Establishing the Sociology and Cybersecurity Nexus Through Experiential Learning: Cybersecurity Innovation on a HBCU Campus

Carlene Buchanan Turner **Norfolk State University**
Claude Turner **Norfolk State University**
Austin Ashe **Norfolk State University**

This article examines the integration of cybersecurity into the sociology curriculum at a HBCU. The article is based on two of the twenty-six modules that were created and taught in a three-year project. The research questions are:

- *Is there increased cybersecurity awareness after the infusion of the Password and Phishing Modules?*
- *Is there a relationship between the use of experiential pedagogy and learning outcomes?*

The socio-cybersecurity modules are grounded in Vygotsky's experiential learning theory.

The methodology included a pre-test survey of cybersecurity awareness, the module's lecture and experiential activities, then a post-test survey of cybersecurity awareness. T-test analysis was performed on the data obtained from quasi-experimental survey data. Content analysis was performed on in-class assignments. Students found the experiential pedagogy helpful and demonstrated their new knowledge. Significant pedagogical research is occurring with African American students. Traditionally, this population has been sidelined in the digital race and its new employment opportunities. When exposed to cyber-education their learning outcomes are primarily significant.

Keywords: *experiential pedagogy, HBCUs, socio-cybersecurity, passwords, phishing*

INTRODUCTION

The discipline of sociology has long accepted the mandate to be the contemporaneous science of society, while at the same time honoring its classical canon. Socio-cybersecurity research and pedagogical thrust honor both these traditions. This article reports on the empirical results from efforts to integrate cybersecurity into the sociology curriculum at a historically Black college and university (HBCU) utilizing experiential learning pedagogy. The research questions that will be addressed in this article therefore are:

- Is there increased cybersecurity awareness in two cohorts of Social Problem students after the integration of a Password Module and a Phishing Module into their curricula?
- Is there a relationship between the use of experiential pedagogy to teach African American students socio-cybersecurity and their learning outcomes?

Socio-cybersecurity can be defined as the socio-cultural aspects of cybersecurity. Within the emerging discourse there is a focus on the accompanying social problems of online connectivity, the socio-psychological implications particularly for criminal justice, its role in modern bureaucracies and institutions, and the position of big data and research methodology. There are limited justifications in the literature for teaching socio-cybersecurity as a sub-field in the sociology discipline (Buchanan Turner & Turner, 2019; Finnemore & Hollis, 2016; Turner & Turner, 2017;).

This research is based on work supported by the National Science Foundation under Grant No. 1623201 and Grant No. 1807164.

A sociological lens is appropriate in understanding the position of different groups in both shaping and responding to cybersecurity. Information assurance vulnerabilities can have social explanations. Odlyzko (2003) stated that computer and Internet systems are only as secure as their weakest link; and in most scenarios the most vulnerable links are people.

The cybersecurity and sociological nexus is increasingly being formalized in the academy because of the importance of the non-technical aspects of information assurance (Spidalieri & McArdle, 2016). It has been argued that a technology-centric focus is insufficient in thwarting future cyberthreats. The political data mining firm Cambridge Analytica successfully merged cyber informatics with socio-cultural norms in 2016 and had a significant impact on the United States presidential election (Hern, 2018). These are justification for introducing a HBCU population to the emerging field of socio-cybersecurity.

Although minority representation within the cybersecurity field exceeds the overall United States minority workforce, continuing disparities persist. Accordingly, only twenty three percent of minority cybersecurity professionals serve the role of director or above according to the Frost and Sullivan white paper (Reed & Acosta-Rubio, 2019). Information from the Bureau of Labor Statistics details a more problematic position with diversity, as in 2016 74% of information security employees were White Americans, 12.5% were African Americans, and 7.9% were Asian Americans (Pals, 2019). Additionally, people of color, employed as cybersecurity professionals, on average earned less than their white counterparts (Reed & Acosta-Rubio, 2019). A career in cybersecurity begins with an educational foundation that provides foundational knowledge. Therefore, this research is appropriately positioned to fill existing voids by evaluating efforts to integrate cybersecurity into the sociological curriculum at a HBCU.

The research conducted for this article evolved from a curriculum development project to integrate cybersecurity into the sociology and criminal justice programs at an HBCU. The discourse being created by these curriculum development efforts should help us understand the role of cybersecurity in sociology and to recognize best-practices instructors use to deliver the content.

BACKGROUND

Theoretical Framework

The students targeted by this project are learning by doing; constructivist theorists recognize that experience is the root of, and stimulus for, learning (Jarvis, Holford, & Griffin, 2012). The curriculum development efforts being analyzed in this article are guided by the social constructivism learning theory. Vygotsky's social constructivism theory of learning reinforces the value of the students' experiences and their social contexts in the learning process (Prawat, 2002). Vygotsky (1997) defined education as "the artificial mastery of natural processes of development" (p. 87), so the premise of this research is that experiential pedagogy mimics the taken for granted process of learning. The theory is relevant to this project as cybersecurity paradigms and praxis can be seen as parts of the new knowledge society. Teaching cybersecurity to non-computer science students may require universities to re-configure the foci of learning to include an interdisciplinary thrust. This includes experiential learning that brings together instructors from computer sciences and sociology, to effectively teach their Black students. The modules were built are hands-on activities from the students' reality. Vygotsky's social constructivism of learning theory supports the pedagogical thrust of the socio-cybersecurity project because the modules were created and taught with experiential techniques. The goal of the project was to create modules that allowed students to experience cybersecurity by doing hands-on activities or engaging in discussions.

The Vygotsky constructivist pedagogy has four important components. First, Figure 1 points to how these African American students encounter the socio-cybersecurity modules with prior knowledge about the Internet. Second, learning occurs in a social context. The identity of the learner from the specific (their academic major) to the macro (their race and ethnicity) is thus seen as important in the learning process. Third, experiential (hands-on or active learning) can lead to development, that is, learning. Therefore, creating a phishing game or creating your own passphrases can lead to development. Finally, language is important in this type of pedagogy. These social science students have to integrate the cybersecurity terms into their social problem assignments. The totality of this framework was appropriate to the team's approach to teaching the modules. The students were therefore required to socially construct what it means to operate in a cyber-safe environment through actual and simulated experiences from the laboratory modules.

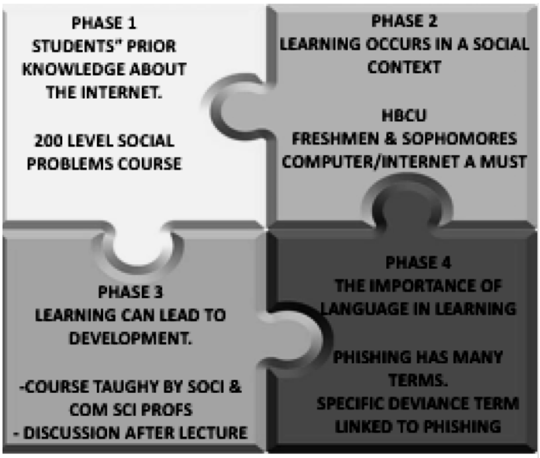

PHASE 1
STUDENTS" PRIOR KNOWLEDGE ABOUT THE INTERNET.
200 LEVEL SOCIAL PROBLEMS COURSE
PHASE 2
LEARNING OCCURS IN A SOCIAL CONTEXT
HBCU
FRESHMEN & SOPHOMORES
COMPUTER/INTERNET A MUST
PHASE 3
LEARNING CAN LEAD TO DEVELOPMENT.
-COURSE TAUGHY BY SOCI & COM SCI PROFS
- DISCUSSION AFTER LECTURE
PHASE 4
THE IMPORTANCE OF LANGUAGE IN LEARNING
PHISHING HAS MANY TERMS.
SPECIFIC DEVIANCE TERM LINKED TO PHISHING

Figure 1. Constructivism Learning Theory for socio-cybersecurity.

The theoretical choices for this project are predicated on the belief that experiential learning is a pivotal part of how human beings learn (Manolis et al., 2013). Each of the module created in the project are required to have a hands-on or laboratory component that can be used to reinforce the concepts being taught. Although the social construction of learning was derived from the field of sociology, sociologists have not used experiential and active learning in the classroom as much as physical and natural scientists. Korgen & Atkinson (2018) point out in their new textbook that active learning allows students to *do* sociology through real-world activities designed to increase learning, retention, and engagement with course material.

Literature Review

The existing literature supports the use of modules to integrate new concepts into a school's or college's existing curriculum (Gardener, 1973; Holmes, 2006). Additionally, the use of modules as instructional resources seems to occur more seamlessly in the physical and computational sciences, more-so than in the social sciences (Nye & Thigpin, 1993; Varma, 2008). The discourse in the literature supports the practice of instructors broadening the teaching of science by enriching the syllabus with interdisciplinary modules. Varma (2008) reviewed teachers' implementation of short inquiry modules like those in our project. The modules featured scientific visualization which can be compared to the laboratory experiential component. The results from their project demonstrated that experiential modules can be difficult to implement at first, but with persistence can reveal positive results. In terms of interdisciplinary modules, Gardener (1973), argued that to be successful such efforts should allow for the appeal to a large general audience of students who need a citizen's complement of science. At the same time it is best if the modules are topical, more investigative, student-centered, enjoyable, flexible, and more integrated than science courses.

The socio-cybersecurity curriculum development process was driven by "the Security Injection Module Framework" (Turner, Taylor, & Kaza, 2011). The adoption of this framework was based on the existing literature and research around cybersecurity pedagogy. The framework has five sections: (1) Identification of the Relevant Topics; (2) Module Background; (3) Security Checklist; (4) Lecture and/or Laboratory exercise with short videos; and (5) Discussion Questions (Turner et al., 2011).

The literature also promotes an interactive process for module development which was adopted in the current project (Cavanaugh & Dawson, 2010). In this process, after the modules were piloted, assessed or evaluated, they were then improved based on feedback from all participants (instructors, students and evaluators) before re-integration. Best practices in module development confirms that it is appropriate to conduct a review of the first set of modules (or piloted modules). In their development of science teaching modules for secondary teachers, Cavanaugh and Dawson (2010) called this step the 'accessibility review.'

These meticulous steps are necessary as Black researchers and professors attempt to carve out a niche in the cybersecurity discipline. As suggested in phase 2 of Vygotsky's theoretical framework, learning occurs in a social context. The U.S. Census reported that as participants in the contemporary digital revolution, between 2013 to 2017, 72.4% of African Americans had access to an Internet subscription (U.S. Census, 2019). This demonstrates that most of the students at HBCUs, even outside of computer science disciplines, need to be more Internet savvy and cybersecurity aware because of the access they have. Consistent with the assertion made by Toldson (2015), HBCUs can successfully prepare their students for postgraduate studies if students are challenged with opportunities like the project being analyzed in this article. This project introduces non-computer science students to cybersecurity through innovative pedagogy because the focus is on building up African American students, not weeding them out (Toldson, 2015).

METHODOLOGY

A two-phase methodology was used to assess the outcomes of the integration of the Phishing and the Password Modules into the Social Problems course. First there were data analysis based on in-class surveys collected through a quasi-experimental framework, and secondly the assessment of the students' laboratory assignments based on the modules. Paired *t*-test analysis was used to compare the indicators' means before and after the module infusion. All the students registered and attending the two sections of the Social Problems courses were the target population for the socio-cybersecurity pedagogical infusion.

Social Problems, the course that was treated in this analysis, is a required course for all sociology majors at Norfolk State University (NSU). The two cybersecurity modules under analysis (a) Password with Rational Choice Theory Module and (b) Phishing and Deviance Module were taught to different cohorts of students. The Password module has been taught in since Spring 2017. Its infusion deliberately followed the chapter on national security issues in the Social Problems curriculum. The title of the module was *Creating Strong Passwords: A Simple National Security Tool.* This module was grounded in Gary Becker's Rational Choice Theory (1988). Each deployment of the module was co-taught by a computer science professor and a sociology professor. All involved professors were Black.

The Phishing and Deviance Module has been taught in the same course since Fall 2017. It is grounded in labeling and strain deviance theories. The module was created and co-taught by a team of computer science and sociology professors; again these professors were Black. The nature of this module makes it a good fit for courses beyond sociology and criminal justice because cybersecurity practices have sociocultural and criminological components.

The Pre- and Post-Test Surveys

The primary methodology that facilitated the evaluation of the module infusion was a quasi-experimental process based on the population of NSU students who were enrolled in the targeted sections of the course. This was based on a one-sample before-and-after quasi experiment design, as the averages of the indicators were measured in a time ordered manner (Schutt, 2019). Each students' response was matched from the pre-test to the post-test. Pre-tests surveys were conducted in the course via the Blackboard Learning Management System (https://help.blackboard.com/Learn/Instructor/Original/Tests_Pools_Surveys/Create_Tests_and_Surveys). The questionnaires captured the concepts taught in the modules. For each module, identical questions appeared on both the pre- and post-test instruments. The Password questionnaire had thirteen items, with four demographic questions, eight password content questions and one pedagogy question. The twelve-item Phishing questionnaire had the same demographic questions, as well as seven phishing questions, and one pedagogy question. The Phishing Module for this analysis was taught in Fall 2018 and the Password Module was taught in Spring 2019.

The mean differences statistical significance was ascertained utilizing the *t*-test analysis with the following hypotheses:

> *H_{1a}: There is no difference in the means of the Phishing Indicators across the pre- and post-test conditions.*
> *H_{1b}: There is no difference in the means of the perception of the helpfulness of the Phishing Lab across the pre- and post-test responses.*
>
> *H_{2a}: There is no difference in the means of the Password Indicators across the pre- and post-test responses.*
> *H_{2b}: There is no difference in the means of the perception of the helpfulness of the Password Lab across the pre- and post-test responses.*

The dependent variable from H_{1a}, Phishing Indicators, was operationalized by seven concepts taught in the module, which were (a) knowing what phishing is, (b) when to open an e-mail attachment, (c) sender to trust, (d) where are scammers from, (e) scammers' personality, (f) scammer's social network, and (g) number of suspicious e-mails received (see Table 1). All of these were ordinal, Likert questions posed from most to the least desirable choice as taught in the modules and practiced in the hands-on exercises.

Table 1

Comparative Descriptive Statistics for Phishing Variables – Social Problems Class – Fall 2018

	Before/After Module Infusion			
VARIABLES	***Pre-Test Condition (N=33)***		***Post Test Condition (N=30)***	
Gender	Female	81.3%	Female	82.1%
Classification	Junior	51.5%	Junior	50.0%
Major	Sociology	45.5%	Sociology	46.4%
Concentration	Criminal Justice	45.0%	Criminal Justice	52.9%
Know Phishing	Yes	69.7%	Yes	100%
Opening Attachment	Expecting Email	48.5%	Expecting Email	78.6%
Sender from USA or Not	Both	84.3%	Both	75.0%
Scammer Location Concern	USA or Not	84.8%	USA or Not	75.0%
Most Scammers Are	Just Greedy	42.4%	Just Greedy	46.4%
Scammers Work	In Groups	45.5%	In Groups	46.4%
Suspicous E-mails Monthly	3-4	43.8%	3-4	28.6%
Completed Phishing Lab	Yes	21.2%	Yes	85.7%
Lab Helpful	Very Much	18.2%	Very Much	75.0%

For H_{2a}, the main dependent variable was Password Indicators. It was operationalized by eight concepts taught in the module as follows: appropriate password length; should passwords be memorable; should passwords have special characters; how often should passwords be changed; what password rules should national security agencies have; can weak passwords compromise America's national security; does the USA experience a lot of cyber-attacks; and is your everyday password secure (see Table 2 for further details). The students were taught all the concepts during the module infusion and practiced them in the laboratory exercises (Choong et al., 2014). In the pre- and post-test questionnaire, the students were presented with options, from most to least desirable, which formed the basis of the analysis.

Table 2

Comparative Descriptive Statistics for Password Variables – Social Problems Class – Spring 2019

	Before/After Module Infusion			
VARIABLES	***Pre-Test Condition (N=17)***		***Post Test Condition (N=13)***	
Gender	Female	64.7%	Female	61.5%
Classification	Junior	47.1%	Junior	53.8%
Major	Sociology	82.4%	Sociology	76.9%
Concentration	Criminal Justice	78.6%	Criminal Justice	72.7%
PassWordLength	At Least 8 Characters	82.4%	At Least 8 Characters	100%
Should be Memorable	Strongly Agree	88.2%	Strongly Agree	100%
Should Have SpcialCharac	Sometimes	52.9%	Always	69.2%
TimetoChange	Every 6 Months	41.2%	Every 3 Months	76.9%
NatSecurity Have Rules	I'm Sure They Do	82.4%	I'm Sure They Do	76.9%
Weak PW Can Compromise	Yes	70.6%	Yes	100%
USA AttackedaLot	Yes	88.2%	Yes	76.9%
Your EvrydyPsswrd	Secure /Somewhat	41.2%each	Secure/Very	30.8%/each
Completed PW Lab	No	82.4%	Yes	92.3%
Lab Helpful	Very Much	17.6%	Very Much	92.3%

For H_{1b} and H_{2b}, the dependent variable was helpfulness of the modules. This was an ordinal question that captured students' self-perceived learning outcome. The four-point scale ranged from not at all helpful to very helpful. This is the main measure of students' outcome in this analysis and was supplemented with the results from the hands-on activities.

Qualitative Data Collection

The qualitative methodology was the secondary research technique used in this article. For the Phishing Module, the students played the interactive 'Anti-Phishing Phil Game' and at the conclusion submitted written discussions on how the obstacles in the game impacted their cybersecurity awareness (CUPS, n.d.). This helps to support or refute H_{1a} which looks at change in understanding phishing because of the treatment. The students responded to questions after the game about what they had learned about phishing, and students were prompted to identify sites set up by 'white-hat' and 'black-hat' hackers. For definitional purposes, cybersecurity specialists define white-hats as ethical hackers who are employed by organizations to finding vulnerabilities in their system. Conversely, black-hats are unethical hackers who illicitly intercept online content (Kremling & Sharp Parker, 2018).

For the Password Module, the students were instructed to use the password creation and management rules to create their own passphrases as a small group exercise (Pham, 2017). The groups presented their passphrases to the class, and fellow students determined if the creation rules were followed. Written discussions also described the usefulness of the creation exercise.

RESULTS

Descriptive Statistics

In examining the descriptive statistics for the Phishing and Social Deviance Module, Table 1 demonstrates the demographic parameters of the students who were treated to the module integration, as well as the differences in their answers on seven indicators across the pre and post-test conditions. There were two other items that directly measured the impact of the experiential pedagogy. This module was offered in the Social Problems course in Fall 2018. Thirty-three students participated in the pre-test survey, while only thirty completed the post-test survey. All the students in this section of the course identified as Black/African American. Most of the subjects were female (81.3% pre-test, 82.1% post-test). Although this was a 200-level course, approximately one-half of the students reported their classification as juniors (51.5% pre-test: 50.0% post-test). In terms of the indicators, there was a 29.3 percentage point increase in students who knew what phishing was in the post-test (100%), over the pre-test condition (69.7%). While 48.5% of the respondents said it was appropriate in the pre-test condition to open an expected e-mail attachment from a known person compared to an increased percentage (78.6%) in the post-test condition.

In both the pre- and post-test conditions, the respondents were likely to say that they were suspicious of stranger e-mails whether they were from the U.S. or another country (84.8% versus 75.0%). When asked to connect deviance typology to cybersecurity, in the pre-test condition 42.4% of scammers were described as just greedy, while it was almost the same (46.4%) in the post-test condition. In both the pre- and the post-tests, students said that scammers primarily worked in groups, in similar proportions (45.5% and 46.4% respectively). As evidence of everyday phishing, in the pre-test condition 43.8% of the students believed they get about 3 to 4 suspicious e-mails monthly, while 28.6% said the same in the post-test.

In terms of the experiential pedagogy indicators, only 18.2% of the in the pre-test said the particular phishing lab helped 'very much,' compared to 75% in the post-test, which is a 57-percentage point difference.

Table 2 demonstrates the characteristics of the students, and the comparative responses to the password items. While 17 students participated in the pre-test, there were four less participants in the post-test. The students in this section of the course all identified as Black/African American. In terms of the respondents' demographics across the pre- and post-test conditions females accounted for 64.7% and 61.5% of the sample respectively; junior was the modal classification (47.1% and 53.8% respectively); more than three-quarters of the respondents were sociology majors (82.4% and 76.9% respectively); and two-thirds of the students identified criminal justice as their concentration (78.6% and 72.7% respectively).

In examining the descriptive statistics for the password content questions, Table 2 demonstrates that the infusion of the module into the Social problem class impacted student learning. There was a 17.6% jump in students who believed that passwords should be at least eight characters long. There was a 11.8% increase in the number of the students who strongly agreed that passwords should be memorable. However, 52.9% of the students said that passwords should have special characteristics 'sometimes' compared to 69.2% who said 'always' after they were taught the module. In the post-test condition, more students indicated that passwords should be changed every three months, rather than every six months. About the same number of students agreed that national security agencies had strong password protocols. There was a 30% increase in the opinion that weak passwords can compromise national security. There was about an 11% decrease in the opinion that the U.S.'s cybersecurity infrastructure has been attacked quite frequently. A combined 82.4% of the students said passwords were secure or somewhat secure in the pre-test, compared to 61.6% who said it was secure and very secure in the post-test.

The assessment of the experiential pedagogy for the last items in Table 2 demonstrates most students (92.3%) said this password lab was very helpful, compared to 17.6% of the respondents who indicated the same in the pre-test.

T-Test Analysis

The impact of the socio-cybersecurity Phishing Module was analyzed through mean difference comparison utilizing the paired *t*-test technique. The analysis was predicated on the following hypotheses:

H_{1a}: There is no difference in the means of the Phishing indicators across the pre- and post-test conditions.

While not conclusive, the paired *t*-test results demonstrated that the infusion of the Phishing Module into the Social Problem class impacted student' learning outcomes for two out of seven concepts (see Table 3). While there were 33 students in the analysis, only 24 students answered both the pre- and post-test for the valid matched pairs. The first significant indicator was "Do you know what phishing is?" The before module condition was (M = 1.33, SD = .565) and after module condition was (M = 1.00, SD = .00); $t(23)$ = 2.892, p = 0.008. "Care taken in opening e mail attachment” was the second significant indicator. Pre-test condition (*M* = 1.60, *SD* =. 500) and after module condition (*M* = 1.20, *SD* = .408); *t*(24) = 3.098, *p* = 0.005.

Table 3

T-Test Results for Phishing Indicators Taught in Social Problems Class Spring 2019, N = 13

	Pretest		**Posttest**		**95% CI for Mean**			**Sig (2-tailed)**
Outcome	***M***	***SD***	***M***	***SD***	**Difference**	***t***	***df***	
Know Phishing	1.33	.565	1.00	.000	.095, .572	2.892	23	.008*
Opening Attachment	1.60	.500	1.20	.408	.134, .666	3.098	24	.005*
Sender from USA or Not	2.20	1.41	2.68	1.46	-1.26, .302	-1.27	24	.218
Scammer Location Concern	3.04	.539	3.00	.646	-.239 .319	.296	24	.770
Most Scammers Are	2.16	1.07	1.88	.881	-.158, 718	1.32	24	.200
Scammers Work	2.28	.842	2.08	.843	-.262, .662	.894	24	.380
Suspicious E-mails Monthly	1.58	.929	1.67	.963	-.495, .328	-.419	23	.679
Lab Helpful	3.72	1.57	1.40	1.00	1.48, 3.16	5.70	24	.000*

H$_{1b}$: There is no difference in the means of the perception of the helpfulness of the Phishing Lab across the pre- and post-test responses.

The second phishing hypothesis analyzed experiential pedagogical efforts used to teach the modules. The item asking whether the phishing lab was helpful was statistically significant. The results were (*M* = 3.72, *SD* = .157) for the pre-test condition and (*M* = 1.40, *SD* = 1.00); *t*(24) = 5.70, *p* = 0.000 for the after module condition.

The Password Module taught in Spring 2019, was also analyzed using identical techniques. Two hypotheses were analyzed based on the data from the quasi-experiment using a paired *t*-test. While there were 17 students in the analysis, only 12 students answered both the pre- and post-test for the valid matched pairs. The first hypothesis was:

H$_{2a}$: There is no difference in the means of the Password indicators across the pre- and post-test responses.

Two of the eight password indicators from the module, had statistically significant mean differences across the pre- and post-test conditions (see Table 4). ‘Passwords should have special characters’ was the first significant predictor; the answer choice for this item ranged from Never to Always. The before module condition was (*M* = 2.62, *SD* = .870) and after the module taught it was (*M* = 3.46, *SD* = .877); *t*(12) = -3.09, *p* = 0.009. The second significant password indicator was ‘How often should you change your password,’ and the variable had four values as indicated in Table 2. The results were (*M* = 2.31, *SD* = 1.11) for the pre-test condition and (*M* = 1.38, *SD* = .870); *t*(12) = 2.80, *p* = 0.016 for the after module condition.

Table 4

T-Test Results for Password Indicators Taught in Social Problems Class Spring 2019, N = 13

	Pretest		**Posttest**		**95% CI for Mean Difference**			**Sig (2-tailed)**
Outcome	***M***	***SD***	***M***	***SD***		***t***	***df***	
PassWordLength	2.77	.439	3.00	.000	-.496, .034	-1.90	12	.082
Should be Memorable	1.08	.277	1.00	.000	-.091, .245	1.00	12	.337
Should Have SpcialCharac	2.62	.870	3.46	.877	-1.44, -.250	-3.09	12	.009*
TimetoChange	2.31	1.11	1.38	.870	-.205, 1.64	2.80	12	.016*
NatSecurity Have Rules	1.31	.630	1.46	.967	-.750, .442	-.562	12	.584
Weak PW Can Compromise	1.54	.877	1.15	.555	-.079, .848	1.81	12	.096
USA AttackedaLot	1.15	.555	1.38	.768	-.593, .131	-1.39	12	.190
Your EvrydyPsswrd	2.77	1.17	2.38	1.39	-1.41, .910	1.59	12	.137
Lab Helpful	3.31	1.65	1.08	.277	1.18, 3.28	4.62	12	.001*

H_{2b}: There is no difference in the means of the perception of the helpfulness of the Password Lab across the pre- and post-test responses.

The indicator that was used to measure the impact of the experiential pedagogy in teaching the Password module were statistically significant. The question asking if the Password module was helpful, was statistically significant. The before module condition was (*M* = 2.21, *SD* = 1.65 and after module condition (*M* = 1.08, *SD* = .277); *t*(12) = 4.62, *p* = 0.001.

Content Analysis—Interactive Phishing Game and Passphrase Creation

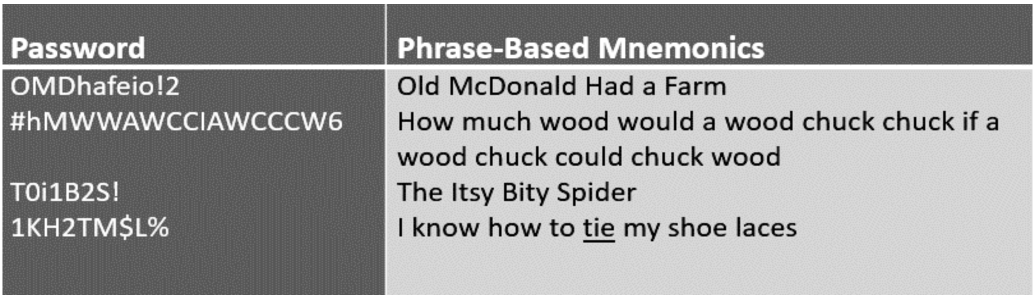
The surveys for the Phishing Module were also supplemented by an interactive game (CUPS, n.d.) and content analysis was used to catalog the student's written answers. Some of the common sentiments from the students were:

> "The game helped me to be more alert about certain sites."
> "The Anti-Phishing Phil games has helped me to better understand how many tricky ways that are to get caught up into the madness of phishing."
> "Another thing that caught my eye was a lot of banking sites and the msn website with the word verify in it as I didn't know that would be a scam site."

Common themes from the students' written discussion demonstrates that they believed the modules had a positive impact. They used phrases such as 'made me more alert,' 'helped me to better understand,' and pointed out that before the lesson they 'didn't know that would be a scam site,' which all illustrate a change in perception. The experiential learning activity after the lecture allowed students to successfully identify illicit versus genuine sites.

The quasi experiment surveys for the Password Module was supplemented by students creating passphrases in groups, and then discussion of the implications. All four groups successfully created passwords that conformed to the password rules taught in the lab. These were: choose a memorable phrase; pull the first letter of main words; include numbers; special characteristics; upper and lower-case letters; and they should not simply be dictionary words (Choong, Theofanos, & Liu, 2014).

The students used information from their environment to create the required passphrases (see Figure 2). This was a collaborative process as they had to take suggestions from all members of the group. Through inter-group evaluations, led by the instructors, the students determined that all of the passphrases used the creation rules, indicating that learning occurred because of the module's instruction.



Password	Phrase-Based Mnemonics
OMDhafeio!2	Old McDonald Had a Farm
#hMWWAWCCIAWCCCW6	How much wood would a wood chuck chuck if a wood chuck could chuck wood
T0i1B2S!	The Itsy Bity Spider
1KH2TM$L%	I know how to tie my shoe laces

Figure 2. Students' password created from the module's lab–Social Problems, Spring 2019.

Discussion

The findings presented in this study, captures the outcomes from integrating cybersecurity into a core sociology course over two semesters. Two distinct modules were integrated, Password with Rational Choice Theory and Phishing with Deviance Theory, and both had positive learning outcomes on the targeted students. The analysis revealed that the experiential pedagogical theory utilized in this project was an appropriate frame to guide the integration of the modules in the two class sessions. The first phase of the Vygotsky constructivist learning theory focuses on prior knowledge. The results from both the phishing and password integration demonstrate that most of the students had not experienced a laboratory session with these concepts before. Of interest is phase 3 of the theory which says that learning can and should lead to cognitive change or development. The question from the *t*-test that responds to this is how helpful the phishing and password labs. This learning outcome demonstrates a positive cognitive development as for both modules, the question 'was the lab helpful' was statistically significant (Phishing Module—75% Very Much; Password Module—92.3% Very Much).

The utilization of the Security Injection Framework to construct and teach the modules was also related to positives learning outcomes (Cyber4All, 2017; Saltzer & Schroder, 1975; Taylor & Azadegan, 2007a, b; Turner & Turner ,2017). This was an innovative pedagogy for sociology and criminal justice courses, which are primarily lecture-based. The focal point of the modules was the hands-on activities in the sessions. The excerpts from the Phishing Module discussion and Figure 5 demonstrate some of the outcomes from the laboratory exercises. Students expressed that the phishing activity resulted in developing new knowledge. For example, *"The Anti-Phishing Phil games has helped me to better understand how many tricky ways that are to get caught up into the madness of phishing."* Similarly, students internalized the concepts of appropriate password creation (Choong et al., 2014) and this is illustrated by the passphrases they created (for example one passphrase, T0i1B2S!–The Itsy Bity Spider). These are positive outcomes for the impact of the modules on the students' cybersecurity awareness.

The positioning of this educational research effort at an HBCU, while being taught to African American students by Black professors, is a critical social context for this project (phase 2 of the Constructivism Learning Theory for Socio-Cybersecurity). The proposed broader impact of the National Science Foundation project is to increase the participation of this population in cybersecurity market by not weeding out African American students before they can even apply for a job (Toldson, 2015). This means that even non-technical students can learn the language of cybersecurity and apply its concepts as productive citizens (phase 3 of the theory). African Americans currently have access to the digital world, even though it is less than White Americans (Internet subscriptions 72.4% and 83.5% respectively (U.S. Census, 2019). Training students at HBCUs in cybersecurity will ensure that minority participation and tangible job prospects is accessible to these graduates (Pals, 2019).

CONCLUSION

The future of the emerging sub-discipline of socio-cybersecurity is rooted both in curriculum development and faculty research interests. Going forward, universities could invest in faculty development efforts to train instructors how to integrate cybersecurity into non-computer science courses. Based on the current findings, this training should be grounded in experiential pedagogy. The Security Injection Framework with active learning is associated with strong, positive student outcomes. Based on the post-test surveys, the students became more proficient in the cybersecurity language, which, Vygotsky (1997) said, leads to development and learning. Projects such as these can prepare students within the HBCU social context who are ready to take their skill set into an increasingly online world.

Faculty development could be centered around training faculty to create experiential, interdisciplinary cybersecurity modules. HBCUs could be at the forefront of this academic pursuit as many other institutions may see a non-technical approach to cybersecurity as non-traditional. The primarily African American students at HBCUs could then be infused with a broader view of cybersecurity that can improve their post-graduate employability and their interests in graduate studies.

Additionally, areas of sociology and criminal justice that align more readily with cybersecurity need extensive research to concretize these areas. In addition to deviance and socio-psychological norms such as rational choice, areas such as policing, individuals' rights, organizational theory, and statistical data management can all be expanded into extensive research areas. These research areas, when paired with the appropriate sociological and criminological theories, can advance an interdisciplinary role for cybersecurity in academia. Therefore, these emerging research areas are an indication of myriad ways academics at minority-serving institutions can offer a socio-cultural contribution to the very important field of cybersecurity.

REFERENCES

Buchanan Turner, C., & Turner, C. (2019). Analyzing the impact of experiential pedagogy in teaching socio-cybersecurity: Cybersecurity across the curriculum. *The Journal of Computing Sciences in Colleges, 34*(5), 12-22.

Becker, G. S., & Murphy, K. M. (1988). A theory of rational addiction. *Journal of Political Economy*, *96*(4), 675-700.

Cavanaugh, C., & Dawson, K. (2010). Design of online professional development in science content and pedagogy: A pilot study. *Journal of Science Education and Technology, 19*(5), 438-446.

Choong, Y.-Y., Theofanos, M., & Liu, H.-K. (2014). *United States federal employees' password management behaviors: A Department of Commerce case study.* NISTR. U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7991.pdf

CUPS. (n.d.). *Anti-phishing phil*. (CMU Usable Privacy and Security Laboratory @ Carnegie Mellon University). Retrieved from https://www.ucl.ac.uk/cert/antiphishing/

Cyber4All. (2017). New 'Cyber4All' cybersecurity minor open 4 all undergrads. Retrieved from http://catalog.nec.edu/preview_program.php?catoid=11&poid=1201&returnto=246

Finnemore, M., & Hollis, D. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law, 110*(3), 425-479.

Gardener, M. (1973). Modules and minicourses for integrated science. *The Science Teacher, 40*(2), 31-32.

Hern, A. (2018, May 6). Cambridge Analytica: How did it turn clicks into votes? *The Guardian*. https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Holmes, H. M. (2006). Integrating the learning of mathematics and science using interactive teaching and learning strategies. *Journal of Science Education and Technology, 15*(3), 247-256.

Jarvis, P., Holford, J., & Griffin, C. (2012). *The theory and practice of Learning* (2 ed.). Kogan Page.

Korgen, K. O., & Atkinson, M. P. (2018). *Sociology in action.* SAGE.

Kremling, J., & Sharp Parker, A. M. (2018). *Cyberspace, cybersecurity and cybercrime*. SAGE.

Manolis, C., Burns, D. J., Assudani, R., & Chinta, R. (2013). Assessing experiential learning styles: A methodological reconstruction and validation of the Kolb Learning Style Inventory. *Learning and Individual Differences, 23*, 44-53.

Nye, B. A., & Thigpin, C. G. (1993). Examining the relationship between process-oriented staff development and classroom practices using integrated mathematics and science instructional modules. *Journal of Elementary Science Education, 5*(1), 10-26.

Odlyzko, A. (2003). Economics, psychology and sociology of security. *Financial cryptography.* (2742, pp. 182-189). Springer.

Pals, M. (2019, October 2018). *Securing ethnic diversity in cybersecurity*. Retrieved from https://www.automox.com/blog/securing-ethnic-diversity-in-cybersecurity

Pedagogical_Benefits. (n.d.). *Pedagogical benefits*. The University of Queensland Institute of Teaching and Learning Innovation. http://www.uq.edu.au/teach/video-teach-learn/ped-benefits.html

Pham, T. (2017). NIST update: Passphrases in, Complex passwords out. *CISCO-DUO.* National Institute for Standard and Technology. https://duo.com/blog/nist-update-passphrases-in-complex-passwords-out

Prawat, R. S. (2002). Dewey and Vygotsky viewed through the rearview mirror-and dimly at that. *Educational Researcher, 31*(5), 16-20.

Reed, J., & Acosta-Rubio, J. (2019). *Innovation through inclusion: The multicultural cybersecurity workforce.* (ISC)2. Silicon Valley, Santa Clara: A Frost & Sullivan white paper.

Saltzer, J., & Schroeder, M. (1975). The protection of information in computer systems. *Proceedings of IEEE, 66*, 1278-1308.

Schutt, R. K. (2019*). Investigating the social world: The process and practice of research* (9th ed.). SAGE.

Spidalieri, F., & McArdle, J. (2016). Transforming the next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies. The Cyber Defense Review, 1(1), 141-164.

Taylor, B., & Azadegan, S. (2007a). Teaching security through active learning. *Proceedings of Frontiers in Education: Computer Science and Engineering* (pp. 1-6). Las Vegas.

Taylor, B., & Azadegan, S. (2007b). Using security checklists and scorecards in CS curriculum. *National Colloquium for Information Systems Security Education*, 4-9.

Toldson, I. A. (2015). Weeding out v. building up: Why Justice Scalia was wrong about Black scientists (Editor's Commentary). *The Journal of Negro Education, 84*(4), 517-518.

Turner, C., Taylor, B., & Kaza, S. (2011). *Security in computer literacy.* Proceedings of the 42nd ACM Technical Symposium on Computer Science Education - SIGCSE '11, (p. 15).

Turner, C., & Turner, C. (2017). Integrating cybersecurity into the sociology curriculum: The case of the password module. *Journal of Computing Sciences in Colleges, 33*(1), 109-117.

U.S. Census. (2019). Types of internet subscriptions by selected characteristics 2013-2017. *American Factfinder*. https://www.factfinder.census.gov

Varma, K. H. (2008). Targeted support for using technology-enhanced science inquiry modules. *Journal of Science Education and Technology , 17*(4), 341-356.

Vygotsky, L. S. (1997). Research method. In Rieber, R. Ed.), *Collected works of L. S. Vygotsky: Vol. 4. The history of the development of higher mental functions* (pp. 27-63). Plenum.

AUTHORS

CARLENE BUCHANAN TURNER is Department Chair and Professor of the Sociology Department at Norfolk State University in Norfolk Virginia.
CLAUDE TURNER is Professor in the Department of Computer Science, Norfolk State University.
AUSTIN ASHE is assistant professor in the Department of Sociology at Norfolk State University.

All comments and queries regarding this article should be addressed to cmturner@nsu.edu