	17.9%
Not Effective	19.5%	14.8%	24.1%	100.0%	23.3%	16.1%
Time Consuming	18.4%	16.6%	20.6%	0.0%	18.2%	18.5%

Interfere with Other Activities	9.3%	7.3%	11.7%	0.0%	10.1%	8.5%
Plan on Doing It	20.0%	20.5%	19.6%	0.0%	18.2%	21.6%

Almost half of all individuals surveyed backup their data across all platform types. Younger individuals are more likely to do so than older individuals. While this may represent many individuals that do backup their data, it also points to a significant number of individuals that are not. Given the prevalence of threats that may cause someone to lose their information, such as ransomware (Al-rimy et al., 2018), this is disconcerting.

Table 8. Data Backup Usage

Tablet SmartPhone	**Totals**	**Female**	**Male**	**Other**	**18-34**	**35+**
Yes	46.6%	48.5%	44.6%	42.9%	52.2%	40.4%
No	46.1%	41.9%	50.4%	57.1%	40.7%	52.0%
Not Sure	5.5%	8.4%	2.5%	0.0%	5.0%	6.1%
Laptop Desktop						
Yes	45.4%	45.1%	45.7%	42.9%	49.5%	40.8%
No	48.1%	45.9%	50.7%	28.6%	43.6%	53.1%
Not Sure	4.8%	7.6%	1.7%	14.3%	5.0%	4.6%

The value of data that may be lost can be significant. Thus, it may not be too surprising that many individuals choose to backup their data for peace of mind (36.6%). Many individuals also find it easy (20.3%) and effective (17.9%). Younger individuals are more likely to find it easy

(24.8%) compared to older individuals (14.2%), while older individuals (42.1% vs. 32.6%) are more likely to backup their data for peace of mind.

Table 9. Data Backup Primary Usage Reasons (N=552)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Inexpensive	7.8%	8.4%	7.2%	0.0%	8.2%	7.3%
Easy	20.3%	18.9%	21.7%	25.0%	24.8%	14.2%
Professional or Someone I Trust	8.9%	10.5%	7.2%	0.0%	10.0%	7.3%
Someone Did It For Me	5.3%	7.0%	3.4%	0.0%	4.7%	6.0%
Effective	17.9%	18.2%	17.9%	0.0%	17.2%	18.9%
I'm a Target	2.5%	2.1%	3.0%	0.0%	2.2%	3.0%
Peace of Mind	36.6%	34.0%	38.8%	75.0%	32.6%	42.1%
Risky Behavior	0.7%	0.7%	0.8%	0.0%	0.3%	1.3%

The amount of effort involved in having backups is too much for many (30.2%). While many plan on implementing a backup solution (26.6%), some believe it is too expensive to do so (15.4%).

Table 10. Data Backup Primary Non-Usage Reasons

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Expensive	15.4%	14.7%	16.1%	25.0%	17.6%	13.5%
Too Complicated or Time Consuming	30.2%	27.6%	32.6%	50.0%	33.3%	27.4%

Don't Know How	12.3%	18.2%	6.4%	0.0%	10.5%	13.9%
Not Effective	9.8%	8.4%	11.0%	25.0%	13.3%	6.8%
Interfere with Other Activities	5.6%	3.6%	7.8%	0.0%	6.7%	4.6%
Plan on Doing It	26.6%	27.6%	26.1%	0.0%	18.6%	33.8%

The prevalence of VPN usage is quite low (18.9%, 27.4%) compared to other protective measures investigated here. Younger individuals are more likely to use a VPN on their various devices, while males (32.5%) are more likely than females (22.4%) to use a VPN on their laptop or desktop.

Table 11. VPN Usage

Tablet SmartPhone	**Totals**	**Female**	**Male**	**Other**	**18-34**	**35+**
Yes	18.9%	18.3%	19.4%	28.6%	22.7%	14.7%
No	72.6%	69.8%	75.6%	71.4%	69.1%	76.5%
Not Sure	6.4%	10.7%	1.9%	0.0%	5.7%	7.1%
Laptop Desktop						
Yes	27.4%	22.4%	32.5%	42.9%	31.0%	23.4%
No	65.4%	67.1%	63.9%	42.9%	62.6%	68.4%
Not Sure	5.5%	8.8%	2.1%	0.0%	4.8%	6.3%

Those that use a VPN generally do so because they believe it is effective (29.3%) or for peace of mind (23.5%). Males are more likely than females to use a VPN because of its effectiveness (34.5% vs. 21.5%). Older individuals are more likely to do so for peace of mind (33.1%) than younger individuals (16.9%).

Table 12. VPN Primary Usage Reasons (N=307)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Inexpensive	4.9%	4.6%	5.2%	0.0%	4.9%	4.8%
Easy	15.3%	16.2%	14.9%	0.0%	10.7%	4.6%
Professional or Someone I Trust	12.1%	15.4%	9.8%	0.0%	15.8%	6.5%
Someone Did It For Me	8.1%	12.3%	5.2%	0.0%	7.7%	8.9%
Effective	29.3%	21.5%	34.5%	66.7%	31.1%	26.6%
I'm a Target	2.3%	3.1%	1.7%	0.0%	1.6%	3.2%
Peace of Mind	23.5%	24.6%	22.4%	33.3%	16.9%	33.1%
Risky Behavior	4.6%	2.3%	6.3%	0.0%	3.8%	5.6%

While many individuals choose to use a VPN, a significant majority of them do not. The greater level of complexity inherent in setting up and using a VPN appears to be a significant contributing factor for its non-use (25.4%), especially for females (36.8%) when compared to males (11.4%). Other reasons noted by a large number of participants include VPNs being too expensive (16.0%), too complicated or time consuming (18.2%), and their propensity to interfere with other activities (19.3%).

Table 13. VPN Primary Non-Usage Reasons (N=705)

	Totals	Female	Male	Other	18-34	35+
Expensive	16.0%	11.9%	21.0%	25.0%	18.9%	13.1%
Too Complicated or Time Consuming	18.2%	14.5%	22.5%	25.0%	18.9%	17.4%
Don't Know How	25.4%	36.8%	11.4%	25.0%	23.2%	27.6%
Not Effective	7.5%	5.7%	9.8%	0.0%	9.3%	5.7%
Interfere with Other Activities	19.3%	18.9%	19.7%	25.0%	16.4%	22.2%
Plan on Doing It	13.6%	12.2%	15.6%	0.0%	13.3%	14.0%

Finally, we turn our attention to two-factor authentication. Most individuals do use two-factor authentication for one or more accounts (79.3%). This is roughly the same for males and females, as well as younger and older individuals.

Table 6. Two-Factor Authentication Usage

	Totals	Female	Male	Other	18-34	35+
Yes	79.3%	79.0%	79.6%	85.7%	80.8%	77.7%
No	20.7%	21.0%	20.4%	14.3%	19.2%	22.3%

Many individuals use two-factor authentication because they believe it is effective (31.0%) with males and younger individuals more likely to select this as their primary reason for doing so. Older individuals are more likely than younger individuals to use two-factor authentication for peace of mind (29.1% vs. 21.3%) and as part of a system requiring it (18.5% vs. 11.1%).

Of note, for this question we also provided participants with an option to indicate they use two-factor authentication primarily because a system requires them to do so. Thus, they are using a protective measure for which they have no choice. Many (14.5%) indicated that this were the primary reason for doing so. A large percentage of individuals also indicated that they use two-factor authentication for peace of mind (24.9%) and because it is easy to do so (16.1%).

Table 12. Two-Factor Authentication Primary Usage Reasons (N=791)

	Totals	**Female**	**Male**	**Other**	**18-34**	**35+**
Inexpensive	2.7%	3.0%	2.4%	0.0%	3.3%	1.9%
Easy	16.1%	16.1%	16.0%	16.%	19.4%	12.2%
Professional or Someone I Trust	5.4%	7.4%	3.4%	0.0%	5.2%	5.7%
Someone Did It For Me	3.7%	5.0%	2.4%	0.0%	3.5%	3.8%
Effective	31.0%	28.0%	34.1%	33.3%	34.0%	27.4%
I'm a Target	1.0%	1.0%	1.0%	0.0%	1.2%	0.8%
Peace of Mind	24.9%	23.3%	26.8%	16.7%	21.3%	29.1%
Risky Behavior	0.8%	0.2%	1.3%	0.0%	0.9%	0.5%
System Requirement	14.5%	16.1%	12.6%	33.3%	11.1%	18.5%

Finally, we take a look at the primary reasons why people do not use two-factor authentication. A plurality of individuals believe it is too complicated or time consuming to use it (42.0%), while many plan on using it in the future (17.9%) once they have time to do so. Females (18.5%) are more likely than males (8.2%) to not use two-factor authentication because they do not know how.

Table 13. Two-Factor Authentication Primary Non-Usage Reasons (N=207)

	Totals	Female	Male	Other	18-34	35+
Expensive	6.8%	4.6%	9.2%	0.0%	9.9%	3.8%
Too Complicated or Time Consuming	42.0%	44.4%	39.8%	0.0%	38.6%	45.3%
Don't Know How	13.5%	18.5%	8.2%	0.0%	13.9%	13.2%
Not Effective	7.2%	2.8%	12.2%	0.0%	10.9%	3.8%
Interfere with Other Activities	12.6%	9.3%	15.3%	100.0%	11.9%	13.2%
Plan on Doing It	17.9%	20.4%	15.3%	0.0%	14.9%	20.8%

Next, we will provide some thoughts on the data analyzed in this section, as well as what this means going forward.

5. DISCUSSION

The preceding results provide a good starting point for further exploration. Several areas of concern are identified with some interesting differences related to gender or age in a few instances. The reasons why individuals either choose to use a specific protective measure or not use it varies based on the protective measure being examined. A VPN may be too complicated for some to use, while backing up data brings peace of mind to many individuals given the importance of the information we have on our computing devices, such as priceless photos of precious memories.

There are a few limitations worth noting. First, common method bias is a concern when a single method is used (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Since data was collected using a survey exclusively, we cannot rule out common method bias impacting the results. However, the risk related to common method bias is minimized in the current context since participants were anonymous to the researchers and asked to simply respond honestly.

Second, social desirability bias is another limitation of this study (DeVellis, 2012). Participants may seek to provide answers consistent with what they believe the researchers would like and/or are deemed socially acceptable. As before, the level of anonymity provided by the procedures employed herein minimize the likelihood of social desirability bias being a major concern.

Finally, participants likely do not represent the populace as a whole. While they do provide a high level of diversity with respect to various demographic indicators, they also generally represent a younger and more educated group of people (Dupuis et al., 2013).

With the above in mind, we believe there are some opportunities for increased and improved use of SETA programs in the cybersecurity space as it relates to individual users (D'Arcy, Hovav, & Galletta, 2009; Posey, Roberts, & Lowry, 2015). Some protective measures require very little technical expertise, while others are more sophisticated and less commonly used, but nonetheless provide a significant level of protection, such as a VPN. Thus, a combination of security tools and improved behavior through security education, training, and awareness (SETA) are needed to effectively mitigate cybersecurity and privacy threats (Dupuis & Crossler, 2019; Dupuis, Khadeer, & Huang, 2017).

For the protective measures requiring a greater level of technical expertise, hands-on training will likely prove particularly effective. For example, hands-on activities will allow individuals to practice the skills needed to effectively implement the protective measure (Beuran et al., 2018). In other instances, game-based activities can help individuals overcome possible psychological hurdles that make employing a technical measure difficult (Jin, Tu, Kim, Heffron, & White, 2018).

This research provides a useful starting point in the identification of where people need the most help and why certain protective measures are not being used. Future research will include the deployment of some of these innovative SETA programs to target the groups and protective measures most in need of improved levels of usage.

REFERENCES

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166.

Anderson, B. B., Kirwan, C. B., Eargle, D., Jensen, S. R., & Vance, A. (2015). Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study. *Journal of Cybersecurity*, *1*(1), 109–120.

Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security*, *78*, 43–59.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

DeVellis, R. F. (2012). *Scale development: Theory and applications* (3rd ed). Thousand Oaks, Calif: SAGE.

Dupuis, M., & Crossler, R. (2019). The Compromise of One's Personal Information: Trait Affect as an Antecedent in Explaining the Behavior of Individuals. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 4841–4850. https://doi.org/10.24251/HICSS.2019.584

Dupuis, M., Crossler, R., & Endicott-Popovsky, B. (2016). Measuring the Human Factor in Information Security and Privacy. *The 49th Hawaii International Conference on System Sciences (HICSS)*. Presented at the Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii.

Dupuis, M., Endicott-Popovsky, B., & Crossler, R. (2013). An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. *International Conference on Cloud Security Management*. Presented at the International Conference on Cloud Security Management, Seattle, Washington.

Dupuis, M., Khadeer, S., & Huang, J. (2017). "I Got the Job!": An exploratory study examining the psychological factors related to status updates on facebook. *Computers in Human Behavior*, *73*, 132–140.

Dupuis, M., & Khan, F. (2018). Effects of peer feedback on password strength. *2018 APWG Symposium on Electronic Crime Research (ECrime)*, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68–73. ACM.

Lévesque, F. L., Fernandez, J. M., & Batchelder, D. (2017). Age and gender as independent risk factors for malware victimisation. *Proceedings of the 31st British Computer Society Human Computer Interaction Conference*, 46. BCS Learning & Development Ltd.

Pavlicek, A., & Sudzina, F. (2018). Internet Security and Privacy in VPN. *International Conference on Digital Information ManagementInternational Conference on Digital Information Management*, *9*, 133–139.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Sears, D. O. (1986). College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology*, *51*(3), 515.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly*, *38*(2), 355–378.