Journal of
Information
Systems
Education

Volume 36
Issue 2
Spring 2025

Teaching Tip

Cyber Hygiene Training: Using a Salesforce Developer Module to Improve Student Online Behaviors

David Kocsis, Morgan Shepherd, and Daniel L. Segal

Recommended Citation: Kocsis, D., Shepherd, M., & Segal, D. L. (2025). Teaching Tip: Cyber Hygiene Training: Using a Salesforce Developer Module to Improve Student Online Behaviors. *Journal of Information Systems Education*, 36(2), 90-110. https://doi.org/10.62273/CUEU6233

Article Link: https://jise.org/Volume36/n2/JISE2025v36n2pp90-110.html

Received: August 13, 2024
First Decision: December 6, 2024
Accepted: February 28, 2025
Published: June 15, 2025

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 36(2), 90-110, Spring 2025
https://doi.org/10.62273/CUEU6233

Teaching Tip
Cyber Hygiene Training: Using a Salesforce Developer Module to Improve Student Online Behaviors

David Kocsis
Morgan Shepherd
College of Business
University of Colorado at Colorado Springs
Colorado Springs, CO 80918, USA
dkocsis@uccs.edu, mshepher@uccs.edu

Daniel L. Segal
Psychology Department
University of Colorado at Colorado Springs
Colorado Springs, CO 80918, USA
dsegal@uccs.edu

ABSTRACT

This paper describes the development of a training module to improve students' individual online behaviors. We developed this module to integrate cyber hygiene concepts into a hands-on learning activity where students develop and secure a mobile web application using the Salesforce Developer tool. This new module aims to prepare the next generation of workers by improving cyber hygiene behaviors through an engaging hands-on activity. We hired two students to help create the dialogue and structure of the module in the summer of 2022. Instructors then implemented the module in introductory information systems courses during the 2022-2023 academic year. During the module, each student a) took a survey to establish a baseline of current knowledge and behaviors (pre-survey), b) performed the training module, and c) completed a survey so we could assess knowledge improvement (post-survey). Post-survey results showed that students were satisfied with the assignment, and that the module taught them essential knowledge and tools for improving cyber hygiene behaviors. Three months later, we sent each student a follow-up survey so we could determine behavioral changes. This follow-up survey showed that students improved self-reported behavioral changes, specifically about using multi-factor authentication, identifying phishing messages, assessing social media settings, identifying antivirus and firewall software, backing up data, and updating software. This study demonstrates that students may benefit from this module to improve online behaviors while preparing them to enter the workforce and help organizations, regardless of their work focus.

Keywords: Cybersecurity, Introductory course, Cyber hygiene, Security education, Computer literacy, Teaching tip

1. INTRODUCTION

Companies are routinely under attack through viruses, password hacks, and phishing attempts from outside and inside threats (Cain et al., 2018). Unfortunately, most organizational training to strengthen employees' knowledge and safety behaviors has been ineffective. Helpful behaviors, known as cyber hygiene, are conceptually defined as "the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack" (Vishwanath et al., 2020, p. 2). Providing current students with a security education, training, and awareness (SETA) module will better prepare them to enter the workforce and help organizations, regardless of their major.

Researchers have advocated for security training to be theory-based (Puhakainen & Siponen, 2010). Using a game-like approach to SETA improves the effectiveness of the training and the participants are much happier with the process compared to a more traditional pedagogical approach (Baxter et al., 2016). While our approach is not a game, we aimed to make the module fun and engaging (i.e., game-like).

The present research and education program aimed to answer the question: *How can we prepare the next generation of students and employees to understand the importance of effective and appropriate cyber hygiene?*

To answer this question, we developed a training module based on cyber hygiene research to improve the cyber hygiene of the next generation of workers and leaders. Hill and Nance (2016) have developed six labs to integrate Information

Systems (IS) concepts into a series of hands-on activities. Using these labs, students gained valuable skills and reinforced course concepts through an innovative activity (Sclarow et al., 2024). However, one important activity, cybersecurity, is missing from the labs.

We created this module focused on cybersecurity using the Salesforce Developer tool. We chose this tool for three reasons. First, the platform is free to use. Second, the students learn about Salesforce and other Customer Relationship Management products in the course, giving them hands-on experience they can add to their resumes. Third, because Hill and Nance's labs were also developed in Salesforce.

2. MODULE DESCRIPTION

2.1 Development of the Salesforce Module

We gathered the necessary requirements for the module from previous research on cyber hygiene. Then we hired two students who were familiar with Salesforce Developer and cyber hygiene concepts to help us write a step-by-step module that integrated cyber hygiene concepts while guiding students through the activity. Consistent with Hill and Nance's Salesforce labs, the module was "written" by a fictional college student in an informal blog post.

We also created surveys to measure the module's effectiveness. At the beginning of the module, students completed a pre-survey to establish a baseline for their current cyber hygiene knowledge and behaviors. After completing the module, they filled out the post-survey, furnishing data about their satisfaction with it and measuring their knowledge improvement. Three months later, we sent a follow-up survey to measure whether their knowledge and behaviors improved or regressed over time. This follow-up survey aimed to measure actual behavior changes rather than behavioral intention.

2.2 Module Components

The module begins with an overview of the Salesforce Developer platform and how to create an account. The platform has a drag-and-drop interface and does not require coding, so students do not need technical skills to complete it. The students then begin the journey of developing a Customer Relationship Management (CRM) system for a fictional company while learning important cyber hygiene concepts. The learning objectives include the following: understanding what cyber hygiene means, the importance of password strength and length, the importance of using a password manager, identifying and protecting against phishing scams, backing up data, how to manage antivirus and firewall settings, managing and improving personal computer security, and managing social media privacy settings. We integrated these key components as they stem from previous cyber hygiene research (see Cain et al., 2018; Kalhoro et al., 2021; Neigel et al., 2020; Parsons et al., 2017; Such et al., 2019; Vishwanath et al., 2020).

In the introductory portion of the module, students learn about malware, types of viruses, phishing, and ransomware and how to protect themselves from these attacks. The remainder of the module explores these concepts in-depth. First, students assume the role of a systems administrator and then create password policies for new user accounts. With these policies, students learn how to enable multi-factor authentication for accounts they create in the Salesforce platform. This helps the students understand the importance of using a password manager.

Next, they set up a new user in the system who will receive these password policies. The user they create will be a fictional victim whom the student will later attack. They then create a phishing message within the Salesforce administrator interface and send the phishing email to their new victim user. By logging into the email account of their victim user, they see the phishing message, which helps them understand how to identify phishing messages and how easy it is for attackers to perform massive phishing attacks.

The students then learn about ransomware and how they can protect themselves from ransomware attacks (e.g., backing up files to external drives or the cloud). They also learn to identify their built-in antivirus software (e.g., X-protect on Mac; Defender on Windows) and firewalls. The module encourages students to use third-party software for antivirus and firewalls to add an extra layer of protection. The module also walks students through how to find out whether automatic updates are enabled for their applications and operating systems.

Next, students learn about protecting their web browsing behavior. The module walks students through turning on a pop-up blocker, clearing cookies, identifying an SSL (Secure Sockets Layer) connection on the browser, and enabling incognito or private browsing. Students also learn that using a stronger web browser, such as Brave or Vivaldi, includes all these secure settings without needing to be manually configured. Once students learn that ads no longer appear at the beginning of YouTube videos, they are often eager to adopt these behaviors.

Next, the module discusses how encryption helps protect the user. It encourages students to use a Virtual Private Network (VPN) when using public Wi-Fi and suggests vendors such as Surfshark or Proton. Finally, it encourages students to improve their privacy settings on social media, such as turning on multi-factor authentication (MFA) and removing from social media connections people they do not know and trust personally. See Appendix B for the complete module.

2.3 Module Deployment

The authors deployed the module at the University of Colorado at Colorado Springs in undergraduate classes of varying levels in the College of Business. The first level was the equivalent of an *Introduction to Information Systems* course, which mainly consisted of third-year students. The second level to adopt the module was an introductory course for first year and transfer students, focusing on business applications such as Excel, PowerPoint, Access, and Outlook. Instructors could assign the module for points in the course at their discretion, either as a regular assignment or as extra credit. Instructors deployed the module in six sections of these courses in the 2022-2023 academic year.

Students took another brief survey that captured their satisfaction with the module and indicated whether their knowledge improved because of the module. After the survey, students received a code to submit to attain credit for the assignment. The module also reminded them they would receive a follow-up survey three months later. If they completed that survey, we entered them into a drawing for a $25 Amazon gift card. All measures from the surveys are provided in Appendix A.

3. RESULTS

This section presents the results of the three surveys.

3.1 Pre-survey

Initially, 160 students completed the module, although sixteen students did not complete the pre-survey completely, giving us 144 valid responses. The pre-survey allowed us to establish a baseline for individual cyber hygiene knowledge and behaviors and to capture demographics. The mean age of participants was 21.89 years (SD = 4.26; range = 18 to 45 years), with a mode of 19 years (20.8%). 89 students identified as a man (61.8%), 50 as a woman (34.7%), three preferred not to say (2.1%), and two as non-binary or third gender (1.4%). The race and ethnicity distribution included 93 white or Caucasian (64.6%), 19 Hispanic or Latinx (13.2%), 12 Asian or Pacific Islander (8.3%), eight multiracial or biracial (5.6%), five who preferred not to say (3.5%), three black or African American (2.1%), two Native American or Alaska Native (1.4%), and two identified as a race/ethnicity not listed (1.4%).

We also asked students which operating system they use, and results showed that 79 used Windows (54.9%), 59 used MacOS (41.0%), four chose another/more than one operating system (2.8%), and 2 did not know (1.4%). The highest level of education achieved included 93 with some college but no degree (64.6%), 36 with an associate degree (25.0%), 11 with a high school diploma, GED, or less (7.6%), three preferred not to say (2.1%), and one other (0.7%).

Lastly, we asked students about their current cyber hygiene knowledge and behaviors. Knowledge responses ranged from strongly disagree to strongly agree, while the behavior responses ranged on a scale from never to always. For both question types, we also included an option of "do not know/understand." Unfortunately, most cyber hygiene scales focus on general or workforce samples (Cain et al., 2018; Parsons et al., 2017; Vishwanath et al., 2020). Therefore, we adopted multiple cyber hygiene measures to fit the context of a student sample. We assess these results together with the follow-up survey results later in this section.

3.2 Post-Survey

The post-survey asked students to evaluate their learning, their satisfaction with the hands-on nature of the module versus traditional learning methods, and how well their understanding of cyber hygiene improved because of the module. Using a five-point Likert-type scale, we adapted the training effectiveness scales from Tan et al. (2003), with each question ranging from strongly disagree to strongly agree. The questions fall into categories of a general evaluation (six questions, Cronbach's alpha reliability = 0.89), the hands-on knowledge and tools for improving their cybersecurity behaviors (three questions, alpha = 0.94), the level of understanding gained (three questions, alpha = 0.76), and the level of improvement in cyber hygiene knowledge (four questions, alpha = 0.84). The questions, categories, Cronbach's alpha (reliability), means, and standard deviations are shown in Table A1 in Appendix A.

3.3 Follow-Up Survey (3 Months After Post-Survey)

The follow-up survey was used to measure the long-term impact of the cyber hygiene module. It contained the same questions as the pre-survey except for demographics. To incentivize the completion of the optional follow-up survey, we entered students into a drawing to receive a $25 Amazon gift card—ten students received a gift card for their participation. Although only 39 of 144 students (27%) completed the follow-up survey, we could still capture results using a paired samples t-test measuring improvements between the pre-survey and follow-up survey.

We observed the following statistically significant self-reported behavioral improvements after three months and present them in Table 1 below:

Behavioral Improvement	*p*-Value
password_knowledge_3	.019
password_behavior_5	.014
email_use_behavior_2	.044
social_media_use_knowledge_1	.018
social_media_use_behavior_2	.048
social_media_use_behavior_3	.038
device_protection_behavior_2	.024
device_protection_behavior_3	.014
update_behavior_1	.037
update_behavior_2	.016

Table 1. Statistically Significant Improvements

We did not identify any significant differences in the opposite direction, although password_knowledge_2 (p = .058) was close, and a few other items did have opposite effects.

The complete results are shown in Table 2, which contains the expected direction of the survey questions (whether the improvement is expected to decrease or increase between the pre-survey and follow-up survey), means, standard deviations, significance, and whether the result was in the expected direction or the opposite direction. Note that the comparisons between the pre-survey and follow-up survey only assessed differences for those who participated in the follow-up survey, so the t-test only included a sample size of 39. In the follow-up columns, the mean and standard deviation are included for both the pre-survey (top of each cell) and the follow-up survey (bottom of each cell). We will discuss these results in-depth in the next section.

	Pre-Survey: N = 144		Follow-Up: N = 39				
	Mean	SD	Mean Pre and Mean Follow-Up	SD Pre and SD Follow-Up	Expected Improvement Direction	*p*-Value	Result
Password Knowledge_1	1.16	0.58	1.13 1.28	0.52 0.89	Decrease	0.160	Opposite
Password Knowledge_2	1.20	0.64	1.13 1.38	0.73 0.99	Decrease	0.058	Opposite
Password Knowledge_3	4.53	0.76	4.46 4.67	0.64 0.62	Increase	0.019*	Expected
Password Knowledge_4	2.28	1.18	1.87 1.90	1.11 1.19	Decrease	0.850	Opposite
Password Behavior_1	4.01	1.19	4.15 4.28	1.16 1.07	Increase	0.168	Expected
Password Behavior_2	1.20	0.45	1.26 1.31	0.50 0.57	Decrease	0.324	Opposite
Password Behavior_3	3.92	1.15	4.18 4.26	1.10 0.94	Increase	0.520	Expected
Password Behavior_4	2.44	1.26	2.28 2.15	1.23 1.14	Decrease	0.257	Expected
Password Behavior_5	3.51	1.31	3.64 3.92	1.11 1.06	Increase	0.014*	Expected
Password Behavior_6	2.13	1.48	2.54 2.46	1.55 1.64	Increase	0.637	Opposite
Email Use Knowledge_1	3.49	1.27	3.44 3.15	1.12 1.25	Increase	0.110	Opposite
Email Use Knowledge_2	1.22	0.55	1.28 1.18	0.79 0.79	Decrease	0.160	Expected
Email Use Knowledge_3	1.26	0.65	1.21 1.15	0.47 0.59	Decrease	0.487	Expected
Email Use Behavior_1	2.44	1.15	2.21 2.05	0.98 0.92	Increase	0.262	Opposite
Email Use Behavior_2	1.21	0.58	1.18 1.08	0.45 0.35	Decrease	0.044*	Expected
Email Use Behavior_3	3.80	1.55	3.95 3.85	1.34 1.39	Increase	0.618	Expected
Email Use Behavior_4	3.42	1.37	3.82 3.87	1.23 1.24	Increase	0.487	Expected
Email Use Behavior_5	3.53	1.49	3.97 4.05	1.33 1.05	Increase	0.555	Expected
Internet Use Knowledge_1	4.31	1.19	4.31 4.49	1.26 1.00	Increase	0.228	Expected
Internet Use Knowledge_2	3.90	1.50	3.92 4.21	1.44 1.15	Increase	0.117	Expected
Internet Use Behavior_1	1.60	0.90	1.67 1.59	0.98 0.97	Decrease	0.412	Expected
Internet Use Behavior_2	3.01	1.51	3.72 3.74	1.34 1.23	Increase	0.886	Expected
SM use Knowledge_1	4.07	1.00	4.44 4.67	0.75 0.53	Increase	0.018*	Expected
SM use Knowledge_2	1.26	0.62	1.59 1.64	1.02 1.18	Decrease	0.689	Opposite
SM use Behavior_1	2.73	1.31	3.31 3.23	1.30 1.27	Increase	0.520	Expected
SM use Behavior_2	4.00	1.22	4.26 4.49	1.02 0.76	Increase	0.048*	Expected
SM use Behavior_3	3.85	1.34	3.92 4.23	1.11 0.87	Increase	0.038*	Expected

SM use Behavior_4	3.34	1.42	3.26 3.51	1.52 1.43	Increase	0.151	Expected
Mobile device behavior_1	1.49	0.80	1.49 1.49	0.79 0.88	Decrease	1.000	Same
Mobile device behavior_2	1.53	0.77	1.56 1.62	0.88 0.96	Decrease	0.534	Opposite
Mobile device behavior_3	2.02	1.32	2.62 2.74	1.53 1.45	Increase	0.536	Expected
Device prot behavior_1	2.28	2.03	3.08 3.67	2.18 1.84	Increase	0.075	Expected
Device prot behavior_2	3.06	1.76	3.03 3.56	1.68 1.39	Increase	0.024*	Expected
Device prot behavior_3	2.83	1.48	3.03 3.38	1.53 1.37	Increase	0.014*	Expected
Device prot behavior_4	3.08	1.51	3.51 3.72	1.41 1.34	Increase	0.198	Expected
Device prot behavior_5	2.01	1.56	2.44 2.72	1.62 1.73	Increase	0.162	Expected
Device prot behavior_6	2.38	1.29	2.64 2.72	1.42 1.50	Increase	0.539	Expected
Backup behaviors_1	3.27	1.41	3.85 4.05	1.25 1.10	Increase	0.088	Expected
Backup behaviors_2	2.13	1.32	2.38 2.33	1.31 1.30	Increase	0.675	Opposite
Update behaviors_1	3.85	1.17	4.26 4.49	0.97 0.76	Increase	0.037*	Expected
Update behaviors_2	3.16	1.50	3.51 4.00	1.36 1.19	Increase	0.016*	Expected

*Note: * = p < 0.05*

Table 2. Question Codes, Means, Standard Deviations, and Results for Pre-Survey and Follow-Up Survey

4. DISCUSSION

The results of our newly deployed Salesforce module showed an overall improvement in cyber hygiene, indicating the effectiveness of the module for this group of students. The post-survey showed that students were highly satisfied with the module, and they would recommend other students participate in the module. The students felt they received knowledge and tools to help them in the future and that they learned how to protect themselves from online threats. They also appreciated this method of learning and sensed they became knowledgeable about the landscape of cybersecurity because of the module. Thus, the game-like module was successful in engaging students in this hands-on learning activity.

The follow-up survey revealed that, after three months, students were surprisingly more likely to think it is acceptable to share passwords with colleagues, classmates, and friends, indicating their knowledge of password sharing decreased. While this finding was disappointing, we were encouraged that their behavior improved regarding sharing their passwords, albeit at a non-significant level. One reason why this could have happened is that the lab focused on other password issues, such as password strength and MFA, but insufficiently on password behavior. This misalignment is interesting and could warrant further research.

Students demonstrated improved knowledge concerning using stronger and longer passwords although this behavior improvement was non-significant. One significant password behavior showed that students improved at enabling MFA for logins, meaning students may be more willing to accept MFA requirements in school and when they are in the workforce.

We did not see any significant changes regarding email use knowledge. However, one behavior improved regarding clicking links from unknown email senders. This indicates that the module helped students become more aware of the prevalence and impact of phishing tactics. We did not observe any significant changes in internet use knowledge or behavior, nor with mobile device behavior, which was disappointing but not surprising. This may indicate their current knowledge and behavior were already strong.

One major improvement that we aimed for was in social media usage, and we were pleased to learn that students improved in knowledge of the importance of periodically reviewing privacy settings on social media accounts. Unfortunately, their behavior did not match this improvement. Two social media behaviors did improve; as they now consider possible negative consequences of posting on social media, and they further assess the authenticity of social media friends and information requests. This implies that students are more cognizant of how they may be perceived on social media, particularly by employers or other authority figures. They also will be less likely to be connected to malicious actors or bots posing as legitimate connections.

Next, we saw improvements in device protection and backup behaviors. Regarding their devices, they improved by knowing they have a firewall running on their computer, they block web browser ads more often, and they now either block or regularly clear cookies on their web browser. By taking these actions, their devices will be less vulnerable to attacks and can improve their online anonymity and privacy (Cain et al., 2018). Moreover, their understanding of the importance of maintaining cloud backups improved. This will help students to keep their files long-term, even when they switch to new devices, while also protecting themselves from ransomware attacks (Vishwanath et al., 2020). Moreover, other researchers have published studies since the implementation of our training module, so future research may refer to them for measures related to cyber hygiene knowledge, awareness, and behaviors (Baraković & Baraković Husić, 2023).

Last, one of the easiest ways for attackers to gain access to systems is when their victims do not update their software. We saw significant improvement with students updating their devices to ensure they have the latest operating system updates, software updates, patches, and antivirus software. This will decrease the chances of students getting viruses and their devices being a target for denial-of-service attackers trying to build a zombie farm (Cain et al., 2018; Vishwanath et al., 2020).

While impactful, we recognize several limitations of the study: the module was only implemented for undergraduate college of business students, the survey method in general, and the small sample size for the follow-up survey. For example, the module was written in a way that engaged undergraduate-aged students, but it is unclear whether and to what extent this training may be appropriate for workplace education, training, and awareness programs.

Also, the College of Business has courses that are focused on technology or innovation, but students from other colleges, especially those from colleges with less focus on technology, may benefit more from the training. In addition, the module does not account for other courses or training students are receiving. Thus, in the three-month period between the module and the follow-up survey, students may have been exposed to other improvement factors unrelated to this module. Future research will investigate the effects of modes of delivery, such as performing the module for points (i.e., an assignment), where students may be more engaged versus extra credit, where students may not pay attention. These differences may show that the mode of delivery has an impact on module effectiveness.

Last, we saw limited improvement in items in the follow-up survey, such as password sharing. This could indicate the module may have limitations in effectively addressing all aspects of password security. While more depth could enhance password understanding, it could also lengthen the module. As such, we encourage instructors to go beyond the module for password depth. Because the surveys are self-report only, it may be useful to measure behaviors using a tracking or inventory tool on participant computers. For example, Esparza et al. (2020) introduced a knowledge-attitude-behavior self-assessment framework, which could be useful for accounting for human factors when designing cyber hygiene questionnaires. Some of these limitations could be resolved by future research with larger and more diverse samples and longer-term follow-up data collection.

5. CONCLUSIONS AND FUTURE DIRECTIONS

The purpose of this project was to improve current cyber hygiene knowledge, awareness, and behaviors through an engaging, game-like, hands-on learning activity developed and evaluated for student learners. The module we developed appears to be an effective way to engage students while improving their behaviors, as seen in the high self-reported satisfaction and improvement questions in the post-survey (see Table A1 in Appendix A). While not all student knowledge and behaviors improved, we observed improvements in several important behaviors such as using MFA, recognizing and protecting against phishing messages, assessing their social media settings, identifying protective software (e.g., antivirus and firewall) on their devices, backing up their data, and updating their software. This will allow students to be safer while using online systems and be better prepared to enter the workforce as employees who understand and value the importance of protecting an organization's systems.

This module targets undergraduate students, and as such, the language and context are currently too informal to target graduate students or professional employees. We are in the process of adapting the language for a more professional audience and hope to provide certified micro-credentials for those who complete it.

Finally, if anyone is interested in using the cyber hygiene module in a course, the entire module is included in Appendix B. Survey components have been removed from the module, so only the cyber hygiene components remain, which take approximately one hour to complete. As one hour may not be significant enough to improve knowledge, attitudes, and behaviors, we also included possible discussion questions and how to deploy this in your learning management system in Appendix C. The module works well prior to cybersecurity and privacy units in information systems courses but can be applicable to introductory cybersecurity courses as well.

6. ACKNOWLEDGMENTS AND FUNDING

We would like to thank Audrey Bloomquist and Arianna Russell, two UCCS College of Business students we hired to help develop the dialogue and content for this training module.

This project was funded by the UCCS Cybersecurity Programs Office and the Office of Research through a Cybersecurity Seed Grant. The grant covered the costs of the student workers, a stipend for one author, travel funds for another author to present this work at a conference, and gift cards for participants.

Next, this module was developed on the foundation of Hill and Nance's (2016) Salesforce Max Labs project, out of San Jose State University.

7. REFERENCES

Baraković, S., & Baraković Husić, J. (2023). Cyber Hygiene Knowledge, Awareness, and Behavioral Practices of University Students. *Information Security Journal: A Global Perspective,* 32(5), 347-370. https://doi.org/10.1080/19393555.2022.2088428

Baxter, R. J., Holderness Jr, D. K., & Wood, D. A. (2016). Applying Basic Gamification Techniques to IT Compliance Training: Evidence From the Lab and Field. *Journal of*

Information Systems, 30(3), 119-133. https://doi.org/10.2308/isys-51341

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An Exploratory Study of Cyber Hygiene Behaviors and Knowledge. *Journal of Information Security and Applications,* 42, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Esparza, J., Caporusso, N., & Walters, A. (2020). Addressing Human Factors in the Design of Cyber Hygiene Self-Assessment Tools. In I. Corradini, E. Nardelli, & T. Ahram (Eds.), *Advances in Human Factors in Cybersecurity* (pp. 88-94). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-030-52581-1_12

Hill, T., & Nance, W. (2016). Innovating Business Systems Labs for Engaging Igeneration Students. AMCIS 2016 Proceedings, 29 https://aisel.aisnet.org/amcis2016/ISEdu/Presentations/29

Kalhoro, S., Rehman, M., & Shaikh, F. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access,* 9, 99339-99363. https://doi.org/10.1109/ACCESS.2021.3097144

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic Cyber Hygiene Education: Accounting for the Human Factors. *Computers & Security,* 92, 101731. https://doi.org/10.1016/j.cose.2020.101731

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (Hais-Q): Two Further Validation Studies. *Computers & Security*, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778. https://doi.org/10.2307/25750704

Sclarow, S., Raven, A., & Doyle, M. (2024). Teaching Tip: Leveraging Learning Strategies at Scale–Big and Small Changes in a Big IS Course. *Journal of Information Systems Education*, 35(1), 1-13. https://doi.org/10.62273/FLSR7630

Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic Cyber Hygiene: Does It Work? *Computer*, 52(4), 21-31. https://doi.org/10.1109/MC.2018.2888766

Tan, J. A., Hall, R. J., & Boyce, C. (2003). The Role of Employee Reactions in Predicting Training Effectiveness. *Human Resource Development Quarterly*, 14(4), 397-411. https://doi.org/10.1002/hrdq.1076

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests. *Decision Support Systems*, 128, 113160. https://doi.org/10.1016/j.dss.2019.113160

AUTHOR BIOGRAPHIES

David Kocsis holds a Ph.D. in information technology with a concentration in information systems from the University of Nebraska at Omaha and is an assistant professor of information systems (IS) at the University of Colorado at Colorado Springs. He teaches courses in Networking, Introductory Information Systems, and the capstone IS projects course. His research interests include collaboration science, social issues in IS, cybersecurity threats, and security education, training, and awareness. He had more than 15 years of industry experience in information technology, networking, and cybersecurity before pursuing academia in 2012.

Morgan Shepherd holds a Ph.D. in information systems and is a full professor at the University of Colorado at Colorado Springs. He teaches courses in Networking, Information Systems Literacy, the capstone IS projects class at the undergraduate level, and Information Systems at the graduate level, both on-campus and online. He has over ten years of industry experience, most of which came at IBM.

Daniel L. Segal is the Kraemer Family Professor of aging studies and professor of psychology at the University of Colorado at Colorado Springs. His program of research focuses on the assessment of psychopathology among older adults, the expression and measurement of anxiety in later-life, suicide risk and resilience and aging, and the impact of personality disorders across the lifespan. He is also interested in cyberpsychology. He is a Fellow of the Gerontological Society of America and of the American Psychological Association (Division 12 and Division 20). He has published over 200 peer-reviewed journal articles and book chapters and 6 professional books.

APPENDICES

Appendix A. Survey Measures

Pre-Survey and Follow-Up Survey
The *pre-survey* contains questions related to cyber hygiene knowledge and behaviors, plus demographics. The *follow-up survey* contains the same questions from the pre-survey, minus the demographics.

The knowledge questions range on a scale from strongly disagree to strongly agree, with an option for do not know/understand. The behavior questions range from never to always, with an option for do not know/understand. We adapted scales based on existing cyber hygiene measures (Cain et al., 2018; Parsons et al., 2017; Vishwanath et al., 2020). When comparing the follow-up survey to the pre-survey, we include a minus sign where answers should be lower in the follow-up survey and a plus sign where answers should be higher in the follow-up survey.

Password Knowledge
1. It's acceptable to use my social media passwords on my bank accounts (-)
2. It's acceptable to share my passwords with colleagues/classmates/friends (-)
3. A long password with a mixture of letters, numbers, and symbols is necessary (+)
4. It is acceptable to store my passwords in my web browser (-)

Password Behavior
1. I use a different password for my social media and bank accounts (+)
2. I share my passwords with colleagues/classmates/friends (-)
3. I use long passwords with a combination of letters, numbers, and symbols (+)
4. I store many of my passwords in my web browser (-)
5. I enable two/multi-factor authentication for logins (+)
6. I store logins and passwords in encrypted online password vaults (+)

Email Use Knowledge
1. It is acceptable to click on links in emails from people I know (+)
2. It is acceptable to click on a link in an email from an unknown sender (-)
3. It is acceptable to open an email attachment from unknown senders (-)

Email Use Behavior
1. If an email from a known sender looks interesting and contains a link, I click on the link (+)
2. If an email from an unknown sender looks interesting and contains a link, I click on the link (-)
3. I don't open email attachments if the sender is unknown to me (+)
4. I check to see if email messages have grammatical or typographical errors (+)
5. I check an incoming email's address and domain name before opening it (+)

Internet Use Knowledge
1. Some websites are malicious, which means if I visit the website, my computer may become infected with malware (+)
2. I can assess the safety of a website by checking the lock icon (also known as SSL) on the web browser to see if a website uses encryption (+)

Internet Use Behavior
1. I download files onto my computer without considering the source (-)
2. I assess the safety of websites by checking the lock icon (also known as SSL) on the web browser before entering information (+)

Social Media Use Knowledge
1. It is important to periodically review the privacy settings on my social media accounts (+)
2. I cannot be fired from my job for something I post on social media (-)

Social Media Use Behavior
1. I regularly review my social media privacy settings (+)
2. I don't post anything on social media until I consider possible negative consequences (+)
3. I assess the authenticity of social media friend/information requests (+)
4. I reassess social media friends/connections (+)

Mobile Device Behavior
1. I send sensitive files using a public Wi-fi network (-)

2. I visit sensitive websites (e.g., banking) using a public Wi-fi network (-)
3. I use a Virtual Private Network (VPN) on an open/public Wi-fi network (+)

Device Protection Behavior

1. I have a firewall running on my primary computer (+)
2. I block ads on my web browser (e.g., AdBlock plug-in) (+)
3. I either block or regularly clear cookies on my web browser (+)
4. I disable pop-ups on my web browser (+)
5. I use a secure web browser (e.g., Brave) instead of the mainstream web browsers (e.g., Chrome, Firefox, Edge, Safari) (+)
6. I use Incognito or Private mode when surfing the Internet (+)

Backup Behaviors

1. I maintain backups of my files in the cloud (e.g., iCloud, Dropbox, OneDrive, Google Drive) (+)
2. I maintain backups of my files on an external hard drive or USB stick (+)

Update Behaviors

1. I regularly update my device to ensure it has the latest operating system, software updates, and patches (+)
2. I regularly update my system's antivirus software (+)

Demographics

1. What is your current age (in years)?
2. Considering this survey is about understanding technology knowledge and behaviors, there can often be significant differences depending on gender identity. The answer you provide will be used solely for this purpose and will be anonymous. Please provide your gender identity.
   a. Man
   b. Woman
   c. Non-binary / third gender
   d. Prefer not to say
   e. Other (feel free to disclose or not):
3. Similarly, there can often be significant differences depending on race/ethnicity. The answer you provide will be used solely for this purpose and will be anonymous. Which of the following best describes you? Please select one answer.
   a. Asian or Pacific Islander
   b. Black or African American
   c. Hispanic or Latinx
   d. Native American or Alaskan Native
   e. White or Caucasian
   f. Multiracial or Biracial
   g. A race/ethnicity not listed here
   h. Prefer not to say
4. What operating system do you use for your primary computer?
   a. MacOS
   b. Windows
   c. Linux
   d. Other/More than one of these
   e. Don't know
5. What is the highest level of education you have completed?
   a. High school diploma/GED/or less
   b. Some college, no degree
   c. Associate degree
   d. Bachelor's degree
   e. Trade school certification
   f. Master's degree or higher education
   g. Other (Please fill in)
   h. Prefer not to say
6. What is (or was) your primary college major?

Post-Survey

We adapted the *post-survey* from Tan et al. (2003) to assess their learning and measure satisfaction with the module. Response options range from strongly disagree (1) to strongly agree (5), showing that the mean was incredibly high for all items.

Category and Reliability	Question	Mean	Standard Deviation
General evaluation (α = 0.97)	I would recommend the cyber hygiene module to other people who have the opportunity.	4.45	0.97
	I have an overall good feeling about how the cyber hygiene module was carried out.	4.45	0.84
	I would recommend that every student take part in this cyber hygiene module.	4.40	0.92
	The cyber hygiene module allowed me to develop specific skills that I can use in the future.	4.39	0.90
	The cyber hygiene module was, overall, very effective.	4.44	0.85
	The cyber hygiene module was very useful.	4.46	0.87
Hands-on scale (α = 0.94)	The cyber hygiene module gave me new knowledge that I could use in the future.	4.50	.80
	The cyber hygiene module sharpened my current cyber hygiene behaviors.	4.48	0.84
	The cyber hygiene module gave me tools to secure my online presence.	4.53	0.78
Understanding scale (α = 0.93)	The cyber hygiene module was a good way to take the "textbook material" to the real world.	4.46	0.86
	The cyber hygiene module gave me a better understanding of protecting against online threats.	4.51	0.83
	The cyber hygiene module allowed me to gain new insight for the scope of online threats.	4.52	0.78
Improvement scale (α = 0.91)	As a result of the cyber hygiene module, I could explain cyber hygiene principles to a non-expert.	4.22	0.83
	I now have new understanding that I can use when talking with people about online threats.	4.34	0.79
	The cyber hygiene module will make me a better user in school and/or work.	4.42	0.86
	The information covered in the cyber hygiene module contributed to my learning.	4.46	0.85

Note: N=144.

Table A1. Questions, Categories, Reliabilities, Means, and Standard Deviations in Post-Survey

Appendix B. Cyber Hygiene Salesforce Module

This appendix contains the full cyber hygiene Salesforce module, which was built and expanded from the Salesforce Max Labs Project.

Business Systems Innovation Labs

Cyber Hygiene Module Pre-flight Checklist

"Cyber hygiene: It's time to give my system a bath"

Welcome! Whether you have or haven't met her yet, follow along with Max Flanagan as she helps you navigate the world of Cyber Hygiene! She will show you how to stay safe and make smart tech choices, while having fun in the process, so get ready!

Prep: Get ready

- ✓ If you have not participated in the Max Labs Project assignments:
  - Be sure you read the Pre-lab backstory (Lab 0) first, so you know Max & what's going on with her.
  - Create your FREE Salesforce Developer Edition (DE) account—follow the steps on the next page, then return right back here.
- ✓ SALESFORCE MAY NOT WORK RIGHT UNLESS YOU turn off ad/popup blockers AND allow cookies:
  - In Safari, select Preferences, click the Privacy tab & make Prevent cross-site tracking unchecked
  - In Chrome, select Preferences, scroll down to Privacy & Security, click on Cookies and other site data& make Allow all cookies checked
  - In Firefox, select Preferences, Privacy & Security& make Standard selected

Learning Objectives: What to "get"

- ✓ What is cyber hygiene and why is it so important?
- ✓ What is a strong password? How can passwords be managed?
- ✓ How to identify and protect yourself from phishing scams.
- ✓ See how Salesforce backs up its user's data, and why backing up your own data is so important.
- ✓ Learn about antivirus and firewall protection for your device.
- ✓ How to manage and improve your personal computer security.
- ✓ Managing your privacy settings.

Tips: Get more

Do not just zoom through the steps—you will miss out if you do. Please follow the embedded hyperlinks when you see them—they're there for you to learn more valuable stuff & get the most from your experience!

Get your CREDIT

Your instructor will provide you with instructions to receive credit for this module.

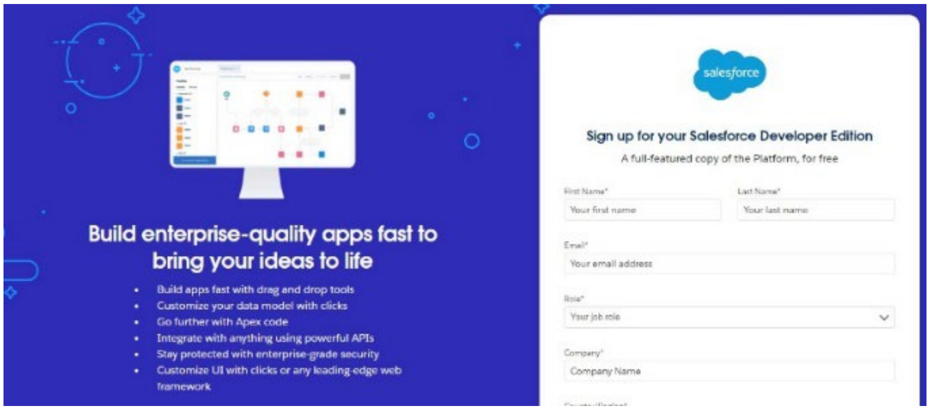
Resources: Get help

Stuck? DON'T TRY TO UNDO/REDO THE WHOLE MODULE – that can make things worse! Instead, just contact your instructor.

Create your FREE Salesforce Developer Account

Note: If you already have a Salesforce Developer account, you may skip this part.

Get a SF account but DO NOT GET THE 30-DAY FREE TRIAL ACCOUNT! Instead, go to https://developer.salesforce.com/signup and get the free, lifetime Salesforce "Developer Edition" (DE) account. The web page with the form should look like this:



Build enterprise-quality apps fast to bring your ideas to life

- Build apps fast with drag and drop tools
- Customize your data model with clicks
- Go further with Apex code
- Integrate with anything using powerful APIs
- Stay protected with enterprise-grade security
- Customize UI with clicks or any leading-edge web framework

Sign up for your Salesforce Developer Edition

A full-featured copy of the Platform, for free

First Name*: Your first name
Last Name*: Your last name
Email*: Your email address
Role*: Your job role
Company*: Company Name

On the signup page, enter your real name and use a real email address—one you can log into—bc they send you an email with the link to set your password & get started. (**Do NOT use a Yahoo, Hotmail or AOL account**—they don't play nice with SF! **To be safe, just create new a Gmail account to use just for this.**)

For **Role** and **Company**, anything's ok, but for **Country**, be sure to pick **United States**, even if you're someplace else, just to make sure everything works like I show you below.

Then for **Postal Code** you can just use your own or you can use mine (**95192**) if you're outside the US. For **Username**, you can enter anything that LOOKS like an email address, even if it's not real, eg "hippo@suitcase.sauce" will work as long as nobody else already used it! Whatever—just make sure you remember it and your pw, especially.

Check the email account you've entered, find the "Welcome...Verify your account" message & click **Verify Account**. Follow the instructions to set your password & voila—you're logged in! Now, kill the "Welcome to Lightning Experience" panel that pops up. (Hit the little "X" on the top right corner.) Don't panic—I'll be your personal trainer/tour-guide!

Now return to the instructions on the previous page before continuing.

Max's Distinctive, Impressive BizTech Student Blog

Wednesday, January 1, 2020

Previously on Max's Distinctive, Impressive BizTech Blog

Happy New Year! It's Max Flanagan again. Still working on that distinctive, impressive BizTech blog from earlier this semester. If you haven't checked out my totally awesome blog yet, make sure to read this summary below. If you have seen my blog, go ahead and ignore the summary and jump down to the next page (you're already my favorite by the way).

Summary

For those of you who haven't read my blogs or completed the six Salesforce labs, allow me to introduce myself. I'm Max (a girl btw – "Margaret" officially), and I'm a Marketing student at SJSU (San Jose State University) stuck in BUS 188 (Intro to Business Technology Systems Something). While I love a good movie binge while eating my favorite snack (chili/cheese fritos + chocolate chips), I'm not at all techie (which is a super tech savvy person btw).

Prof (short for professor) wanted us to make a blog to keep track of what we learn and build our "personal brand", and so far, it's been a real success, if I do say so myself. We are learning all about innovation, entrepreneurship, and how we can manage data. We got to mess around with and create databases through Salesforce, a hot tech right now. In class we just kinda messed around with it and did the basics, but I wanted to take it one step (and then many steps) further.

I went to this entrepreneurship meeting and got to see both sides of BizTech (business technology, I like abbreviations lol), the suits and the geeks. Suits—or people in, well, suits—focus more on the business side of things. Geeks are the ones who know the tech and do all that techie sort of stuff...both people are super smart. Anyways, I met this Suit there named Riley who talked to me about startups and investors and how they have all this info that they need organized for their startup, they needed a geek.

Somehow that geek turned out to be me (and I am NO tech pro by any means). I just used the stuff I learned about Salesforce in class and thought "hey this might be super helpful to Riley." Long story short, she loved the idea and I started getting paid for pretty much messing around with a database to make what she needed! Pretty neat, huh!?

I've helped Riley with everything from creating and managing Pitches to creating automatic emails and replies through a Customer Relationship Management system (you heard about CRM in class, right?). I also helped her prioritize her investments (separate the big $ from the not so big $) and get rid of copied data, which threatens the integrity of a database. I even created relationships between databases, which basically creates your own handy-dandy personal cyborg in Salesforce to do all the work for you.

OK, time to clean up…

Max's Distinctive, Impressive BizTech Student Blog

Saturday, January 4, 2020

So, you think you're safe? Think again!

My Prof says the start of a new year is always a great time to check your cyber hygiene. Ever heard of that? I hadn't, so I decided to read some articles, and it was actually really cool. Here's what I found:

Not only businesses, but individual people, face cyber threats every day. In fact, I read a cool article that said there are around 2,200 successful cyberattacks per day, which equates to more than 800,000 people being hacked per year…insane, right?! And that's just attacks on individual people. I found this article with some examples of the biggest cyber attacks of the 21st century. It's crazy to see all these big companies getting hacked. Like what would people have to gain from hacking companies like Yahoo (twice, yikes). Turns out people want more than just money or physical stuff.

Before I started researching cyber hygiene, I thought cyberattacks were just a fancy tech way for executives like Elon Musk and Mark Zuckerberg to threaten one another. I thought cyber threats were all about companies holding information from other companies just to get more money and power. After digging deeper, however, I realized you and I are just as likely, if not MORE likely to be attacked by those dark-hooded basement witches.

Some of the most common forms of cyber threats I found in my research were malware, phishing, and social engineering threats. There are a ton more but these are some of the biggest ones.

Malware (short for "malicious software") is a file or code, usually delivered over a network, that infects, steals, or conducts pretty much any behavior an attacker wants on your computer. Types of malware include computer viruses and worms, along with one of my favorite terms I found in my research: a Trojan horse. A Trojan horse is a type of malware that downloads onto a computer disguised as a legit program…clever term, right?

Phishing, not at all related to fish in anyway, is when attackers send you a fake email pretending to be a trusted source. Their goal with these messages is to get you to give them your private info so they can access your computer and put bad things on there. Stuff like viruses and ransomware. **Viruses** affect or alter the function of your device, either breaking it internally or making it not work well at all. It also can spread from computer to computer. **Ransomware** is when the hackers hold your information hostage, asking for money in exchange for your data or info back. Pretty evil stuff.

Social engineering is another attack hackers use that can be incredibly effective. This can be used with really any sort of attack, phishing included. It's when people use our humanity to persuade or trick us. It doesn't use any brute force or insane code to get into your computer, its "hacking" us as people, hacking our brains kinda. It's psychological manipulation that persuades us into giving up private and sensitive info to those hackers. Prof showed us this example in class…it's a must watch, I promise! It's less than 3 minutes long.

So I know these all sound like big words that have no relevance to our lives, but if you think about it, they really do. Every time we hop on Instagram or Facebook to check out our friends' latest post, or check our emails for the best coupon, we're at risk if our cyber hygiene isn't up to par…just like you're at risk of being "that" person if you don't shower…don't be "that" person.

Well that's all I have for now. But don't worry, there'll be plenty of stuff to come.

To be continued… (also always wanted a reason to say that haha)

Max's Distinctive, Impressive BizTech Student Blog

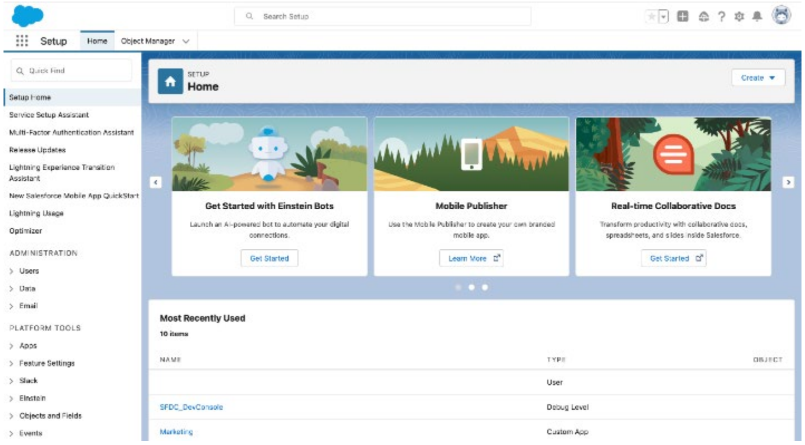
Friday, January 10, 2020

Interface Check (kinda like fit check...get it?)

Okay so a little update on me and Riley and my awesome app that I created for her. As I was reading those articles about Cyber Hygiene, I sent some of them to Riley. I thought maybe she would know something about it.

Turns out that stuff kinda freaked her out. She got nervous that her or her clients' information could be stollen, rightfully so. She tasked me (since I had already done all this research) with finding some ways to keep her and her company more safe from those evil hooded people of the internet. But before we get into the nitty gritty of staying tech safe, I think a quick refresher of Salesforce might be helpful.

Thankfully, the big genius Salesforce creators made their program/database easy for average joe business students (like yours truly) to use. The Salesforce homepage has tabs at the top of the page, which consists of an App Launcher (the little "waffle" thingy under the cloud that has some different apps to use and develop within Salesforce) and Object Manager (where you can create new objects and view the past objects you created). There's a search bar, the handy dandy gear icon in the top right, your account icon, and a few other things there at the top. On the left side under the waffle App Launcher, is a list of a bunch of different tools that have been very useful for building that app for Riley. (See image below for the "home screen" when you click that gear in the top right and click Setup, I do this a lot)



Get Started with Einstein Bots

Launch an AI-powered bot to automate your digital connections.

Mobile Publisher

Use the Mobile Publisher to create your own branded mobile app.

Real-time Collaborative Docs

Transform productivity with collaborative docs, spreadsheets, and slides inside Salesforce.

Most Recently Used

10 items

NAME	TYPE	OBJECT
	User	
SFDC_DevConsole	Debug Level	
Marketing	Custom App	

Knowing these basic Salesforce functions is like putting on deodorant before going to an important meeting...it's very necessary and helps prevent a whole lotta embarrassment. It's better to prevent a stinky situation than have to recover from it.

What's a Hackers Favorite Season? Phishing Season

(How do you choose a strong password? Go to the gym and find the one lifting the heaviest weights!)

I know, you're tired of my blog already. So let's get to work! You should have created your Salesforce account earlier, so go ahead and log in (login.salesforce.com) if you aren't already.

BTW, you should be using Firefox or Chrome for this, not SteveFari (er, Safari – but I think they should rename it to honor Steve Jobs) nor Edge/Internet Explorer. Those stink. IRL, you should use a browser that protects you better, like Brave. If you haven't heard of it, it does a lot of cool stuff to protect your privacy – popup blocker, ad blocker, cookie blocker – it even removes those annoying YouTube ads! BTW, make sure you turn off any popup blockers for this app (I know, it's totally anti-cyber hygiene, but it will work better – just shower when you are done lol). But again, for this module – Chrome or Firefox will do.

Guess what? I gave myself a promotion. I'm now the Senior Systems Administrator (SysAdmin) for Riley. I get to create/manage users, install patches on our network, make sure passwords are good, etc. I'm kind of a big deal – in the real world it's a big responsibility, but it can also be big $$$$. And congrats – you are a Senior SysAdmin now too! So you have your own powerful account on the app, but let's create two more users – because without users, what is the point of having a CRM? One user is going to be a pretend hacker and one will be a pretend victim. But first, we need to set up some policies for our passwords:

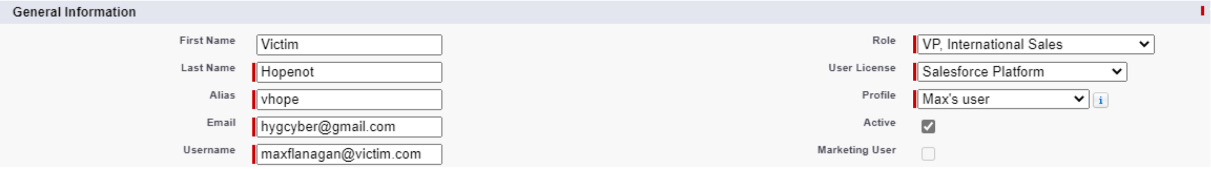
1. Go to the big **Setup** gear icon on the top right corner (next to the bell) and click **Setup**
2. On the left, under **Administration**, click **Users – Profiles**
3. Salesforce has all these built-in authorization profiles. Kind of like for Canvas or Blackboard or Moodle for your class – Prof can see and change everyone's grades, but students can only do what the Prof lets us. So we can set up a profile with all sorts of rules for authorizing our users. We'll even set up a password policy. In our case, we'll borrow a profile that's already been set up
4. Click **Next** at the bottom of the page
5. Scroll down to **Standard Platform User** and click **Clone**
6. Name our new profile "Max's user" and click **Save** (BTW, never include the quotes unless I tell you to)
7. Click **Edit** so we can set it up. ALL my users will get these settings, so I don't need to change it every time I set up a new user!
8. Scroll way down to the bottom under **Password Policies**

Now, we need to have a serious talk about passwords. Do you ever see on Facebook or Insta that some friend from grade school gets hacked? Yeah, that should never happen. Basically, these hackers brute force attack passwords – they try all these different password combos until they get it right. We want passwords that are long, strong, and complex – Prof calls it entropy. You can see how long it takes a hacker to crack your password here. Remember when you set up your account, Salesforce only required 8 characters, with at least one number and one letter. Guess what? The password "hiImMax8" takes a whopping 1 hour for a hacker to crack. So, we are going to force our users to have stronger passwords:

9. Change **Minimum password length** to "12"
10. Change the drop-down menu for **Password complexity requirement** to "Must include numbers, uppercase and lowercase letters, and special characters"
11. We could change some of these other things, but hey, we need to type in these passwords, so let's not go too overboard
12. Scroll up to **General User Permissions**
13. See where it says **Multi-Factor Authentication for User Interface Logins** on the right? Prof calls this MFA or 2FA (two-factor authentication). Basically, when you log in, the app will shoot ya a text message with a code. This is SUPER secure and you should ALWAYS do it. Your Insta will almost never get hacked if you use it. However, it would take about 50 steps to set up MFA, so we'll leave the box unchecked
14. At the bottom of the page, click **Save**

Now we're talkin' – we just forced our accounts to have long, strong, complex passwords (even though we didn't use MFA). I feel more secure already and can prove it. If I used the password "hiImMax12?!1" – it would take a hacker 400,000 years to crack it. And it would be even more difficult for a hacker if we did use MFA. Now let's create a user, who will BE. OUR. VICTIM. Du Du Duuhhh...

15. On the left, under **Administration**, click **Users – Users — New User** (in the middle)
16. For **First name**, call him "Victim"
17. For **Last name** – "Hopenot" then hit tab so **Alias** fills in automatically
18. For **Email**, use YOUR email address. Tab down and it will automatically fill in the **Username**, but let's change the **Username** to "firstnamelastname@victim.com" (using YOUR first and last name)
19. Change **Role** to "VP, International Sales" – seems like a fun role to hack
20. Change **User License** to "Salesforce Platform" and **Profile** to "Max's user"
21. Click **Save** at the top
    If you get some ERROR that says "Duplicate Username," just add a number to the end of the username. The important thing is that you have a new account for our victim, and you'll create the password later.



General Information

First Name	Victim	Role	VP, International Sales
Last Name	Hopenot	User License	Salesforce Platform
Alias	vhope	Profile	Max's user
Email	hygcyber@gmail.com	Active	☑
Username	maxflanagan@victim.com	Marketing User	☐

You should get an email in your inbox for your new victim user. Sign out of Salesforce (the profile icon on the top right). Then click the victim email you received so we can finish setting up his account (just click Verify Account in the email you received).

Remember when you set up your own account? 8 characters, 1 uppercase, blah. Now look, it contains the requirements we set up earlier!

Create a password and security question for the Victim user. Oh, and Prof reminded me of two things. 1) NEVER let your browser store your passwords. Thieves love when dummies do that! 2) Sick of creating all these passwords? Me too. I used to just make everything the same PW, which is some terrible old school habit. Like, my bank account had the same password as my ESPN and Netflix accounts. *Face slap.* You gotta make your passwords different. Prof said to use a password manager like LastPass or 1Password. I started using LastPass and I never have to worry about passwords and all my passwords are different! Seriously, try it – it changed my life.

Next step – I want to see how strong your password is. Please type (or write) in your password **here:** ______________________. JK. Never ever ever give your password to someone. I don't even give my passwords to my MOM.

Now let's move on and do some phishin'!

I talked about phishing earlier. Let's be the hacker and try to lure (get it?) someone in. Log out of the victim's Salesforce account (profile icon on top right – Log Out), then log into Salesforce using YOUR account.

22. Go to **Setup** (gear icon on top right) – **Setup**. We are going to create an email message template that we (as a hacker) can send to potential victims. By the way, I already created a phishing website, so our phishing message will tempt them to visit our fake website. You can see the URL below step 30
23. Go to **Administration – Email – Classic Email Templates**
24. Click **New Template**, click **Custom (without using Classic Letterhead) –** Click **Next**
25. Check the box for **Available For Use**
26. For **Email Template Name**, call it "phishing" – tab down to accept the **Template Unique Name**
27. In the **Description**, type "For getting passwords and maybe $"
28. For **Subject**, type "<Salesforce AWARD, CLICK NOW!>" – click **Next**
29. In the **HTML Email Content** section, copy and paste the following into the **HTML Body**:

    Dear NAME, <br>

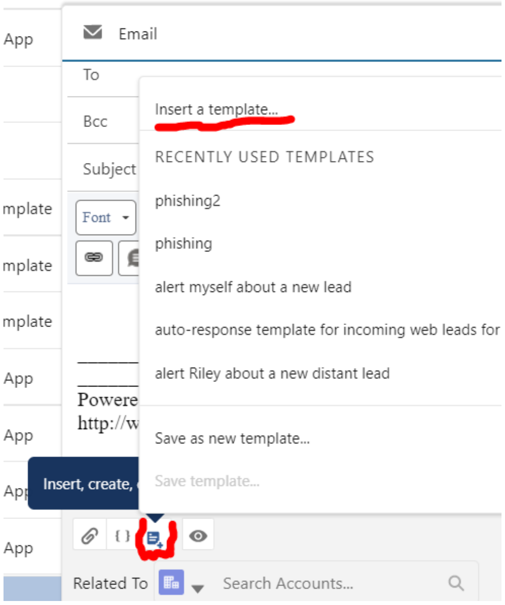
    My name is Max Riley and I'm the head of customer relations at salesforce. Because of your recent activity using our programs, we've selected you as the winner of our annual entrepenership grant of $3000! <br>

    To except your award, please click the link below: <br>
    <a href="https://hygcyber.weebly.com/" target="_blank">Click Here! </a><br>

    This is a once in a lifetime opportunity to grow your business so be sure to click now! If you don't respond within the next 12 hours, we will give this award to another candidate. <br>

    Looking forward to hearing from you, <br>
    MR

30. Click **Next**
31. At Step 4, click **Copy text from HTML version –** on the warning window, click **OK** then click **Save** (don't worry about the lack of spacing)
32. Now let's send our phishing message! Click **Global Actions** (the gray and white plus sign on the top right, near the **Setup** gear icon) – **Email**
33. In the **To** section choose **Victim Hopenot**. Remove your email address from Bcc (you're already gonna get the email anyways)
34. At the bottom, above Related To (see screen shot below), click the **Insert, Create, or Update Template** button – **Insert a Template** (you might need to click "all classic templates" in the top left dropdown menu) – choose the **phishing** template we created earlier (if you get a message that says "Inserting this template...blah blah," just select **Insert**)



35. Click **Send** then check your email. BTW, you might need to check your SPAM or JUNK email folder!
36. This is clearly SPAM and a phishing attempt. How do I know, and how can you identify phishing messages?
    - First, it may have ended up in your SPAM/JUNK. Clear indication. But not all SPAM messages get filtered
    - Look to see who the sender is. This actually came from Salesforce.com, but the name looks phishy
    - It just says “Dear NAME” – a legit message would have your name (but sometimes illegit will too)
    - There are some typos – but beware, some phishing messages have good grammar. With the emergence of ChatGPT, there are a lot fewer misspellings now, so watch out!
    - Sometimes there will be some real long URL. Not this one – it’s high quality. See the Click Here!? Move your mouse and HOVER (do NOT click) the Click Here! Notice it goes to weebly.com. If it was legit, it would be Salesforce.com
37. Don’t do this IRL...but since WE created this fake email, let’s test it out. Click the **Click Here!** link in the email you received
38. Scroll through the page – the hacker tried to make it look like Salesforce, but the URL is off, and the website is a joke lol. Like, <NAME>, come on! And that logo??? Grammar?
39. But let’s keep being good victims. Click the **click here to claim your award** button
40. This is what the attackers try to do—get you to enter your username and password. And guess what—if you enter this info, the hacker now has it! They also might ask to enter your bank or Venmo info too. Feel free to put in some fake info and click Submit.

That was a tiring day of phishing and getting phished. I’m getting seasick. Get a drink of water and we’ll move on...

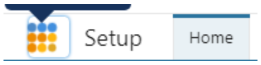
<u>Protect your computer like you would protect your dog</u>

OK, friends. It’s time for a serious talk. Prof tells me that when our computers send information it isn’t actually sending information. What she means is, if I send you a video of my dog eating my homework, it’s not a video that’s going over those wires and air waves – the computer is sending bits, which are just a bunch of 0s and 1s. And if a hacker can see those 0s and 1s, it’s a problem. Not so much for my dog video, but it’s a serious problem if she gets my Social Security number or my bank account.

OK, how to protect those pesky bits...it’s like I have some spinach in my teeth, I gotta work on that (cyber) hygiene. Prof has some suggestions that most (not all) businesses do, and all people should do.

In general, you should always **back up** your data to an external hard drive or the cloud. I use OneDrive because it’s free at school. Luckily Salesforce backs stuff up automatically to the cloud for us, so let’s see how that works.

41. Click the 9 dots (the ones that kinda look like a waffle or rain under a cloud, aka the **App Launcher**) in the top left next to **Setup** – click **Marketing**



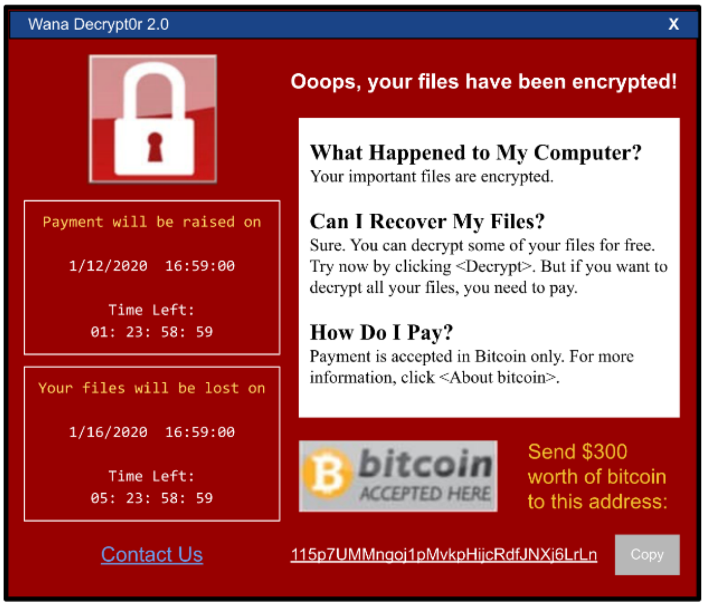
42. Click **Contacts** at the top of the page
43. Click **New** at the top right to create a new contact
44. For **First Name**, type “Audrey” and for **Last Name** type “Millionaire” – click **Save**

Imagine Audrey is some millionaire who was going to give us $1,000,000 for an investment. Then some newbie goes into the system and deletes Audrey. They are gone, and we cannot contact them. Or can we? Let’s delete Audrey and find out.

45. Click **Contacts** at the top again
46. To the far-right side of the **Audrey Millionaire** user you just created, click the down arrow and click **Delete** (Salesforce pops up a confirmation window to delete the contact – click **Delete** again)
47. Click the **App Launcher** (those 9 dots on the top left next to **Setup**) – search for **Recycle Bin** and click it
48. There she is, the **Audrey Millionaire** user! To the far-right side, click the down arrow and click **Restore**. Go back to the Contacts tab and you will see that Audrey is back. WHEW – we almost lost a cool million

Backing up our files and systems is incredibly important for accidental hacks like deleting users or files. But it can also protect us from hackers too, so **backup** is a big cyber hygiene best practice.

My uncle is a big wig at some company who was a victim of ransomware. The hackers encrypted his company’s files and would not decrypt the files until the company paid $2 million. If you’ve never seen what happens when you get infected with ransomware, here’s a scary example:



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.

Can I Recover My Files?
Sure. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Payment will be raised on
1/12/2020 16:59:00
Time Left:
01: 23: 58: 59

Your files will be lost on
1/16/2020 16:59:00
Time Left:
05: 23: 58: 59

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Ever since then, my uncle’s company spent big $$$ on backing up their files to the cloud and to external drives that they store in another city – if a hacker ever holds the files hostage, my uncle can say “who cares, it’s all backed up.” Holding those files in another city also protects them from natural disasters like floods and tornados.

So are you feeling protected? Or vulnerable? Check out your system to see how well it is protecting you. If you are on Windows, continue to step 49. If you are on a Mac, skip to step 54.

Windows steps:

49. Go to the bottom left corner of Windows, in the **Type here to search** bar, and type “Virus” – you should see **Virus & Threat Protection** (click this to open the security info on your computer)
There is a LOT of stuff here. 10 years ago, Windows did not have all this – you had to do it yourself. But now that security (and cyber hygiene) is so huge, Microsoft is better about building security into the system. You will see if there are any current threats, scan status, virus settings, ransomware protection, etc.

50. On the right side—under **Who’s protecting me?** —click **Manage providers**. This part has three sections—Antivirus, Firewall, and Web protection. We’ll look at those first two
51. **Antivirus** protects you from viruses and malware and spyware (a virus that will spy on you, like being able to see everything you type, yikes!) Even if a virus does get on your system, your Antivirus will clean it for you (unless it’s a really bad virus)

Windows even has its own antivirus BUILT INTO the system. It's called Microsoft Defender. If you have your own antivirus, it will also be listed here (e.g., Webroot, Norton, AVG, etc.). If you do not have an additional antivirus, get one

52. **Firewall** blocks traffic coming into your computer/network. Basically, any trusted apps/traffic are allowed by default. But you can go in and block/allow any apps you need. So, firewall and antivirus are two key pieces of software to protect your operating system. If Firewall is off, turn it on NOW!

Another important thing to do is make sure your operating system is updating itself regularly. Without updates, hackers find holes in your system and exploit it, rendering your protection settings useless

53. Go back to the **search bar** on the bottom and type "Update" – click **Windows Update Settings**. Hopefully it says "You're up to date" – if not, run your updates as soon as you get done with this assignment. Microsoft got smart about this a few years ago – updates *should* install automatically by default

Now that you feel protected and up to date, skip down just below step 61 to meet up with our Mac users…

Mac steps:

54. Go to the top right corner of your Mac. In the **Spotlight Search** bar, type "Security" – you should see **Security & Privacy** pop up (click this to open the security info on your computer)

There is a LOT of stuff here. 15 years ago, Apple didn't have all this – you had to do it yourself. But now that security (and cyber hygiene) is so huge, Apple is better about building security into the system.

55. At the top of the **Security & Privacy** page, you should see four tabs – General, FileVault, Firewall, and Privacy. Click **Firewall**
56. If Firewall is off, turn it on NOW! A **Firewall** blocks traffic coming into your computer/network. Basically, any trusted apps/traffic are allowed by default. But you can go in and block/allow any apps you need

Antivirus protects you from viruses and malware and spyware (a virus that will spy on you, like being able to see everything you type, yikes!). Even if a virus does get on your system, your antivirus will clean it for you (unless it's a really bad virus).

Mac even has an antivirus BUILT INTO its system. It's called XProtect (sounds like an Avenger character lol). If you have your own antivirus, it'll also be listed in your top navigation bar (e.g., Webroot, Norton, AVG, etc.). If you do not have an additional antivirus, get one! But let's check on XProtect:

57. Click the **Apple menu** – **About This Mac**
58. Click **System Report** – **Software** – **Installations**
59. Scroll down until you find **XProtectPlistConfigData** – this will show you the current version of your XProtect software (it's always ON by default, but you won't see this)

So, firewall and antivirus are two key pieces of software to protect your operating system.

Another important thing to do is make sure your operating system is updating itself regularly. Without updates, hackers find holes in your system and exploit it, making your protection settings pretty useless.

60. Go back to the **Spotlight Search** bar in the top right corner of your Mac and type "Update" – click **Software Update**. Hopefully it says "Your Mac is up to date" – if not, run your updates as soon as you get done with this assignment (tell your teacher this is an order from Max…respectfully of course).
61. At the bottom of the **Software Update** page, there should be a checkbox next to **"Automatically keep my Mac up to date."** If this box isn't already checked, CHECK IT (another order from Max, but I promise I'm just trying to protect my fellow cyber friends).

****OK, all my Windows and Mac users should be HERE NOW. ****

Remember, we only looked at your PC/laptop settings. You should set all these up on your phone/tablet too! **Q:** How does a virus/malware/spyware get in? **A:** Holes in the operating system or an app (update all your apps too!), or YOU downloading a file from the Internet or from an email. YOU should always KNOW what file/app you are opening…but also keep your antivirus and firewalls running too.

OK we only have a few more things to talk about for PROTECTING yourself and becoming clean cyber users…hopefully you're this clean irl too. You use the Internet, right? DUH. Like, constantly. What web browser do you use (Chrome/Firefox/etc.)? Do you ever look at the settings? Do you use public wi-fi, like at Starbucks (cause I definitely do…nothing like enjoying an iced caramel macchiato with homework, am I right?)

If you use Chrome, Firefox, Safari, or Edge – these browsers have some…but not much security. But you can make them more secure:

62. Open your browser and go into the settings (top right corner – 3 dots or 3 lines) – click **settings**
63. **Turn on a pop-up blocker**. Pop-up windows are a common way viruses get on computers. My Grandpa will call me every couple months – "MAX, I clicked on this popup window, and now my computer is slow" – I help him do an antivirus or anti-spyware scan, and it usually fixes it, but it's a pain in my you know what. You can even install ad-blocking plug-ins, cause sometimes ads can get creepy. Oh, and with an ad blocker, you won't have to sit through YouTube ads! I'll wait a moment while you turn on your pop-up blocker (search your settings for "pop-up") and install an ad blocker (here is the extension for Chrome; here is the extension for Firefox; it's free—if they ask you to pay, you can, but you don't have to)
64. **Clear your cookies** every so often (every week at least). Cookies are these little files that get installed on your computer every time you visit a website – so those websites can TRACK you. Just search your browser settings for "cookie" to clear them
65. Go back to your Salesforce page. Is your connection secure? Just go to the top left corner, next to the URL – if you see a lock icon, you have a **secure SSL connection**, they call it. If you are on a website and you do **not** see this lock— —be careful—and do **not** enter any sensitive information like your credit card #!
66. If you just want all these settings above without too much effort, you got 2 options. First, use **incognito or private** browsing. Just go to the top right corner of your browser, click the 3 dots or lines depending on your browser, and choose **new incognito** (or **private** window). A second option, use the Brave web browser – it has all these settings built in!

Remember how our computers only read those 0s and 1s – the bits? Well, encryption is great because it actually scrambles those bits like an egg, so hackers can't read the bits. If you are ever on public wi-fi, log into a **Virtual Private Network (VPN)** first. VPN encrypts all those bits – Prof said she will even do banking on public Wi-fi with VPN, but NEVER without VPN. My school gave me a free VPN, but you can use a public one like Surfshark or Proton.

LAST thing, I promise, before I end this assignment. Click LIKE if you are on social media. Jk, there is no LIKE button on this blog…that was just another thing I've always wanted to say. But make sure you go check your **social media privacy settings** – turn on MFA, lock down your **privacy settings** so future employers cannot see your photos, and stuff like that. Heck, I don't want my current employer to see me – I had a friend get fired for some stupid video she posted on YouTube. Oh, and if you don't know a person friending you, do NOT accept their request! Those strangers will probably just try to social engineer you.

All this info might seem overwhelming (trust me, it was for me when I first learned it) and Im not trying to turn you into one of those super paranoid tin foil hat people! Just trying to help you guys be more aware of all the ways you can keep you and all your tech stuff safe (in a not over the top crazy person way).

Alright, that's all I got for this one, this new cyber hygiene wizard is signing off…btw, what did the hacker's out of office message say?

Gone phishing. ;)

(and don't forget to get your credit)

Appendix C. Cyber Hygiene Module Assessment and Discussion Suggestions

Assessment and Adding to a Learning Management System (LMS)

For students to receive credit for the module, we provide the following instructions:

To receive your credit, take the following TWO screenshots and submit them on Canvas (LMS). You may paste the screenshots into a Word document, or you can just upload the image files individually—up to you. The third item below includes a brief reflection.

1. Is your firewall running? Take a screenshot of your firewall. If you don't know what it is, I cannot help you, because you went through the steps earlier!
2. Take a screenshot of your antivirus software showing that it is ON. I do not care if it is the built-in antivirus or a third-party. Again, you should know how to find this!
3. Write a brief reflection (a few paragraphs) that includes the following:
    a. Was your cyber hygiene good or bad prior to this module? Explain and be specific.
    b. What are three interesting things you learned in this module?
    c. In what ways will you improve your cyber hygiene?

Possible Discussion Questions

Instructors can use this follow-up discussion to the cyber hygiene module either in person or virtually. In an asynchronous online course, instructors may easily convert this to a discussion activity. For in-class discussions, we suggest putting students in small groups, then sharing with the entire class (like a think-pair-share activity). Feel free to use any or all of these questions, or modify the questions to fit your needs. If you would like to receive some suggested answers, please contact the corresponding author.

Answer the following questions regarding cyber hygiene topics, which are based on the module learning objectives:

1. In your own words, describe cyber hygiene.
2. Let's presume you currently use—or will begin using—strong and long passwords, and you will not use the same password on more than one app/website. How can you manage this?
    a. Consider showing students how your password manager works (e.g., auto-login to websites, vault, etc.).
    b. Follow-ups:
        i. How are password managers more secure than storing via web browser?
        ii. What is MFA?
        iii. What apps are available for password storage and MFA? Have you used them? What do you like/dislike about them?
3. What are best practices for identifying phishing messages? Has ChatGPT changed how we identify phishing messages?
    a. Consider showing students examples (found online, or in your own Junk folder).
    b. Emphasize that ChatGPT and other generative AI has improved the quality of phishing messages, requiring students to be more diligent.
4. What antivirus and firewall are running on your computer?
    a. Follow-ups: What is the purpose of antivirus? Firewall? Why is it smart to use a 3rd party antivirus/firewall in addition to the built-in operating system software?
5. Why is it important to update ALL applications and your operating system, both on your computer and phone?
    a. Follow-up: Keeping software updated is extremely important for your antivirus and firewall software, right? Why?
6. What are the benefits of backing up your files, both at an individual level and for an organization? List and describe at least three benefits.
7. Have you assessed your social media connections since this module? Will you be more aware of this danger in the future?
    a. Follow-up: If a stranger looks at your Facebook page, what will they see?
8. List and describe three ways your cyber hygiene behaviors have (or will) change since doing the cyber hygiene module. If you will not change any behaviors, why not?
9. Describe a cyber hygiene issue that you have personally been a victim of. If you cannot think of one, share the story of a friend/relative. Be specific (what happened, how you recovered from it, what type of violation it was, etc.).
    a. Did you or this other person recover? How? How long did it take?
    b. Note: We find that students relate to these stories. While these seem like "scare tactics," some of those tactics are successful.

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS

iscap

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)