UNGUIDED CYBER EDUCATION TECHNIQUES OF THE NON-EXPERT

THESIS

Seth A. Martin, Captain, USAF

AFIT-ENG-MS-19-M-041

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY
Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-19-M-041

UNGUIDED CYBER EDUCATION TECHNIQUES OF THE NON-EXPERT

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Seth A. Martin, BS

Captain, USAF

March 2019

AFIT-ENG-MS-19-M-041

UNGUIDED CYBER EDUCATION TECHNIQUES OF THE NON-EXPERT

Seth A. Martin, BS

Captain, USAF

Committee Membership:

Lieutenant Colonel Mark G. Reith
Chair

Lieutenant Colonel Alan C. Lin
Member

Lieutenant Colonel Eric D. Trias
Member

AFIT-ENG-MS-19-M-041

Abstract

The United States Air Force and Department of Defense relies on its total workforce to provide the first layer of protection against cyber intrusion. Prior research has shown that the workforce is not adequately educated to perform this task. As a result, DoD cybersecurity strategy now includes attempting to improve education and training on cyber-related concepts and technical skills to all users of DoD networks. This thesis describes an experiment designed to understand the broad methods that non-expert users may utilize to educate themselves on how to perform technical tasks. Since education of non-experts on the path toward understanding is the goal of all education, the insights gained by this experiment may lead to further improving education in general for non-experts in any field wishing to gain knowledge through their own efforts. Results from the first stage of the experiment informed subsequent experiments that directly compared frequently utilized, but flawed resources to improved versions of those resources to determine preferable educational methods. This paper provides the protocol and population characteristics for both phases of the experiment, results from phase one, and preliminary results from phase two. In a related effort, the Air Force Institute of Technology is designing and implementing an online learning platform for centralizing a variety of cyber-educational materials. This platform is built-on prior groundbreaking educational research understanding how people, especially young people, learn best in the modern era. This thesis will assist in informing the design of educational platforms, like AFIT's, by providing a unique understanding of how participants search for and select cyber-education on their own, and demonstrating which self-instruction resources are the most and least effective. This is the first experiment of

its kind to combine human subject provided variables, while attempting to statistically measure those human provided variables in the military cyber-education domain.

Acknowledgments

Many people are owed thanks for their support of my research. Lt Col Reith was a tireless advocate for my efforts, ensuring that I got the support I needed from many organizations and people to push through some difficult bureaucratic hurdles. My lack of experience with Python was apparent to 2nd Lt Micah Hayden, without whom I would have spent many weeks getting my test network to properly report and record its status. Capt Marcus Catchpole, 2nd Lt Landon Tomcho, Capt Joshua Mosby, Capt Senobio Chavez, and surely many others made wonderful colleagues whose conversations and critique over many a game and many a beer made all of our research better and more fun. Lastly, my wife for her constant encouragement to press on despite my many roadblocks, while continuing to work full time and pursue her masters simultaneously. I'll never be as dedicated or talented as her, but I'll never stop trying anyway.

Seth A. Martin

Table of Contents

Page

List of Figures

List of Tables

UNGUIDED CYBER EDUCATION TECHNIQUES OF THE NON-EXPERT

I. Introduction

I.1 Importance and Motivation

This thesis investigated educational material modality paths selected by non-expert participants when attempting to complete technical tasks in the absence of formal guidance, specifically in the domain of cybersecurity. We have defined ”non-expert” as not possessing computer related degrees or cybersecurity related certifications or courses. For the purposes of this study, educational modes are ways in which education is consumed. Examples include visual education through video or pictures, audio education through verbal instruction or text, and many others. This study intends to discover which modes and paths should be incentivized and disincentivized on multi-model, modular learning platforms such as the Air Force Institute of Technology’s Cyber Education Hub (www.afit.edu/ceh-learn), Udemy (udemy.com), Kahn Academy (kahnacademy.org), and others. We observe which educational modes and paths participants utilize most frequently, and which modes and paths are most likely to result in successful completion of the task.

The CEH is a platform designed to allow DoD personnel to create, edit, curate, rate, and discuss cyber related educational material in one central location. It is built around the premise that allowing our wide range of users from different backgrounds and experience levels to participate in the improvement of the learning ecosystem will yield

benefits to their productivity and effectiveness. One key aspect of the design of the CEH, is the ability for any user to create and post content without any kind of approval or vetting process. This feature seeks to capitalize on the benefits of rapid updating of cyber related information at the risk of the information being incorrect or, presented in a non-ideal manner. Balancing this benefit against this risk is done more effectively with quantitative measurements of the risk and the benefit. This research seeks to quantify the benefit of this type of open design, without regard to the risk.

By combining our understanding of the risk/reward analysis of rapidly produced content with our improved visibility into the most and least efficient ways to train the workforce to understand cyber concepts sufficiently to play their part in defending the network, we can improve the resiliency of Air Force networks against cyber-attacks that utilize the workforce as their attack vector. The workforce attack vector has been recognized by the cybersecurity as one of the most important defensive vulnerabilities for large-scale organizations. “In order to effectively combat cybersecurity threats at home and in organizations, it is imperative to achieve higher end-user cybersecurity compliance” (Reddy, 2017). For users to comply, they must be taught what to comply with. That training is optimum when it is both effective and quick.

Our research focuses on discovering which of the enormous quantity of resources available for self-teaching technical tasks non-experts demonstrate a preference for, and evaluating the effectiveness of the preferred resources at guiding non-experts

towards completing a task, and completing quickly. This study was partitioned into a pilot phase and a comparison phase. The pilot phase was conducted to narrow the broad universe of educational material pertinent to the provided challenge that the subjects identified and consumed, and to evaluate the usefulness of those materials. Test subjects were given the task without any specified educational material. Each participant pursued educational material in line with their preferences through a provided Internet portal. Researchers then evaluated their effectiveness by way of the participant's success and speed. By giving the participants a technical task to complete, providing access to the Internet, but not any guidance or learning materials, and observing the behavior of the participants, we identified common starting points and key enablers of success for completing the task. By viewing the attempts of each participant to complete the task, we identified four key milestones on the path to success. We then analyzed which specific educational resource was responsible for achieving each successful milestone by each participant. This analysis yielded a specific resource, a vendor specific web guide we have titled Ω, which was responsible for a disproportionate number of successful milestone achievements. Further detailed analysis showed that Ω contained errors owing to being written for an older firmware version that directly caused some users to quit the experiment without success. In the second phase, we modified Ω by updating the instructions it provided to be applicable to the current version of the firmware. The effectiveness of the participants was then evaluated against each other based on the task completion and task duration of the participants in order to measure the effects of updating the educational resource.

This two-step approach was instrumental to developing a better understanding of participant behavior and keys to their success. Without the first phase, the design the second phase of the experiment would have been too dependent on research team hypothesis and predications. After detailed analysis of pilot phase participants, the design of phase two was influenced by behavioral observations that were not foreseen prior to phase one.

I.2 Problem Statement

When asked to perform multi-step, cybersecurity related tasks in the absence of formal training (classes, certifications, degrees) how do non-experts typically pursue the information, and are those pursuit techniques effective in assisting them in completing the task?

I.3 Field of Research Contributions

This research shows, through human trial evidence, the array of resources that non-experts pursue when attempting to complete technical tasks without formal guidance. It further refines this knowledge by measuring the impact to productivity of non-experts by updating a single, authoritative resources within the vast pool of available and accessible educational material. This information can be used to guide science, technology, engineering, and math (STEM) educational processes, as students starting out in those fields are similar to the “non-experts” defined in this study, and non-cyber technical education may have strong parallels to cyber education.

Other applications exist as well. The high-turnover of military produces a persistent demand for training. Those initially entering military service frequently do not have a technical background and would be equivalent in experience to the non-cyber workforce (Dacus, 2018). Additionally, the loss of trained military personal to the private sector often requires the military to look beyond its own walls for effective education and training. This research is therefore pertinent to improving the training used to rapidly utilize an “always new” workforce.

Even experts find themselves frequently in the situation of the non-experts in this experiment. Cybersecurity is one of the most rapidly developing and changing disciplines (Hamby, 2018). New skills are required on at least an annual basis, and rapid teaching techniques with high success rate are similarly necessary for these learning ventures.

Clearly, the need to rapid and effective teaching of technical tasks to those without that knowledge is critical for a variety of situations and applications. While most relevant to this research, cybersecurity education within the military is not alone in its need to overcome these obstacles.

I.4 Research Questions

Consider the following three investigative questions as related to the above problem statement.

i. Investigative Question 1: What educational materials do non-experts seek when attempting to complete a cyber-technical task beyond their knowledge?

Hypothesis: Participants will seek a variety of materials including but not limited to technical manuals, videos, guides, and published instructional materials.

The full range of educational materials available for technical tasks is too voluminous to enumerate. By observing a group of participants, we will identify the materials that participants express a preference for. For data recording, use of educational materials is generalized to the mode of the material (video, web page, manual, etc.) in order to understand usage trends of the participants.

ii. Investigative Question 2: Which educational materials are the most effective in teaching non-experts to complete a technical task beyond their knowledge?

Hypothesis: Participants will be most successful when accessing video guides to complete the task. This would be in line with previous research on similar topics (Fadal, 2008).

Some educational materials are more effective than others. Observing which materials led a participant to rapid, successful completion (measured as completion percentage

and task duration) of the task will identify the most effective materials known to the participants at the time of the trial.

iii. Investigative Question 3: What impact to the participants can be quantified when highly effective available content is further improved?

Hypothesis: The participants will be slightly more likely to complete the task (<10%), and the average completion time will be slightly faster (<10%) than in phase one, but the effects will not be pronounced.

Because we will only be modifying a single resource against a backdrop of thousands of available resources, we suspect that improvement in results will be limited only to participants who both access that resource and who would have been delayed or halted by the errors that previously existed in the resource.

I.5 Methodology

We directed non-expert cyber users to implement a Media Access Control (MAC) address filter on an instrumented test network. We provided no direction or educational material except for the familiarization with the test network, and an open Internet connection. For phase one we observed users and logged the educational material they accessed via the Internet. Analysis of phase one users revealed a single website that was predominately responsible for user success, but was providing guidance for outdated firmware, which prevented some users from succeeding. For phase two, we re-directed all links from that website to a copy of it created by the test team, which provided updated instructions. This allowed us to compare not simply the effectiveness of one set

of instructions to another, but rather we compared the entire Internet-based ecosystem of information containing a single, outdated resource to the entire Internet-based ecosystem of information containing the single, updated resource.

I.6 Assumptions and Limitations

i. Assumptions

The following assumptions were made during the design of the experiment.

1. The participants gave their best effort to the task, resulting in their best abilities to research and complete technical tasks being recorded.

2. The inclusion criteria of the sample are appropriate and therefore, assures that the participants experienced the same or similar levels of difficulty from the task.

3. Participants have a sincere interest in participating in our research and do not any other motives, such as delaying their daily tasks, impressing their job supervisor because they agreed to be in our study, or other unknown motivational drives.

4. The participants were honest in their pre-screening study, and therefore did not have any prior knowledge of the study, the study hardware, or the specific task they were asked to complete. Additionally, test subjects were

honest about their lack of cyber training, certifications, and degrees, and therefore were “non-experts” as defined by this study.

5. The test hardware did not exhibit significant differences between trials, including updating logs and status LEDs, applying router changes, and otherwise operating as intended by the manufacturers and the research team.
6. The participants did not “cheat” by accessing educational material via non-recorded methods during the experiment, or by discussing the task with other future participants after their experimental period was complete.
7. Nearly all test subjects came from within the Air Force Institute Technology. It is reasonable to suspect that they were subject to more exposure to cyber topics and research than the general DoD employee due to the proximity of the Cyber Technical Center of Excellence and the opportunities proximity to that organization provides to AFIT employees such as guest speakers, student presentations, symposiums, etc. It is unlikely that these opportunities specifically covered the research task.
8. Participants in the study selected material that was preferable and more effective for their learning than material they didn’t select. This assumption is similar to the Efficient-Market Hypothesis from economic theory (Fama, 1965), and suffers from similar limitations when viewed with behavioral context of human beings (Thaler, 2015).

ii. Limitations

The following limitations should be considered when analyzing and generalizing the results of the experiment.

1. The specific performance of the computers and the Internet connection in the study was not recorded or monitored for consistency. Some participants may have been delayed by fluctuating Internet connection speed, or technical issues not encountered by other participants. While researchers were available to correct these issues, should they arise, they were not actively observing the experiment and only would take action if requested by the participant.
2. Participants' self-evaluation of their computer skills is highly subjective. As the Dunning-Kruger effect has often showed, people of low ability have illusory superiority of their abilities, whereas those of greater ability also have illusory inferiority of their abilities (Kruger, Dunning 1999). We specifically asked participants if they had accomplished the research task before to attempt to mitigate this effect.
3. Our ability to recruit limited our participation numbers. The numbers achieved are sufficient to develop conclusions, but do not serve as empirical proof of the results without further study.
4. Due to the length of time provided to the participants (3 hours) being substantially longer than the longest participant attempt (2 hours), we presume that no test subject experienced time pressure or terminated the

test artificially early in order to meet a schedule requirement. Some may have had outside commitments they did not disclose that pressured them into terminating the experiment early.

I.7 Research Contributions

The key contribution of this research effort is the quantification of the improvement in task duration and task completion speed for a technical task by a non-expert when the non-expert has access to fully current content instead of outdated content. This knowledge, when combined with similar quantifications of asynchronous versus synchronous education, modular versus serial education, and temporally delayed versus just-in-time education, contributes to the development of the optimum model for providing educational content to technical skill learners, such as STEM students.

I.8 Conclusion

This experiment is carefully designed to provide an open world for users to explore, in order to answer questions about user preferences in education, and then to further evaluate the quality of their preferences in determining suitable and effective educational material for completing challenging technical tasks. This information, properly gathered, curated, organized, and reported, will build upon previous research into self-teaching methods, educational methodologies, and training strategies to improve the foundation upon which educational platforms such as the Cyber Education Hub utilize to maximize effectiveness in providing education and training to their customer base.

II. Literature Review

II.1 Overview

In the past decade, the proliferation of cyber education has been phenomenal. As is generally the case with new markets for education, the cyber education market has stepped up to provide education and certification for millions of professionals (Newhouse, 2017). As is also generally the case, the quality of that education has varied significantly from degree mills producing people who struggle with basic concepts to prestigious institutions producing the foremost experts of our time (Parrish, 2017). As the Department of Defense (DoD) hires or produces cyber personnel to serve its own purposes, it has identified a need to provide quality controlled initial and continuing education for those personnel. Additionally, as both academia and industry have begun increased focus on educating the user as a critical part of system security, the DoD has added requirements to provide similar education to all its network users (Dacus, 2018). In order to determine how to do this we must fully understand the research space in two main areas: first, the most effective educational techniques and second, what available modes students are pursuing to acquire knowledge. *If we understand these two areas, we can design experiments and research to bring them closer together, and provide education using the best techniques to those searching for it on their own.*

II.2 Education

Recent research is changing the way we see education. As students' backgrounds become more diverse, and their access to information continues to proliferate, research has identified changes in how best to educate modern students. Leading Air Force researchers have further shown the effectiveness of these educational methods are not fully realized by Air Force educators.

Bradwell (2009) comments: "Teachers and lecturers have to deal with a much greater range of information processing styles, cultural backgrounds and styles of learning. As a result, the ideal for teaching in higher education is now recognized to involve much more than lectures as the means of information provision." While the lecture mode of education has served our society for centuries, research continues to show that multimodal education provides superior results in modern students. Studies on multimodal learning from a neuroscience perspective (Fadal, 2008), an educational perspective (Hazari, 2004), and a cognitive science perspective (Picciano, 2009) all agree on one principle summarized best by Fadal; "students engaged in learning that incorporates multimodal designs, on average, outperform students who learn using traditional approaches with single modes." Multi-modality is inherent to self-teaching by way of Internet resources. Search engines routinely return results for searches that include text, video, and audio content. The understanding of how users combine multi-modal content to develop knowledge, skills, or abilities is critical to achieving the goal of optimizing that process. With that perspective, designers of educational platforms must

ensure that users have parity of access to many modes of education for every topic they may wish to learn on the platform. This is specifically relevant to the military, whose longstanding culture of schoolhouse education goes back to nearly its inception (Abrams, 1989).

In addition to multi-modality, continuing research demonstrates benefits to incorporating asynchronous learning environments, where students study, learn, and complete courses at their own pace instead of at a pre-determined group pace. In 2006, a study of 540 students predominantly employed in managerial or technical fields and taking synchronous and asynchronous courses determined that those who took asynchronous courses have statistically improved understanding of course material than those who did not. This held true even for students who had never taken non-traditional classes before (Carswell, 2006). Further study including studies of instructors (Anderson, 2009) and surveys of graduates (Eom, 2016), confirm the benefits of including asynchronous learning options for students. Not all students purely benefit from asynchronous learning, of course. Anderson reports on accounts by some instructors of students procrastinating and then rushing to complete the class rapidly, to their detriment. Eom found that some students found asynchronous study to lack compulsion. They felt a reduced drive to perform well in the class, or stick to a schedule. Clearly, an element of self-motivation and drive is required to get the most out of asynchronous learning, but with that drive, the benefits are clear.

Research is already underway into how to most effectively nurture that self-motivation in military cyber students. Using the "Octalysis Framework" for understanding human core drives, Tomcho et al. (2019) have devised and tested strategies for maximizing the drives "Epic Meaning and Calling", "Development and Accomplishment", "Ownership and Possession", "Empowerment of Creativity and Feedback", and "Social Influence and Relatedness" for both creators and consumers of educational content. Responding to a survey about their experiences with the CEH, users reported a desire to seek out education on their own time both on the hub and outside of it. Users responded at an average level of 5.15 out of 7 on a Likert scale confirming their increased motivation for self-teaching. Users also reported an average of 5.14 out of 7 that the Core Drive strategies motivated them to consume more content. For users who did not identify as gamers, when presented with the statement "I consumed more content on the Cyber Education Hub than I would have if I did not have access to the KSA Tree [the core drive targeting mechanism]" the users responded in agreeance with an astounding average of 6.7 out of 7. Contrast this to military training that does not designed to target these core drives. Users responding to survey questions about their desire to complete that training unanimously indicated they would *only* complete training when required of them. It is thus clear that "self-motivation" is not simply an inherent quality of a learner that cannot be influenced, but rather can and should be deliberately influenced by designers of education and training to significantly improve outcomes in modern training models.

While the benefits of multi-modality, asynchrony, and intrinsic motivation are known, the Air Force's schoolhouse culture stands in contrast. This culture's limitations are recognized by leading cybersecurity researchers from within the Air Force. In "Rethinking USAF Cyber Education", Reith et al (2018) break down the limitations of traditional schoolhouse education into three core issues: scalability, currency, and complexity. Schoolhouse style education does not scale at the rate necessary to train non-experts at the speed the Air Force requires. Maintaining "class size" targets is an antiquated and unsustainable way of growing training corps to their necessary throughput to meet future demands. Schoolhouse education also leads to currency issues. With the field of cybersecurity being one of the most rapidly changing landscapes, the process of requesting, creating, reviewing, approving, and distributing more current classroom content is too slow. By the time classic processes are applied to the verification of the content, the new content is now just as outdated as the old content was at the initiation of the update. Lastly, schoolhouse material suffers from the burden of fixed complexity. While some students possess foundational knowledge that would enable accelerated training, others lack pre-requisite information necessitating retarded training. When grouped together in a classroom format, the fixed depth, breadth, and pace of traditional schooling harms both of these groups' learning experiences.

The fact that the Air Force has not pursued these new techniques in cyber education is no secret. Numerous papers identify and re-identify issues with how the Air Force is

educating its cyber workforce. In “Teaching Beyond Cyber Fundamentals to Develop an Expert Workforce” (Skoda and Rich, 2017) the authors observe “that many training programs re-teach fundamental knowledge, skills, and abilities (KSAs) in their courses to ensure learners have a similar baseline entering the course. The KSA review is typically inadequate for a novice to learn the material and by including elementary material, causes advanced learners to disengage from the course.” Here they have identified that current Air Force cyber training is not sufficiently modular to adapt to the individual learner. Furthermore, in 2016, members from USCYBERCOM, SAF/CIO A6, AFSPC, AETC, ACC, AMC, 23 AF, 25 AF, and other partners in industry and academia conducted a “design sprint” and published their report as “Air Force CyberWorx”. Guided by the AETC framework known as the “Continuum of Learning”, CyberWorx identified that current training was not asynchronous, modular, or career field oriented (Chiaramonte et al, 2016). Finally, Dacus (2016) identified no less than 91 separate Air Force and DoD cyber courses available from 20 organizations. Currently, no office in the Air Force has the responsibility for tracking and managing this training for airmen within the cyber career field, or without. This results in disjointed training, where topics unnecessarily overlap between courses, unknown information gaps exist, and information is presented very differently, sometimes even contradictorily, in different environments (Reith, 2018). Additionally, cyber concepts cut across career fields, affecting medical teams, security personnel, maintenance, acquisitions, and virtually all other military professions in some capacity. Cyber training management that ensures these courses are consistent, available, and effective is not centrally controlled or tracked, which

contributes to making the optimization of this type of training by reducing overlap and increasing consistency all the more challenging.

Long-standing research in education has shown that just-in-time training in the context of the task being performed is more effective than formal training, which is temporally disconnected with the task, or includes inauthentic facsimiles of the tasks. Connecting task learners with live assistance from peer task experts has resulted in superior outcomes in worker training (Collins, 1997). Further research quantified the temporal loss of knowledge, specifically in high tech training. If training is separated from task execution by one month, 40% of that knowledge is lost in the temporal gap. After 6 months, the knowledge loss rises to 90% (Globerson, 2001). Access to just-in-time training created and provided by peers of the student is just one more force multiplier available to the optimize cyber education.

In response to these studies, the Air Force Institute of Technology began development of the Cyber Education Hub (CEH). The CEH was designed to support cyber-education for DoD employees by a providing secure, asynchronous, modular, or career field-oriented training material created by users, for users, and curated by users. The CEH is a cloud based educational content curation and distribution engine, providing the opportunity for far more knowledge to be centralized, including customized content that effectively conveys cyber concepts to members of disparate career fields who have unique jargon and career experience.

II.3 Trust

Furthermore, information given to non-experts by experts must be trusted for it to be effective. Previously, we have argued that non-expert computer users are psychologically very much like medical patients, and the cybersecurity experts attempting to garner compliance for them are share much in common with doctors when it comes to their relationship with their "patients". The experts in both cases reap the highest probability of compliance from their charges by earning their trust. That trust is earned by standing on two pillars: demonstrated competence and perceived caring. While this thesis does not pursue further understanding the caring relationship, we do demonstrate insights into demonstrating competence and how easily the non-experts' trust can be mishandled or abused. Without this competence on the part of the expert creating educational content, the user may not trust the provider, and without that trust they are less likely to comply with any direction or training they receive (Martin et al., 2017). In this way, future network breaches stemming from user behavior issues may be traced back to the quality of information provided by authoritative sources. For example, simply failing to update user guides when new versions of software are released may be the root cause of a user-induced critical incident.

II.4 Research Gaps

Education has taken a clear turn into a less formal direction, where students complete multi-modal coursework on their own time, at their own pace, and with sporadic contact with instructors. Many students therefore pursue their own material to fill their

needs. Current research does not fully understand how this affects workforce productivity in filling the cyber-educational needs of the non-cyber workforce. This research seeks to fill that specific gap.

III. Methodology

III.1 Overview

Recall from the chapter one, this study investigates educational material modality paths selected by non-technical participants when attempting to complete technical tasks in the absence of formal guidance, specifically in the domain of cybersecurity. For the purposes of this study, educational modes are ways in which education is presented. Examples include visual education through video or pictures, audio education through verbal instruction or text, as well as styles of instruction such as how-to guides, product manuals, question and answer forums, and real time electronic communication with experts. By observing which educational modes and paths participants pursue most frequently, and which modes and paths are most likely to result in successful completion at the task, this study uncovers which modes and paths should be incentivized and disincentivized on multi-modal, modular learning platforms.

This chapter describes the specific protocol, equipment, and variables assessed in our experiment.

III.2 Experimental Protocol

Here we will describe in detail the experiment, including the hardware, software, network configuration, participant selection, participant briefing, and data recording used to complete the experiment.

This research project has been approved for the use of human participants by the Air Force Research Laboratory's Institutional Review Board (IRB) FWR20180182H v1.00 in accordance with AFI 40-402 and AFRLI 40-402.

Protocol design and writing took approximately one week. Institutional approval took approximately two weeks before going to IRB. IRB sent suggested edits after six weeks, and approved the edits one week later. The entire protocol approval process therefore was ten weeks.

iii. 3.2.1 Independent Variables: Factors and Levels

This study is a within-participant evaluation with measurements on many individual investigative tasks. In phase one of the experiment, users are given no direction and the materials they access are left unchanged. There is one factor in phase one of this experiment - the educational materials accessed. In phase two, a single piece of educational content is modified to provide directions that more closely match the test environment. This introduces a second factor in phase two, the educational material identified and modified. The experiment consists of a single task that is difficult for non-experts to perform without additional guidance, but does not require knowledge synthesis or critical thinking. Completion of the task will depend entirely on the information the participant is capable of learning either directly from the provided Internet access, or from informed trial and error.

iv. 3.2.2 Measurements & Dependent Variables

There are two dependent variables in this study: task completion (assessed using network analysis software) and speed of task completion (assessed using network analysis software and screen recordings).

v. 3.3.3 Task Environment

The task environment for the study was the implementation of a media access control (MAC) address whitelist on a simple consumer network using a Netgear WGR614 router (the router calls this simply an "Access Control List"). MAC addresses are unique number/letter combinations that specifically identify network interface devices such as WiFi adaptors and Ethernet adaptors. MAC address whitelists are security measures used to specifically identify authorized network interface devices to permit on the network, while blocking all others by default. We selected MAC address whitelisting as the basis for this study for the following reasons.

1. We hypothesized that intended participants were unlikely to have accomplished the task before. While most routers support MAC address whitelisting, users uncommonly implement it. Out of the 22 respondents to the call for participants, only 1 had implemented a MAC filter before, suggesting that the hypothesis was reasonable.
2. It is a procedure that intended participants could understand. In the preparation for the study, we explained MAC address whitelisting to volunteers who met the

requirements for participation in the experiment, and found them able to understand it readily.

3. The process requires combining knowledge from different categories. Participants needed to understand how a router fits in to a network, what a MAC address is, how to interface with devices through terminals, acquiring and using credentials, and a basic understanding of security vocabulary such as “authorized”, “unauthorized”, and “blocked”.
4. We believe this technical task to be representative of other technical tasks in both the cyber and STEM fields.
5. Other tasks were evaluated for suitability for this experiment prior to selection of the MAC address whitelist. WiFi encryption was evaluated to be too familiar to likely participants, and therefore too likely that participants would have accomplished it previously. Replacing the firmware with 3rd party firmware (DD-WRT) was also considered. A dry run of that challenge proved to be too lengthy a task, even when performed by experts.

During each investigation, participants interacted with a provided network and router, and attempted to implement MAC address filter on the router via the provided terminal. Six Raspberry Pi 3s running Raspbian Nov-18, were attached to the network and act as nodes for the participant to allow or disallow via MAC address filtering as well as report progress to the participant, and record their status. Raspberry Pis were selected because they were already purchased in the department, easy to use, and met all requirements for acting as nodes and recording their data. Raspbian was used

because it was already loaded on the devices, and met all functionality requirements. Using six devices provided redundancy for the data collection aspect of the test setup, which was useful in precisely determining timing of user activities logged by the Pis. The WGR614 was selected because it was inexpensive, was representative of consumer grade routers, supported MAC address filtering, but that support was sufficiently challenging to find within the firmware to be challenging. Additionally, the router did not support Ethernet MAC filtering, so participants could not accidentally block the Network Terminal during the experiment. Only WiFi devices could be blocked.

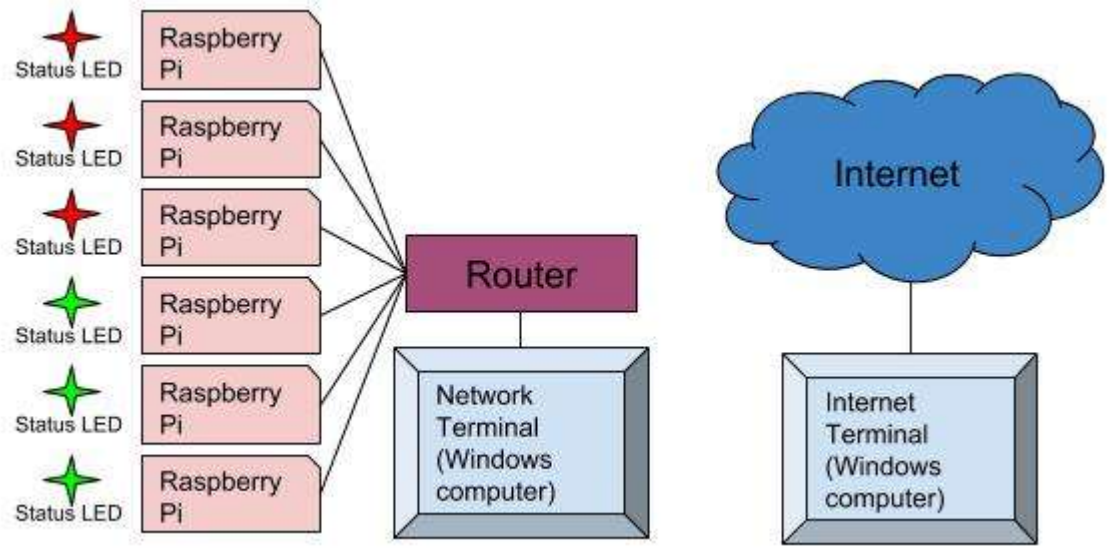


Figure 1 - Test Network Diagram

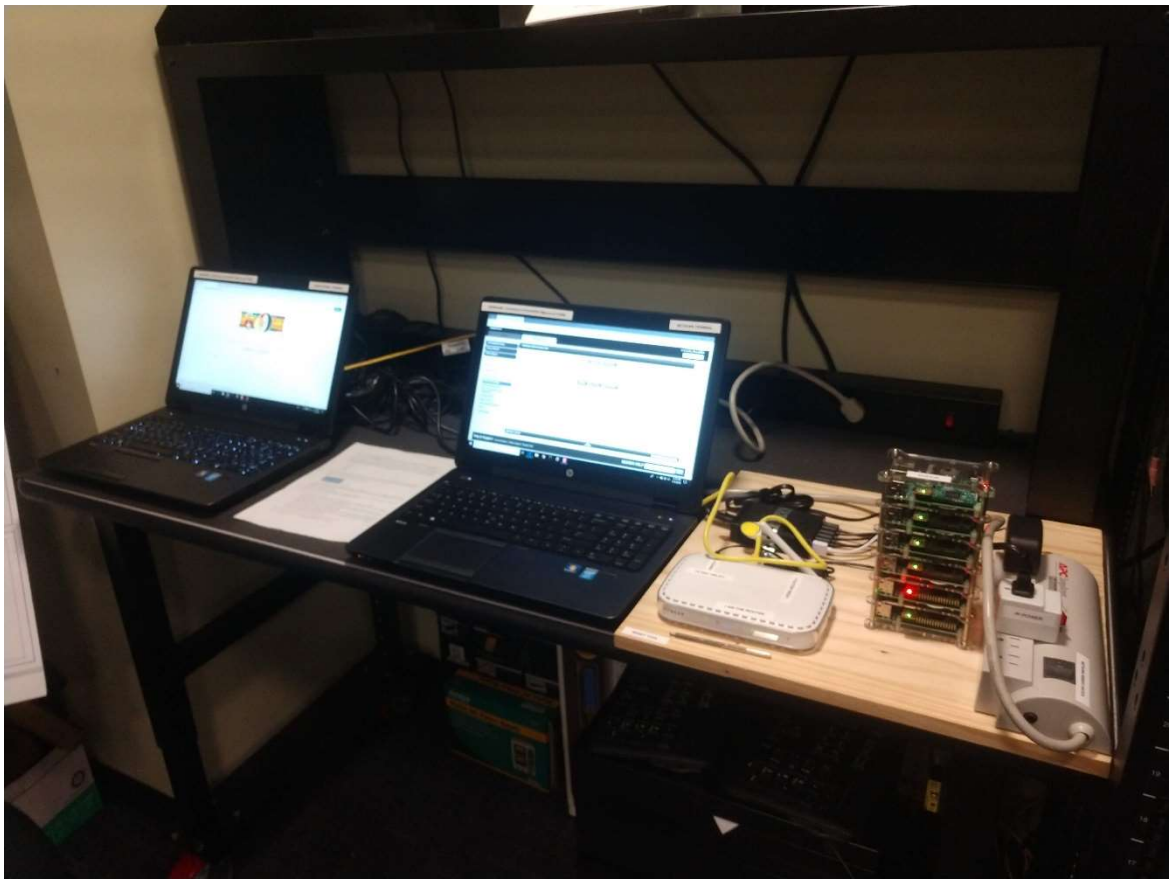


Figure 2 - Full Test Setup

We performed three dry runs with volunteer participants. The first dry run was a member of the research team. The second was a colleague (Cyber Operations student) who was an expert, but not a member of the research team. The third was a non-expert who had been present for much of the planning of the experiment, and therefore was ineligible, but did not have expert knowledge. These dry runs revealed weaknesses in the data collection methods that were corrected. For example, the Pis were originally configured to record all test data to a single .txt file, but failed to re-open and write to that file after a reboot. This was discovered in dry run 1, and led to a change in the code that created a new log file for each session on the Pi. Instructions were also improved due to dry run 3. The volunteer noted that while he was able to deduce that he needed to reboot the devices during his attempt, he wasn't sure he was permitted to, or how. A hardware switch was added, and language was clarified in the directions to ensure participants were given specific instruction on how to reboot the Pis and the Router should they need to. Dry runs, experiment modification, and data analysis took approximately two weeks.

vi. 3.3.4 Human Participant Task Sequence

Each participant experienced the experiment for a maximum of 3.5 hours: The first half hour (setup) familiarized the participant with the interface and the task, while the remainder of the time (experiment) involved the participant attempting to complete the task. Participants attempted the experiment at will, and were told at the beginning of the experiment that they may terminate the experiment at any time for any reason. They were not required to utilize the full experiment time to attempt completion of the

task. The setup and experiment period occurred sequentially. Participants completed a pre-study questionnaire during setup (see Attachment 3).

vii. 3.3.5 Setup Overview

The participant first completed a questionnaire regarding their educational experience and technical confidence. The researcher then familiarized the participant with the network and available resources. They were shown the network, as well as the computer connected to the test router (network terminal) and the computer connected to the Internet (Internet terminal). See Figure 1 - Test Network Diagram for a diagram of the network setup and Figure 2 - Full Test Setup for an image of the test setup. The basic outline of the task and the metrics for success of the task were explained and provided to the participant (see Attachment 2). The participants were told to allow only three MAC addresses on the network from three of the Raspberry Pis. Because the router only supported WiFi MAC filtering, whitelisting the Ethernet connected network terminal was unnecessary. The participant was informed that they may use any material or information accessible from either of the two provided terminals, but no information retrieval was permitted outside of those two terminals, eg., the participant's smartphone.

The experiment measured the ability of the test participant to complete the task in the time allotted, and measured the time it took to achieve completion. Participants were given 3 hours. Due to the length of the experiment, participants were permitted to leave

the room and return to complete the task, but not to access outside materials when not in the room. Participants who did not complete the task within the three hours were considered unsuccessful. Participants who completed the task within the three hours were considered successful, and their level of success is determined by the speed at which they completed the task. Participants completed the task separately – only one participant at a time.

Setup

1. Recruit participant
2. Investigator assigned participant number
3. Participant completed the pre-experiment questionnaire
4. Investigator provided instructions on activity and measures. Participants were briefed about the task, the time limit, the provided equipment, and the allowed and disallowed resources.

Execution

1. Participants completed the execution phase. Participants were given three hours to complete the experiment. A researcher ended the experiment when any of the following criteria were met:
    a. The participant successfully implemented the MAC filter as prescribed (the LED lights on the test setup were displayed as shown in Figure 1 - Test Network Diagram).
    b. Three hours of test time elapsed

c. The participant voluntarily terminated the test (recorded as unsuccessful).

Data collection

1. Collect video recordings:
    a. Stop recording via the Camtasia software
    b. Camtasia rendered the save file
    c. Save the file as “Test Subject [number] [terminal name]”
    d. Copy the file to a flash drive to transfer to the data analysis network.
2. Collect Raspberry Pi data
    a. Complete a factory reset on the test router
    b. Turn off the test network, and relocate it to the data analysis network.
    c. Turn on the network
    d. Connect a KVM setup to each Raspberry Pi, and download every results#.txt file where # >= 1 to a flash drive in a subfolder titled “Pi N” where N is the unique designator of the Pi. These files contain the network connection logs recorded by the Raspberry Pi.
        i. During the data collection session (Session A), the Pis will still be recording network data, as this function occurs any time the devices are powered. This data is being saved to results.txt during the session, and should not be collected.
        ii. On the first boot after the data collection cycle (Session B), the results.txt file that was created in that section will be renamed

results0.txt, and a new results.txt will be created to log activity during Session B. Upon a reboot of the Pis and therefore an initiation of Session C, this results.txt will be renamed results1.txt and a new results.txt will be created to log Session C, and so on.

iii. The number of sessions, and therefore the number of results files, depends on how many times devices are rebooted, but the previous participant's data collection session logs will always be saved as results0.txt and the current participant's data collection session logs will always be visible during the data collection session as results.txt, and therefore should not be collected.

iv. Summarized: results1.txt, results2.txt, etc. contain the participant data and should be downloaded and saved by the data collector, results.txt and results0.txt contain data only from data collection sessions, and should not be saved by the data collector.

3. Reset experiment
    a. Refresh all browsers by clearing all their stored data
    b. Reinstall the network interface on the network terminal via the Device Manager Control Panel to ensure that any changes made by participants are undone.
    c. Verify router was factory reset in step 2A

d. Confirm Ethernet connection between the network terminal and the router (ping 192.168.1.1 from command prompt to confirm without polluting browser history)
e. "Pi Power" should be "ON" and "Network Reboot Switch" should be "OFF".
f. Both terminals should be on and connected to dedicated power separate from the Network Reboot Switch.
g. Internet Terminal should have Internet access. (ping www.google.com from command prompt to confirm without polluting browser history)
h. Network terminal should have WiFi disabled.

Experimental Measures

We manually analyzed the recordings of the computer screens the participants used during the experiment, and mapped their activities including what resources they used, for how long, and the order during their attempt to complete the task. Network logging software running on the Raspberry Pis identified when devices were blocked, unblocked, or rebooted, and recorded that data to text files on the Raspberry Pis numbered sequentially starting with results0.txt

In phase two, we modified access to a single resource so it correctly represented the current version of the router's firmware. Burp Suite (a network traffic monitoring and editing security tool) was installed on the Internet terminal. Burp changed all links on downloaded webpages that were pointing to a specific Netgear resource

(https://kb.netgear.com/13112/How-to-configure-Access-Control-or-MAC-Filtering-Smart-Wizard-routers shown in Figure 3 - A Screenshot of the Outdated Resource) to point to a researcher generated and modified copy of that resource (http://timandkrysta.net/sethsproject/ shown in Figure 4 – A Screenshot of the Updated Resource). Because the link modification happened at the HTML level, it was virtually transparent to the test subjects, ensuring the highest likelihood that they would believe they were accessing the authentic website from kb.netgear.com. Since authoritative sourcing can be important in determining the quality or usefulness of material, this subterfuge was important to ensuring that participant utilization rates of the material remained unaffected by the fact that the researchers created the material, rather than the router manufacturers. Should participants have been aware that the source of the information was not authentic, it would have introduced a second independent variable to the experiment (content source) alongside the intended independent variable (content accuracy). No measures were taken to increase the likelihood that participants would access this material. Their likelihood of selecting this material and reasoning behind such a selection is identical to phase one. Participants in Phase Two were asked after the experiment if they accessed the spoofed resources. Participants who did were asked if they noticed the URL change. None of them responded that they noticed the change.

To configure Access Control or MAC filtering with Smart Wizard:

1. Use an Ethernet cable to connect a computer to any one of the four LAN ports of the NETGEAR router.
2. In a web browser, enter the router IP address, either **http://192.168.0.1** or **http://192.168.1.1** by default.
   If these IP addresses are not working, see How do I login to my NETGEAR home router?
3. When prompted for a username and password, enter the username and password. The default username and password are **admin** and **password**, respectively.
   NETGEAR recommends changing the default password to increase the security of your network.
4. From the main menu on the left, select **Advanced > Wireless Settings**.
5. Click **Setup Access List** to open the Wireless Card Access List.

Figure 3 - A Screenshot of the Outdated Resource

To configure Access Control or MAC filtering with Smart Wizard:

1. Use an Ethernet cable to connect a computer to any one of the four LAN ports of the NETGEAR router.
2. In a web browser, enter the router IP address, either **http://192.168.0.1** or **http://192.168.1.1** by default.
   If these IP addresses are not working, see How do I login to my NETGEAR home router?
3. When prompted for a username and password, enter the username and password. The default username and password are **admin** and **password**, respectively.
   NETGEAR recommends changing the default password to increase the security of your network.
4. On the top tabs, select **Advanced**
5. On the left toolbar, select **Advanced Settings** > **Wireless Settings**.
6. Click **Set Up Access List** to open the Wireless Card Access List.

Figure 4 – A Screenshot of the Updated Resource

Measure 1: Task Success

A participant's attempt is considered a success if a MAC filter is implemented on the router (see Figure 5 – An example MAC address filter on the test router) which permits

only the three specified devices to transmit wireless network traffic and blocks all others. The Raspberry Pis report their network access to the participant a custom designed printed circuit board containing two status LEDs. The remaining three Raspberrfy Pis simulate unauthorized devices and report their network access via the status LED. Raspberry Pis with a connection to the router access illuminate a green LED as shown in Figure 6 - The Initial State of the Network.

Figure 5 - The Initial State of the Network

Raspberry Pis without a connection to the router illuminate a red LED as shown in Figure 6 - A Network with no Router Connection.

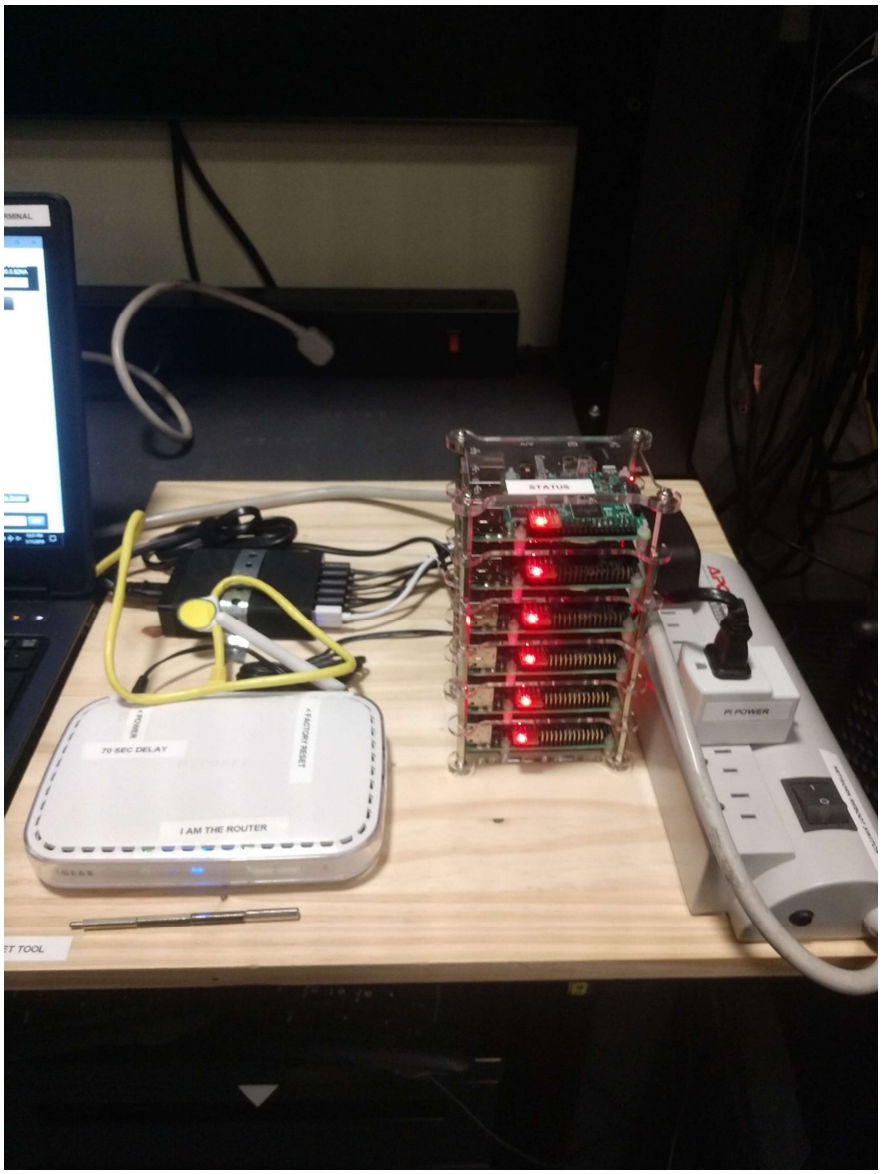


Figure 6 - A Network with no Router Connection

A participant was deemed successful when the upper three Raspberry Pis on the stack illuminated red and the lower three Raspberry Pis illuminated green as shown in Figure 7 - A Successful Participant. The Pis use Python scripts to change their LEDs as well as to record their network status for use in data analysis. The Python code is included in Attachment 1.

Figure 7 - A Successful Participant

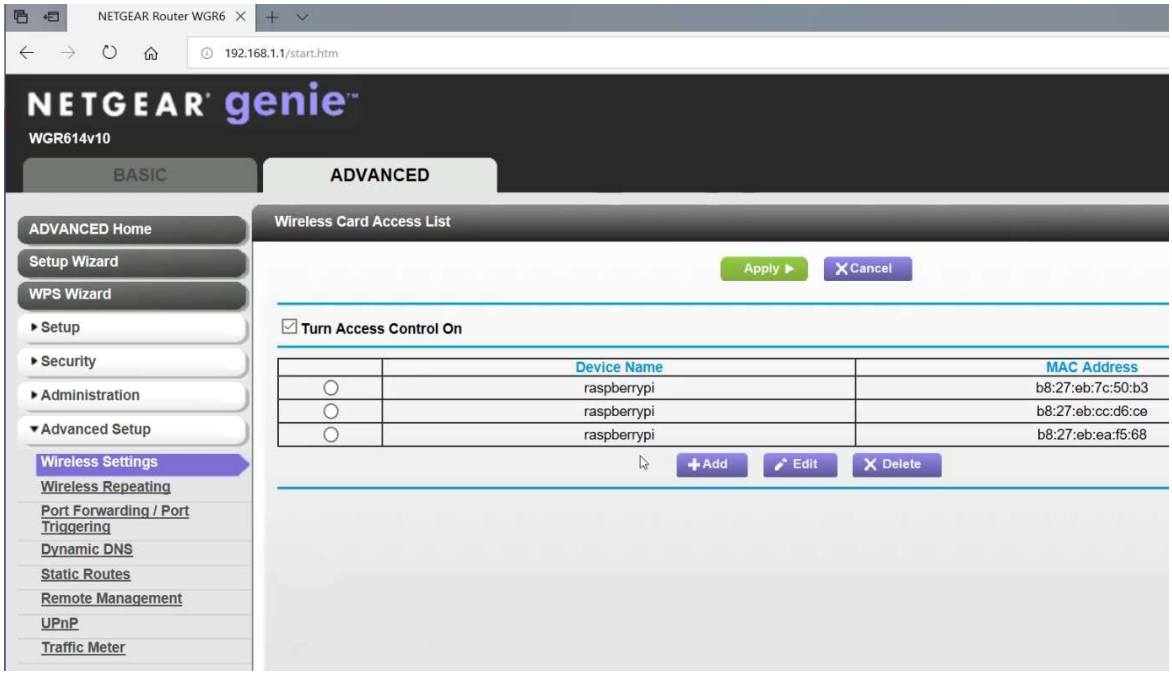


Figure 8 – An example MAC address filter on the test router

Measure 2: Task Time

Throughout the experiment, the displays on the two terminals were recorded. After the experiment, researchers analyzed the recordings to determine which resources were used, for how long, in which order, and identified if the participant was successful or unsuccessful. At the completion of the experiment (successful or otherwise), the amount of time the participant used was recorded based on the end time of the two terminals' recordings.

III.3 Inclusion Criteria:

A participant who has met all of the following criteria was eligible for participation in the study:

- Able to operate a mouse with either hand.
- Able to operate a keyboard.
- Has sufficient visual acuity to use a computer with a monitor.
- Can read and understand English.

III.4 Exclusion Criteria:

A participant who meets any of the following criteria were disqualified from participation in the study:

- Unable to use a mouse or keyboard
- Visual impairment preventing using a computer
- Specific motor, perceptual, or cognitive conditions that preclude use of a computer, reading small characters on a computer monitor, or hearing and comprehending verbal commands presented by the experimenter
- Participants who possess cyber expertise prior to the experiment as reported on Attachment 3 – Pre-experiment Questionnaire.

III.5 Recruitment

i. Recruitment Method:

ii. Volunteers were solicited from two organizations utilizing their established human research recruitment processes: The Air Force

Institute of Technology (AFIT) and the 711th Human Performance Wing. All respondents were from AFIT.

iii. Participant Recruitment Email:

"The Air Force Institute of Technology (AFIT) is conducting a study in which participants will perform a computer-based task using a mouse and keyboard. A variety of data regarding task performance will be acquired during the study. The main goal of this study is to determine how non-experts educate themselves to complete technical tasks. Participation in this study is voluntary and there is no compensation. However, participation in the study will allow you to take part in important research about education. Volunteers will be asked to participate in the computer-based experiment in the lab. Participants will work on the task for up to 3.5 hours on one day. This research project has been approved for the use of human participants by the Air Force Research Laboratory's Institutional Review Board in accordance with AFI 40-402 and AFRLI 40-402."

IV. Analysis and Results

IV.1 Overview

Phase One participants performed the technical task with an open Internet connection and no changes to their search results or accessed materials. The most valuable resource to these participants was identified for modification in phase two.

Phase Two participants performed the identical technical task with an open Internet connection, but search results that linked to the identified resource were modified to link to a researcher-updated version of the research. The results were compared to participants in phase one to measure the potential improvement achieved by improving the resource.

Participants in phase one completed the study from 28 October 2018 through 10 December 2018. Seventeen total participants performed the experiment of which 11 were successful and 6 failed. There were 7 males and 10 females. The vast majority of participants were DoD contractors, accounting for 14 of the test subjects. Of the remainder, 1 was a military officer, and the remaining 2 were non-DoD civilians. No DoD civil servants took part in the study. The total data collected spanned 15 hours and 9 minutes. Data analysis took approximately 150% of participant time (a 20 minute participant took 30 minutes to analyze) once data collection had been completed. Data

collection took between 15 minutes and 1 hour, due to variations in video rendering time. Total data collection and analysis for Phase 1 is estimated at 40 hours.

Participants in phase two completed the study from 12 December 2018 through 20 December 2018. 5 participants performed the experiment. 4 were successful and 1 was unsuccessful. Four participants were females and 1 was male. 2 military officers, 1 DoD contractor, and 2 non-DoD civilians made up the participant pool. No DoD civilians took part in the study. No subject participated in both phases of the experiment. A minimum of 10 more participants were necessary to achieve a satisfactory p-value in a two-factor t-test to accept or reject the null hypothesis. The total data collected spanned 2 hours and 51 minutes. Full data analysis was not performed on Phase Two due to time constraints, but all data products were still collected. Data collection is estimated at 2.5 hours.

Test subjects were solicited through mass e-mail, notice board postings (both physical and electronic), by word-of-mouth, and by in-person requests by researchers. The in-person method was, by far, the most effective, successfully recruiting 19 of the 22 participants. One responded to the e-mail request, and the remaining two contacted the researcher after being reached by word-of-mouth.

Overall, data collected shows a wide variety of educational materials accessed including guides published by the manufacturer, published by others, videos, forums, and product

manuals. The most effective resource was the manufacturer published guide. When researchers improved the manufacturer published guide to account for updates to the firmware, test results indicated a likelihood of a strong increase in user success, but test subject quantities were not statistically significant enough to prove the connection.

IV.2 Results

Phase One (unmodified connection to the worldwide web):

Participants varied on the amount and types of materials used. The amount of resources accessed varied from 2 to 16 with an average of 8.6. During analysis, we broke up each specific accessed material into categories. The recorded categories are as follows:

- User experimentation (U): When a user was exploring the firmware, operating system, files, or any other component of the system without utilizing any guidance, it was recorded as user experimentation.
- Manual (M): Accessing the full, written manual for any product was recorded as a “manual” resource.
- Video (V): Any video media accessed is recorded as “video”, whether the media was embedded in another webpage or was hosted from its own webpage.
- Search Engine (S): Any time a user provided a typed query into a search box it was recorded as a search engine. Predominately, users used “Google”, but also “YouTube” as well as search engines for specific websites, such as Netgear’s internal search.

- Webpage (W): Any webpage that did not meet the criteria for any other of the categories is recorded as simply “webpage”
- Netgear Webpage (N): Any webpage provided by Netgear was recorded as a separate category. This included Netgear’s manuals database, knowledgebase, forums, support pages, and guides.
- Specific Netgear Resource (Ω): Any access to this specific webpage was recorded separately. The URL for the website is https://kb.netgear.com/13112/How-to-configure-Access-Control-or-MAC-Filtering-Smart-Wizard-routers as of January 2019

The frequency of use for each resource type varied widely. The results are listed in Table 1 - Resource Type Utilization Rates.

Resource Type	Phase 1 Participants who used resource type	Percentage
U	15	88.2%
M	3	17.6%
V	5	29.4%
S	17	100.0%
W	12	70.6%
N	12	70.6%
Ω	12	70.6%

Table 1 - Resource Type Utilization Rates

Once all user experiences were analyzed and annotated, four specific milestones were identified that needed to be completed in order to complete the task.

1. Router credentials – The instructions indicated that the router’s firmware credentials were left to the default settings, but the default credentials were

not provided to the participant. They could be found online, were printed on the bottom of the router, or were given to the participant by the firmware after several failed login attempts.

2. Locate the Access Control List – The Access Control List (ACL) is several layers deep in the router's firmware interface. To access it, participants must click the "Advanced" tab after logging in, then the "Advanced Settings" header, then the "Wireless Settings" link. A button labeled "Set Up Access List" will take the participant to the ACL. See Figure 9 - Access Control List Location.

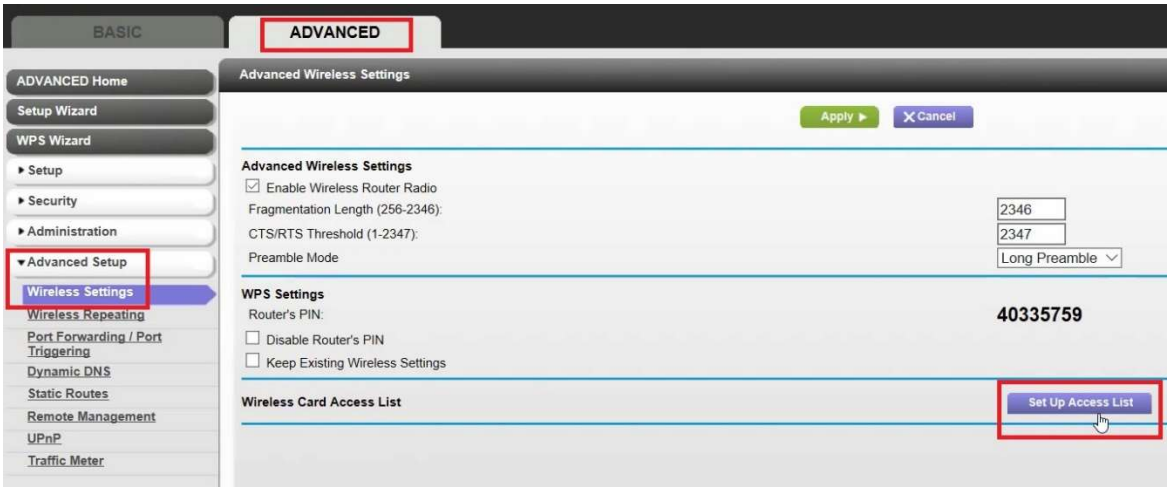


Figure 9 - Access Control List Location

3. Configure the ACL – Participants must either manually add the MAC address of each authorized device, or select the device from the "connected devices" list and add them to the ACL. Only one device at a time can be added to the ACL. After the devices are added, there is a checkbox that must be checked to enable the filter, and the "Apply" button must be selected. Doing these steps

out of order will block authorized devices from the router, resulting in them disappearing from the “connected devices” list. They can then only be added manually. See Figure 10 - A Completed Access Control List.

4. Reboot Pis – The router does not forcibly remove devices after the ACL is created in a timely manner. In order to complete the task, the user must reboot the Pis in order for them to attempt to connect to router, and be accepted or rejected based on the ACL. Participant instructions included directions on how to reboot the Pis (cycling a provided and labeled switch).

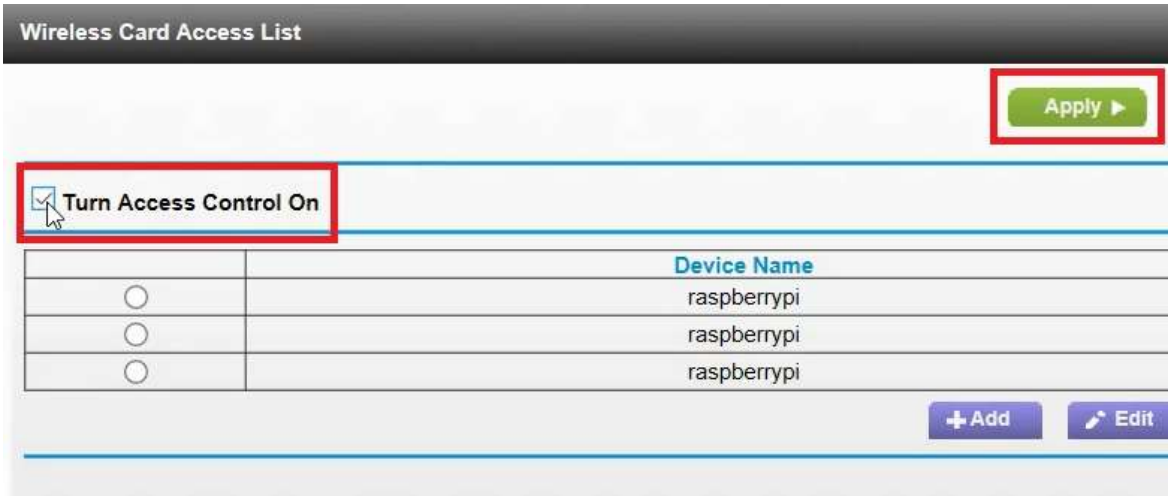


Figure 10 - A Completed Access Control List

In phase one the average participant took 53:28 to complete the experiment. Successful participants finished marginally faster, averaging 46:45. Unsuccessful participants finished marginally slower, averaging 1:05:48. A complete list of phase one participants and results is in Table 1 - Phase One Test Subjects and Results

Test Subject	Gender	Employment	Success	Time	Number of resources	U	W	V	S	N	M	Ω	Router Credentials	Locate ACL	Configure ACL	Reboot Pis
1	Male	Contractor	No	1:23:00	14	Y	Y	N	Y	Y	N	Y	N	Ω	Ω	U
2	Female	Contractor	Yes	0:38:45	5	Y	Y	N	Y	Y	N	N	U	N	U	U
3	Female	Contractor	No	1:00:00	12	Y	Y	Y	Y	Y	N	N	N	-	-	-
4	Male	Military	Yes	0:08:00	1	Y	N	N	Y	N	N	N	S	U	U	U
5	Male	Contractor	Yes	0:19:41	2	Y	N	N	Y	N	N	Y	Ω	Ω	Ω	U
6	Female	Non-DoD	Yes	0:41:21	9	Y	Y	N	Y	Y	N	N	N	U	N	U
7	Female	Contractor	Yes	0:11:54	2	N	N	N	Y	N	N	Y	S	Ω	Ω	U
8	Male	Contractor	No	1:39:00	7	Y	Y	N	Y	Y	N	Y	N	Ω	Ω	-
9	Female	Contractor	No	1:09:00	10	Y	Y	Y	Y	Y	N	N	N	-	-	-
10	Female	Non-DoD	Yes	1:59:18	11	Y	Y	Y	Y	N	N	Y	S	Ω	Ω	U
11	Female	Contractor	No	0:45:51	16	N	Y	N	Y	Y	N	Y	-	-	-	-
12	Male	Contractor	Yes	0:37:17	2	Y	N	N	Y	N	N	Y	Ω	Ω	Ω	U
13	Female	Contractor	Yes	0:35:09	7	Y	N	N	Y	Y	Y	Y	U	Ω	Ω	U
14	Female	Contractor	Yes	1:24:08	14	Y	Y	N	Y	Y	Y	Y	Ω	Ω	Ω	U
15	Male	Contractor	Yes	0:44:14	7	Y	Y	Y	Y	Y	Y	Y	S	Ω	Ω	U
16	Male	Contractor	Yes	1:14:25	14	Y	Y	Y	Y	Y	N	Y	W	Ω	Ω	U
17	Female	Contractor	No	0:37:58	14	Y	Y	N	Y	Y	N	Y	U	W	W	-

Table 2 - Phase One Test Subjects and Results

Phase Two (modification of a single web resource):

Phase Two participants were not analyzed to the same granularity as phase one participants due to time limitations. Their results were recorded, but their step-by-step actions were not observed and recorded. The average phase two participant took 34:07 to complete the experiment. Successful participants averaged 24:30. The unsuccessful participant took 1:13:31. A complete list of phase two participants and results is in Table 2 - Phase Two Test Subjects and Results

Test Subject	Gender	Employment	Success	Time
18	Female	Military	Yes	0:27:24
19	Female	Contractor	No	1:13:31
20	Female	Non-DoD	Yes	0:11:18
21	Male	Military	Yes	0:35:38
22	Female	Non-DoD	Yes	0:23:39

Table 3 - Phase Two Test Subjects and Results

IV.3 Analysis

During the detailed analysis of phase one participants, it became clear that a single resource was highly utilized by the participants, 58% of the time. The webpage used was a guide to implementing MAC address filtering on Smart Wizard routers (which the test router is a member of) written and published by Netgear on their knowledgebase. Each phase one participant had the opportunity to complete all 4 milestones, but some did not complete the test. *In all, 57 milestones were achieved and 22 of them (38.6%) were achieved while utilizing the Netgear knowledgebase article.* However, this resource was not a panacea. 4/6 of unsuccessful subjects did locate and utilize the article, but it did not result in their success. In fact, in two cases, it appeared to contribute directly to the user's failure. The article includes screenshots and instructions guiding the user to the Access Control List in the firmware, but it is written for an older version of the firmware, which has the ACL located in a different directory within the firmware's settings. These two users were unable to find the ACL in the test version of the firmware, and more importantly: during their resulting user experimentation the users changed other settings in the firmware, which were not related to the task, but did have the effect of

blocking all the Raspberry Pis from the network. *The inability to recover from this mistake during user experimentation resulted in the user's failure.* After seeing these dramatic results, we hypothesized that simply updating this resource to match the current firmware may have a profound effect on the success of the users. This hypothesis led to the crafting and implementation of phase two.

Phase Two changed the material from one website from outdated to current and saw striking improvement. The number of phase two participants is lacking, and requires further experimentation with larger pools, but the initial results are certainly promising. *Participants who successfully completed the experiment did so 47.6% faster (22:15 faster) than those who completed it in phase one* (4 and 11 participants respectively).

Additionally, 80% of phase two users were successful whereas 65% of phase one participants were successful, however; the low number of participants significantly limits the reliability of this figure. See Table 3 - Summarized Results.

	Average Run	Average Success	Average Fail	Success %
Phase 1	0:53:28	0:46:45	1:05:48	65%
Phase 2	0:34:18	0:24:30	1:13:31	80%
Total	0:49:07	0:45:38	1:06:54	68%
Phase delta	35.85%	47.60%	-11.72%	15%

Table 4 - Summarized Results

Statistically, there is insufficient data to conclude empirically that updating the specified resource changed the average time to success, or the likelihood of success of the

participants. Using JuliaBox (a free web interface similar to JupyterBox for Python, but for coding in Julia, a statistics analysis language), we can show that our values are insufficient to reject the null hypothesis (that the treatment had no effect on the

participants).

```
#All Participants

using CSV
using DataFrames
using HypothesisTests
using Distributions

#Phase One
data1 = [1.38,0.63,1.00,0.13,0.32,0.68,0.18,1.65,1.15,1.98,0.75,0.62,0.58,1.40,0.73,1.23,0.62]

#Phase Two
data2 = [0.45,1.22,0.18,0.58,0.38]

println(HypothesisTests.UnequalVarianceTTest(data1, data2))
```

```
Two sample t-test (unequal variance)
------------------------------------
Population details:
    parameter of interest:   Mean difference
    value under h_0:         0
    point estimate:          0.3221176470588235
    95% confidence interval: (-0.1725, 0.8167)

Test summary:
    outcome with 95% confidence: fail to reject h_0
    two-sided p-value:           0.1732

Details:
    number of observations:   [17,5]
    t-statistic:              1.4869594034535278
    degrees of freedom:       8.489003730156423
    empirical standard error: 0.21662840714460077
```

Figure 11 - Unequal Variance T-Test for all Participants

```
#Successful Participants Only

using CSV
using DataFrames
using HypothesisTests
using Distributions

#Phase One
data1 = [0.63,0.13,0.32,0.68,0.18,1.98,0.62,0.58,1.40,0.73,1.23]

#Phase Two
data2 = [0.45,0.18,0.58,0.38]

println(HypothesisTests.UnequalVarianceTTest(data1, data2))
```

```
Two sample t-test (unequal variance)
------------------------------------
Population details:
    parameter of interest:   Mean difference
    value under h_0:         0
    point estimate:          0.373409090909091
    95% confidence interval: (-0.033, 0.7798)

Test summary:
    outcome with 95% confidence: fail to reject h 0
    two-sided p-value:           0.0686

Details:
    number of observations:   [11,4]
    t-statistic:              1.9862513315725057
    degrees of freedom:       12.918448474161053
    empirical standard error: 0.1879968989692079
```

Figure 12 - Unequal Variance T-Test for Successful Participants

It's clear that while the data collected is indicative of improved outcomes for the participants, more data collection is required to successfully reject the null hypothesis (the change to the resource did not affect the user's ability to complete the task or the speed completing it).

A hypothetical analysis was performed by cloning the results of the current group for phase two four times, and in that hypothetical scenario the null hypothesis was successfully rejected.

Initially, we had hoped to create a mapping of user activity over the course of the experiment, showing their activity at each resource, how long they were there, how they got there, and how they left. Viewing of user activity showed that the activity was rarely linearly organized. For instance, many users created a search on one browser tab. From the list of results, they selected four resources that enticed them and opened each in a new tab. They would then rapidly jump between the several tabs, and performing experimentation on the network, creating a complex web of cognitive interactions between each resource and the test network. As a test, Subject 6's activity was charted. Subject 6 completed the test in just over 40 mins. This was fairly close to the average. Subject 6's activity was also one of the more linear progressions, despite starting out complex. These facts made Subject 6 an ideal test case for the mapping. As shown in Figure 13 - Subject 6 Resource Usage Map, the linear portion of the test starting after the first milestone is reached follows a predictable pattern: a search is performed, then a resource is accessed, then the resource deemed insufficient so another search is performed, and the process repeats itself until the subject achieves all four milestones and completes the test.

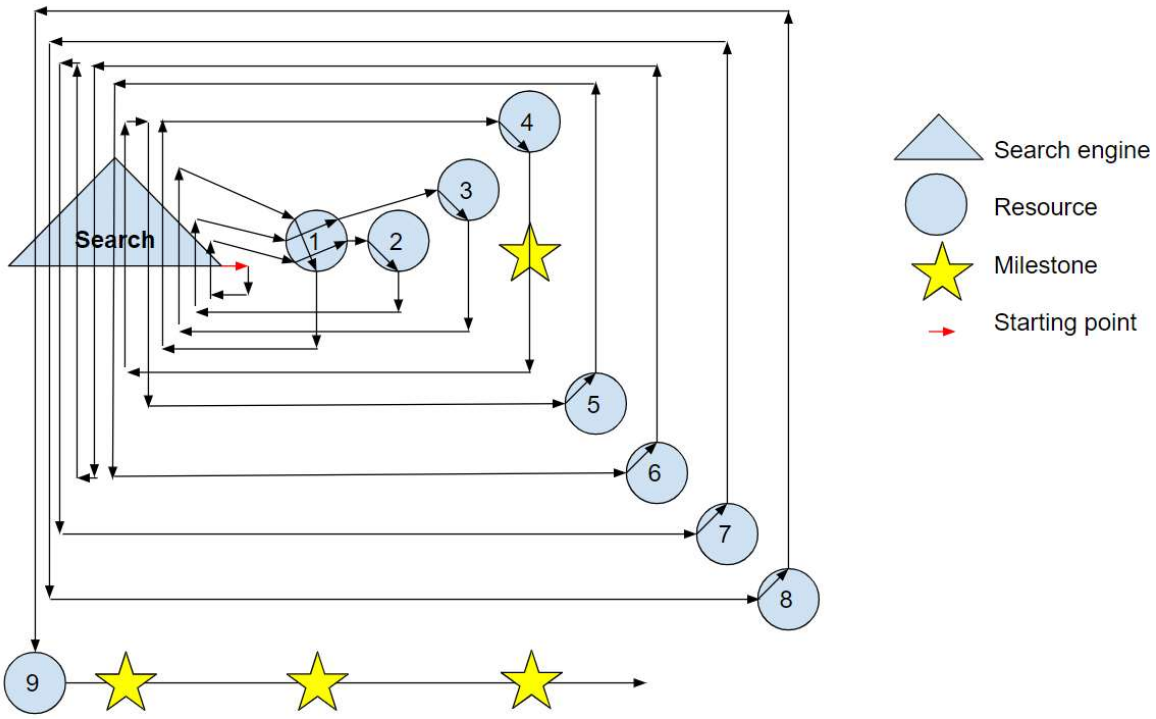


Figure 13 - Subject 6 Resource Usage Map

While Subject 6's pattern is visually intuitive, it is among the shorter, and certainly one of the more simple patterns. Showing a usage map of the entire test group was deemed infeasible and incomprehensible.

IV.4 Summary

In phase one we set out to identify of the global availability of educational material, what materials were non-experts accessing and utilizing in order to complete technical tasks beyond their skill level, and which ones worked and did not work. By viewing video records of 17 participants, we identified a single web guide created by the router's manufacturer that instructed users on how to complete the task. This single resource was responsible for over 1/3 of milestones achieved, but also led some participants to

failure due to being outdated and forcing them to explore, and ultimately guess which actions were necessary to complete the task.

In phase two we set out to identify the measurable impact of updating a single, authoritative source for information on the Internet. As user generated instructional and educational content continues to grow in popularity, it is now more likely that material accessed and consumed will be more current. While the hypothesis that current technical guides are superior to outdated material is hardly novel, a detailed measurement of the benefit of a single improvement of a single piece of material within a sea of options proves interesting. The single resource was updated using a method transparent to the participants, and a second group attempted the experiment under the new conditions. This group experienced a slightly higher (though not statistically significant) task duration, and a significantly higher (though also not statistically significant) average completion speed. More participants are required to statistically confirm the indications from the current test data.

V. Conclusions and Recommendations

V.1 Conclusions of Research

For technical tasks, non-expert users continue to seek out a variety of resources, but the most frequently utilized resources remain search engines and webpages, far outpacing videos. Webpages created and maintained by authoritative sources lead the way in both utilization and effectiveness. Interestingly, websites spoofed to appear as authoritative sources appear to have no change is user utilization, highlighting the risk of both intentional and accidental deception. Intentional deception of this nature, such as a man-in-the-middle attacks, can result in the same level of trust in misinformation as legitimate information with relatively little effort. Non-expert trust in cybersecurity expertise derives from the same two pillars as patients' trust in doctors: competence and caring. First impressions of the competence of information sources are critical to engendering compliance from the information users. Even brief compromises in the perceived competence of authoritative sources, whether from malicious information or simply bad information, has the power to significantly reduce user compliance (Martin et al., 2018).

The speed and frequency at which these resources are maintained and updated have significant impacts on the effectiveness of non-experts when attempting to complete technical tasks. Delaying or neglecting to update these materials may double the time the average non-expert user completes a task. For frequently used materials, this may

have a significant cost to worker productivity. Any organization that relies upon its average users to perform technical tasks in order to help safeguard that organization's systems, should ensure availability of up-to-date materials for the completion of those tasks. Organizations with the resources to create and maintain a database of instructional materials should limit any roadblocks or bureaucratic mechanisms which delay or otherwise impede the production and publishing of these materials. To not do so has a measurable impact on their workforce's productivity and comes at significant opportunity cost to that organization's human resources. Additionally, instructional materials should be broken down in to small segments. Users in this experiment had little tolerance for large data sets of materials (long videos, full product manuals, etc.). They generally preferred to find just the piece of information they needed at that moment, overcome that hurdle, and move on to find the next hurdle. They did not consume extra material to gain total understanding of concepts, rather limited their information search to precisely the minimum needed information to clear the hurdle directly in front of them. While instructional databases may contain large sets of material that can, in total, provide that understanding, it should be stored and curated in small segments that users can rapidly determine the utility of so as to most quickly find the right one.

V.2 Significance of Research

The Air Force Institute of Technology, under the guidance of the Air Education and Training Command, is creating a platform to allow DoD users to create, share, discuss,

and rate cyber educational materials. One of the key questions asked during the formation of this system is how approvals and authorizations to create and publish material should be managed. The culture of the younger generations of Airmen is shaped by social media, where no such filter or approval process exists. The culture of the elder generations of Airmen is shaped by military processes, which require approvals and authorizations for nearly all activities. We sought to provide insight to the debate by providing a measured cost to any delay in the production of new materials. By showing that non-experts performing technical tasks do so more quickly when they have access to the most current possible materials, we our results suggest that there is significant opportunity cost associated with delays or barriers to publishing of cyber-educational material. In this way, the Cyber Education Hub's philosophy of providing a platform for users to rapidly create and publish educational material will reduce the number of man-hours required for the Air Force workforce and userbase to learn the knowledge and skills they will need to be adequate defenders of their networks. When compared with other proven education techniques such as just-in-time availability, asynchrony, and modularity, our research indicates currency of content stands among them as another key to optimization of cyber-education.

This research also has implications for the military acquisition community. When acquiring systems for military use, often user manuals are purchased after system procurement, either from an oversight, or as an attempt at cost savings. This research shows that for users of systems, manuals are not likely to be the most useful material for learning operation. Sometimes contractor provided training is procured as either a

supplement or replacement to the manuals. Again, this research demonstrates a likelihood that this type of training for system users is sub-optimal. The military may be better served by having trained operators produce real-time, fully up-to-date, modular lessons on the system, saving both cost and increasing the overall effectiveness of the training.

Additionally, insights from phase two of the experiment unexpectedly demonstrated the trust that users put in authoritative sources is vulnerable to spoofing. When an authoritative website was supplanted by a researcher-designed mimic of the authoritative source, but with a drastically different URL and some noticeable formatting differences, users exclusively treated the source as if it were the authoritative source. If we provided malicious instruction changes instead of benevolent ones, it seems very likely those instructions would have also been followed by the participants. This clearly highlights the vulnerability that the non-educated user poses to a network, which has already been called the greatest threat to global cybersecurity (Hamby, 2017). Recall from Chapter II we asserted that for users to comply with expert instructions, they needed to perceive both competence and a caring attitude from their instructor. Much like in the medical profession, some sources receive a "benefit of the doubt" affect when users evaluate their competence; however, we've shown that that trust can be misplaced. When authoritative sources publish outdated or mistaken material, as Netgear did in this case, this erodes the pillar of competence in the trust relationship between user and expert. This lack of trust leads to a lack of compliance with instructions, policies, protocols, and training that can lead to network penetration

and exploitation by adversaries (Martin et al., 2018). Our combined research suggests that *incorrect information provided either maliciously or intentionally may indirectly result in catastrophic cybersecurity failures in large networks*.

Lastly, non-cyber military career fields should investigate the feasibility and potential effectiveness of similar educational platforms designed around the same platforms as the Cyber Education Hub. The foundations discussed in Chapter II are not limited to cyber-education, but are generalized to all educational ventures. Certain career fields which impact many other operational areas, such as recruiting, may find modular, multi-modal, accessible education platforms most useful in improving their members skills and knowledge.

V.3 Recommendations

While the DoD is unlikely to move away from schoolhouse training in the near future, due to the cultural inertia as well as the monetary investments in the schoolhouses, educational leaders in the DoD can use the results of this and related research to re-shape the role of the schoolhouse and it's instructors. Previously, students performed synchronous learning as taught by a singular instructor per subject. Currently, undergraduate cyber training (UCT) is shifting to an asynchronous philosophy. The goals of this shift are to more quickly fill workforce gaps in the military by allowing students with previous knowledge, skills, or the ability to learn more quickly to complete training faster and enter the military workforce. This shift is partially enabled by a shift to Internet enabled learning, but this technological tool opens the door to an even more effective shift in philosophy. Schoolhouse instructors currently act as the sole-source authorities,

providing classroom material, evaluations, lectures, and readings to the students. When students graduate and begin their military careers, their ability to send feedback to the schoolhouse is limited by the transaction costs, such as the difficulty in finding an avenue for that feedback, or the likelihood of that feedback being accepted and incorporated into that curriculum. By lowering the transaction cost, we can encourage and enable that direct feedback line to continually improve education occurring at the schoolhouse. In this model, instructors cease being the sole-source provider of material, and instead act as guides through material provided by them, by others, and by peers who are narrowly ahead of the current students on the same path. Instructor expertise is still required, as misinformation is sure to occasionally come through the new conduits to the pupils. But if instructors embrace this role of guiding, rather than directing, the total knowledge and understanding of their students stands to be improved significantly. Outside of schoolhouses, the Air Force is pursuing a cloud enabled education and training eco-system strategy titled Air Force Learning Services Ecosystem (AFLSE). While the cultural and training implications of this certainly differ from the schoolhouses, enabling crowdsourcing of material or user comments and discussion of material still stands as an effective strategy for maintaining currency of any content being produced and distributed via this system. Similarly, barriers to user content or commentary also stand to delay currency, contributing to precisely the detrimental effects demonstrated by this research.

Either in formal education environments such as schoolhouses, or informally via the AFLSE, USAF leaders should design systems that architecturally enable, encourage, and

reward rapid creation, curation, feedback, and discussion of material to maximize knowledge, learning, skill building, and create the most effective fighting force possible.

V.4 Future Research

We have not shown whether the production quality of material is also significant in the completion of technical tasks. In phase two, the edited material was carefully crafted to appear like the authentic, authoritative, but outdated material. Additionally, the experiment was configured to hide from the participant any indication that the material was not from the authoritative source they thought it was from. Further studies seeking to replicate and expand upon this study should isolate this factor and provide both low production value material (such as simple screen recording with narration or lectures recorded with webcams) and high production value material (such as including animation, high quality video and audio editing, or scripted content) and measure the difference in performance of participants. If low production material significantly impedes participants from completing the task, it may balance or outweigh the benefits of frequently updated material. If it does not significantly impede participants, or benefits them, then the conclusions of this study are further confirmed.

One of the touted benefits of the Cyber Education Hub is its roots as a social network, connecting educators, learners, experts, career field managers, and others through their conversations centered on educational content. While perhaps enjoyable and engaging, the measurable effects of such an environment are unknown. Further research is

needed to determine if fostering such an environment spurs useful conversation that improves learning outcomes, or conversely, creates an opportunity for confusion where common misunderstandings are given more exposure, harming outcomes.

Lastly, the longevity of the form of training provided by the Cyber Education Hub should be compared to legacy training. We know that formal training has a 40% decay rate at 1 month and a 90% decay rate at 6 months (Globerson, 2001). A six month study of users of the CEH or a similar platform can show us if asynchronous, modular, user-curated, current content results in a slower decay rate than the opposite style of content.

V.5 Summary

This research sought to determine how non-experts in the cyber field sought and utilized educational materials from the Internet in order to complete technical tasks without formal guidance or education. Phase One of the experiment consisted of 17 participants. Researchers viewed logs of the participants completing the task of implementing a MAC address filter on a consumer grade Netgear router. We analyzed which resources were accessed most frequently, least frequently, and which resources were most beneficial to the participants. During the analysis of phase one, we identified a specific Netgear guide that was responsible for roughly 1/3 of participant successes, but was outdated and incorrect in some aspects, resulting in some participant failures. Using this information, we created phase two of the experiment where we utilized BurpSuite to redirect participants who attempted to access the flawed resource to a

spoofed website that looks like the Netgear resource, but is updated to correctly guide participants through the current version of the firmware. Data collected indicates that this simple change to one resource in the ecosystem of available educational content may significantly decrease completion times and increase task duration of non-experts attempting to complete the task; however, limitations in the acquisition of test participants resulted in the statistical significance of the gathered data being too weak to draw authoritative conclusions.

Bibliography

Abrams R., (1989). "The U.S. Military and Higher Education: A Brief History", in *The Annals of the American Academy of Political and Social Science", Vol 502, Issue 1, 1989*

Chen, N., Tsai, C., Martin, (January 2009). "Knowledge infrastructure of the future*" Journal of Educational Technology & Society Vol. 12, No. 1, pp. 249-257*

Baker M., (May 2016). "Striving for Effective Cyber Workforce Development", *Software Engineering Institute.* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=473573

Bradwell P., (2009). The Edgeless University. Demos, London

Bruza M., Reith M., (2017). "Multi-Domain Command and Control: The Need for Capability Transparency", *Proceedings of International Command and Control Research & Technology Symposium*, Los Angeles, California, November.

Carswell A.D., Venkatesh V., (2002). "Learner outcomes in an asynchronous distance education environment*," International Journal of Human-Computer Studies, vol. 56, no. 5, pp. 475–494*

Caulkins B.D., Badillo-Urquiola K., Bockelman P., Leis R., (2016). "Cyber workforce development using a behavioral cybersecurity paradigm" *Proceedings of International Conference on Cyber Conflict*.

Chiaramonte M.V., Howe D.R., Collins J.A. (2016). *Air Force CyberWorx Report 16-001: A 21st Century Training Model for Flexible, Quick, and Life-long Workforce Development*. USAF Academy, CO: CyberWorx.

Collins J.A., Greer J.E., Kumar V.S., McCalla G.I., Meagher P., and Tkatch R., (1997). "Inspectable User Models for Just-In-Time Workplace Training," in *User Modeling*, pp. 327–337.

Dacus C., (2013), "Cyber Education and Training.", Air Force Cyber College

Defense Information Systems Agency. (2017). "Department of Defense Cyber Awareness Task" https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm

Fama T., Eugene F., (1965). "The Behavior of Stock Market Prices". *Journal of Business.* 38: 34–105.

Eom S.B., Ashill S.B., (2016). "The Determinants of Students' Perceived Learning Outcomes and Satisfaction in University Online Education: An Update*," *Decision Sciences Journal of Innovative Education*, vol. 14, no. 2, pp. 185–215, 2016.

Fadel C., (2008). Multimodal Learning Through Media: What the Research Says. San Jose, CA: Cisco Systems.

Globerson S., Korman A., (1991). “The use of just-in-time training in a project environment”, in *Journal of Project Management, Vol 19, Issue 5, July 1991, pp. 279-285*

Hamby, Janice M. (2018). “ICCWS 2018 Keynote.*” International Conference on Cyber Warfare and Security, 8 Mar. 2018, Washington D.C., National Defense University*.

Hazari A., (2004). Applying instructional design theories to improve efficacy of technology-assisted presentations. Journal of Instruction Delivery Systems, 18(2), 24-33.

Lt Col Howe D.R., Lt Col Chiaramonte M.V., and Col Collins J.A., (2016). “A 21st Century Training Model for Flexible, Quick, and Life-Long Workforce Development,” rep.

Kruger J., Dunning D., (1999). "Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments". *Journal of Personality and Social Psychology. American Psychological Association*.

Kahn Academy. [Online]. Available: https://www.kahnacademy.org. [Accessed: 01-Jan-2018].

Kim C., Jin M.H., Kim J., and Shin N., (2012). “User Perception Of The Quality, Value, And Utility Of User-Generated Content” *Journal of Electronic Commerce Research, vol. 13, no. 4, pp. 305–319*, 2012.

Lacey H., (2008) “Multiple choice: Is modular education the way forward?” *The Guardian*, 24-Nov-2008. [Online]. Available: https://www.theguardian.com/education/2008/nov/25/modular-education-multiple-choice. [Accessed: 01-Jan-2018].

Macedonia M., (2002) “Games, simulation, and the military education dilemma,” *Internet Univ. 2001 Forum*, *pp. 157–167,* 2002.

Capt Martin S., Lt Col Reith M., “Cybersecurity is like Medicine, Users are like Patients, let’s treat them that way”, *2018 Journal of The Colloquium for Information System Security Education, Edition 5, Issue 1 – October 2018*

Mayadas F., *“Asynchronous learning networks: A Sloan Foundation perspective,” J. Asynchronous Learn. Netw., vol. 1, no. 1, pp. 1–16, 1997*.

Netflix. [Online]. Available: https://www.netflix.com. [Accessed: 01-Jan-2018].

Newhouse F., Keith S., Scribner B., and Witte G., (2017). “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” 2017.

Nicholas A.J.. (2008). *“Preferred learning methods of the millennial generation,”* Int. J. Learn., vol. 15, no. 6, pp. 27–36, 2008.

Parrish A., (2017) “Long-term View Needed for Cybersecurity Education,” *Insid. High. Ed*, vol. 2017, pp. 1–10, 2017.

Picciano A.G., (2009). Blending with purpose: The multimodal model. Journal of the Research Centre for Educational Technology, 5(1), 4-14.

Lt Col Reith M., (2016) “Forging Tomorrow’s Air, Space, and Cyber War Fighters: Recommendations for Integration and Development”, *Air & Space Power Journal*, Winter, Vol 30, No. 4, pp 96-107.

Lt Col Reith M., (2017). “Brandishing Our Air, Space, and Cyber Swords: Recommendations for Deterrence and Beyond”, *Air & Space Power Journal*, Winter, Vol 31, No. 4, pp 103-114.

Lt Col Reith M., Lt Col Trias E., Dacus C., Capt Martin S., 2nd Lt Tomcho L. (2018). “Rethinking USAF Cyber Education & Training”, *International Conference on Cyber Warfare and Security*

Lt Col Reith M., Pentecost S., Celebucki D., Kaufman R., (2017). “Operationalizing Cyber: Recommendations for Future Research”, *Proceedings of International Conference on Cyber Warfare & Security*, Dayton, Ohio, March.

Sankey M., Birch D., & Gardiner M.. (2010). Engaging students through multimodal learning environments: The journey continues. In C.H. Steel, M.J. Keppell, P. Gerbic & S. Housego (Eds.), Curriculum, technology & transformation for an unknown future. *Proceedings ascilite Sydney 2010 (pp.852-863).*

Reddy S., Dietrich G., (October 2017). “Cybersecurity Training and the End-User: Pathways to Compliance”, Journal of The Colloquium for Information System Security Education, Edition 5, Issue 1,

Skoda J. and MSgt Rich M., (May 2017). “Teaching Beyond Cyber Fundamentals to Develop an Expert Workforce,”

Tang Q., Gu B., and Whinston A.B., (Jan 2012). “Content Contribution for Revenue Sharing and Reputation in Social Media: A Dynamic Structural Model,” *Journal of Management Information Systems, vol. 29, no. 2, pp. 41–76,*

Thaler R., (2015), “Misbehaving: The making of behavioral economics.”

Udemy. [Online]. Available: https://www.udemy.com. [Accessed: 01-Jan-2018].

Wagner K.D., Stephens V., and Member C., (2016) “Analyzing Learning Domains: A Study Of Preferred Learning Styles And Age Levels Of Learners Enrolled In Developmental Mathematics Courses At A Local Community College,” November, 2016.

Wallace M., Mackenzie, L., (2012). “Distance Learning Designed for the U.S. Air Force.,” *Academic Exchange. pp. 55–60.*

Zlatintsi A., *"COGNIMUSE: a multimodal video database annotated with saliency, events, semantics and emotion with application to summarization,"* Eurasip J. Image Video Process., vol. 2017, no. 1, pp. 1–24, 2017.

Wingo, J. (2017) Personal interview as the USAF Cyberspace Operations Officer Career Field Manager. Used with permission. 22 December 2017.

Yannakogeorgos, P., Geis, J. (2016) *The Human Side of Cyber: Organizing, Training, and Equipping the Air Force Cyber Workforce*. Maxwell AFB, AL: Air University Press.

YouTube. [Online]. Available: https://www.youtube.com/yt/about/. [Accessed: 01-Jan-2018].

Attachment 1 – Python Code

1. ping.py – This code pings the router and records the results to a text file, as well as updates the status LED on the Pi.

```
import RPi.GPIO as GPIO
import socket
import os
import time


ROUTER_IP = "192.168.1.1"


def check_ping(ip):
    return_str = ""

    # GPIO Setup:
    RED = 20
    GREEN = 16

    # Socket Stuff:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    rep = os.system("ping " + ip + " -c 3")
    if rep == 0:    # Working
        s.close()
        ledState = True
        return_str += "{}, - Working at,{},\n".format(ip, time.time())
    else:         # Not Working
        s.close()
        ledState = False
```

```
27.         return_str += "{}, - No Response at,{},\n".format(ip, time.time())
28.     GPIO.output(GREEN, ledState)
29.     GPIO.output(RED, not ledState)
30.     time.sleep(2)
31.     return return_str
32.
33.
34. if __name__ == '__main__':
35.     RED = 20
36.     GREEN = 16
37.     ledState = False
38.     GPIO.setmode(GPIO.BCM)
39.     GPIO.setup(RED, GPIO.OUT)
40.     GPIO.setup(GREEN, GPIO.OUT)
41.     GPIO.output(RED, True)
42.     GPIO.output(GREEN, ledState)
43.     while(True):
44.         results = open("results.txt", 'a')
45.         hostnames = ROUTER_IP
46.         myPings = check_ping(hostnames)
47.         results.write(myPings)
48.         #print(myPings)
49.         results.close()
```

4. python_startup.py – This code checks to see if the record file already exists at the start of the program. If so, it saves off the old file and creates a new one. This allows

the researcher to identify times at which the Pi was rebooted and ensures continuity of data recording.

```
1.  import os
2.  i = 0
3.  while os.path.exists("results%s.txt" % i):
4.      i += 1
5.  command = "results%s.txt" % i
6.  command = "cp results.txt " + command
7.  os.system(command)
8.  os.system("rm results.txt")
```

Attachment 2 – Participant Instructions

Thank you for participating in this challenge!

Your job is to secure this **wireless** network by ensuring that only the three devices that we want on the network are able to connect to the **router**. The security feature you're trying to implement is called an "**access list**".

As you can see, there are 6 tiny computers (called Raspberry Pis) on the tower in front of you. Each one has an LED on the side labeled "**Status**" that will tell you if they can talk to the router (there is another LED pair on a different side of the computers, this is just for power. Be sure you're looking at the "Status" LED). The top three represent unauthorized devices. The bottom three represent authorized devices. When you are successful, the LEDs will be:

- Red
- Red
- Red
- Green
- Green
- Green

They will start all off green (because right now, any device can connect to the network). There are several other issues with the security of the router, but your job is *only* to implement the access list on the wireless network.

The MAC addresses of the three authorized devices are:

- B8:27:EB:CC:D6:CE
- B8:27:EB:7C:50:B3
- B8:27:EB:EA:F5:68
- All other devices are unauthorized

You have two laptops. One is the "**Network Terminal**". This laptop is connected to the "**Router**" and will allow you to configure the router. The router has a username and password. We don't remember what they are, but they are still set to the default credentials.

The other is the "**Open Internet Terminal**". This laptop is connected to a regular Internet connection, and you can use it to access any resources that will help you complete the challenge.

How to interact with the network:

- If you need to reboot the router, use the "<**Power**" button to turn it off, then on again.
- If you need to factory reset the router (undo all changes), use the "**Reset Tool**" on the "<**Factory Reset**" button for 10 seconds. The router will take **70 seconds** to reset**.**
- After applying any new settings to the router, it may take up to **70 seconds** to apply them and for the LEDs to update. The status LEDs may change color during stabilization (all will turn red, then the ones that can connect will change to green once 70 seconds elapses).
- If the LEDs don't illuminate as expected, try rebooting the tiny computers using the red "**Pi Power**" switch
- Don't connect or disconnect any cables or use any buttons other than the ones mentioned and labeled.

- If you need to reboot either terminal laptop, please notify the researcher you're rebooting the laptop so they can save and restart the recording software.

You have 3 hours to complete the challenge, but may quit at any time if you wish.

You may now begin. Please turn on the "**Network Reboot Switch**" to begin.

Attachment 3 – Pre-Experiment Questionnaire

Pre-Experiment Questionnaire

How would you characterize your knowledge of computer network configuration?

Response items: Very Poor, Poor, Fair, Good, Very Good

How would you characterize your knowledge of Internet based learning platforms?

Response items: Very Poor, Poor, Fair, Good, Very Good

Have you ever attempted to or successfully implemented MAC address filtering on a network?

Response items: Yes, attempted. Yes, succeeded. No. I don't know.

What sort of electronic devices do you use?

Response items:

Personal computer/Desktop/Laptop

TV/Game Console

Smartphone/Tablet

Enterprise Server

Other, please list _____

How often do you use electronic devices?

Response items: Daily, A few times a week, Once a week, Never

Do you use electronic devices in your job?

Response items: Yes, No, Prefer not to answer

Do you have any cyber security experience?

Response items: Yes, No, Prefer not to answer

Have you earned any cybersecurity certifications?

Response items: Yes, No, Prefer not to answer

If yes:

Please list any cyber security certifications you have earned:

_____

_____

_____

What's your highest education level?

A. Lower than high school
B. Graduated from high school
C. Some college, no degree
D. Associate's Degree
E. Bachelor's Degree
F. Master's degree
G. Ph.D. degree

Do you have any reason(s) to believe that your ability to accomplish tasks during this study (including learning about and implementing a network configuration) today would be abnormal (for example: you had a job as a network admin, or extensive experience with a network configuration management in the past; today you were distracted, overly tired, hungry, stressed, injured)? _____

If yes:

Do you still want to participate in the cyber study today? (Yes / No)

If participant doesn't want to complete experiment today:

Would you like to reschedule participation for another day?

If participant does want to complete the experiment today:

Describe the reason(s) which may make your ability to accomplish these tasks abnormal: (open-ended response)

Attachment 3 – Implied Solution as shown in Modified Netgear Webpage

How to configure Access Control or MAC Filtering (Smart Wizard routers)

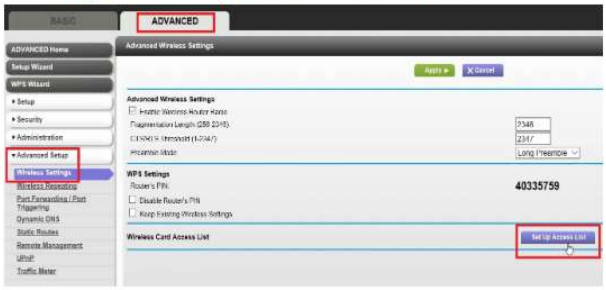
Was this article helpful? Yes No | 9 people found this helpful in last 30 days

Once your network is secured with an encrypted password, you can increase security by restricting access to your network to a set of devices on the Wireless Card Access List. Once you enable the Access List, wireless devices that are not on the list will **not** be allowed to join your wireless network.

Note : This article describes the setup of the access control feature on older NETGEAR wireless routers. For newer routers with the genie user interface, see Configure Access Control / MAC Filtering using genie

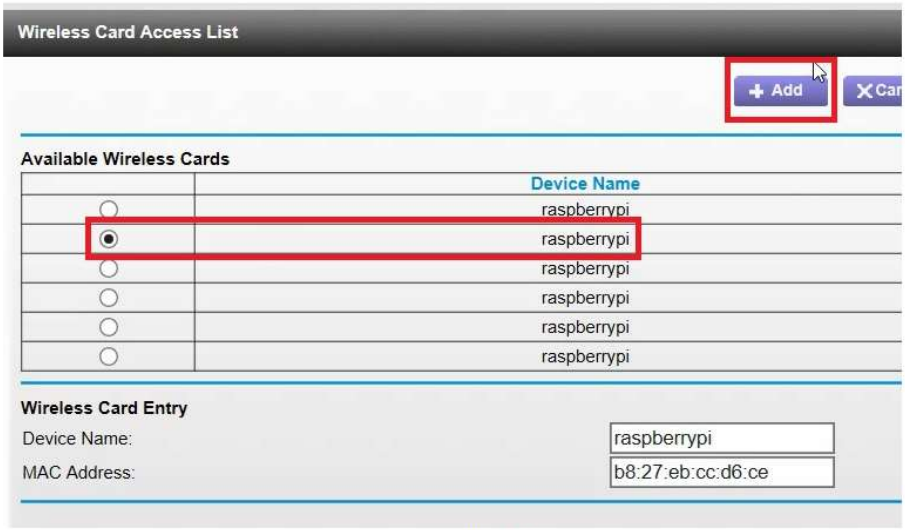
To configure Access Control or MAC filtering with Smart Wizard:

1. Use an Ethernet cable to connect a computer to any one of the four LAN ports of the NETGEAR router.
2. In a web browser, enter the router IP address, either **http://192.168.0.1** or **http://192.168.1.1** by default.
   If these IP addresses are not working, see How do I login to my NETGEAR home router?
3. When prompted for a username and password, enter the username and password. The default username and password are **admin** and **password**, respectively.
   NETGEAR recommends changing the default password to increase the security of your network.
4. On the top tabs, select **Advanced**
5. On the left toolbar, select **Advanced Settings** > **Wireless Settings**.
6. Click **Set Up Access List** to open the Wireless Card Access List.

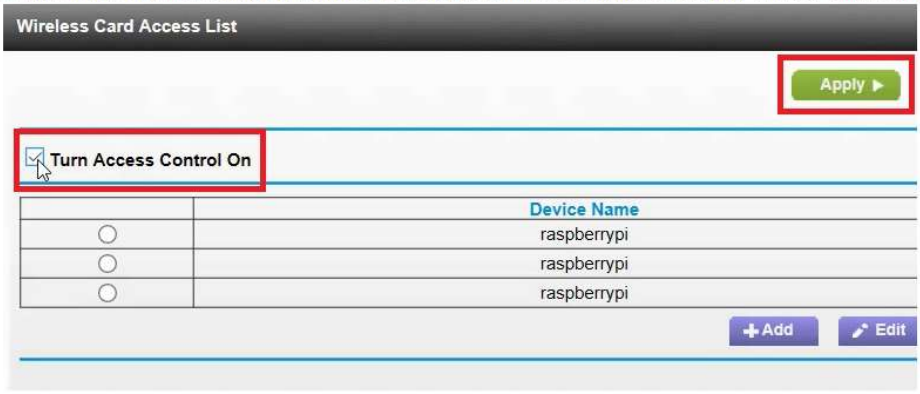


7. The current access list is displayed. To add devices to the access list, click **Add**.

8. If the device that you want to allow to connect wirelessly is not listed, you can add it manually.
   You will need to know the MAC address, see How to find a computer's MAC Address
9. Either select the radio button for the device you'd like to add, or enter a descriptive name for the computer into the **Device Name** field and enter the computer's MAC address into the **MAC Address** field,
10. Click **Add**.



11. Repeat these steps to add all approved wireless clients to the allowed list.
12. When you have completed adding all the wireless MAC addresses allowed to connect to wirelessly with your router, select **Turn Access Control On**.



13. Click **Apply**. Your settings are saved and only the wireless clients with MAC addresses listed will be allowed to connect to your router.
14. You may need to power cycle the router and/or power cycle the devices in order to fully implement the MAC filter

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
21-03-2019	Master's Thesis	August 2017 - March 2019

4. TITLE AND SUBTITLE
Unguided Cyber Education Techniques of the Non-Expert

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Martin, Seth A., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
Wright-Patterson AFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENG-MS-19-M-041

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release: Distribution unlimited.

13. SUPPLEMENTARY NOTES
This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The United States Air Force and Department of Defense continues to rely on its total workforce to provide the first layer of protection against cyber intrusion. Prior research has shown that the workforce is not adequately educated to perform this task. As a result, DoD cybersecurity strategy now includes attempting to improve education and training on cyber-related concepts and technical skills to all users of DoD networks. This paper describes an experiment designed to understand the broad methods that non-expert users may use to educate themselves on how to perform technical tasks. Preliminary results informed subsequent experiments that directly compared frequently utilized, but flawed resources to improved versions of those resources to determine preferable educational methods. This paper provides the protocol and population characteristics for both phases of the experiment, results from phase one, and preliminary results from phase two. In a related effort, the Air Force Institute of Technology is designing and implementing an online learning platform for centralizing a variety of cyber-educational materials. This platform is built on prior groundbreaking research understanding how people, especially young people, learn best in the modern era. This thesis

15. SUBJECT TERMS
Cybersecurity, education, human factors

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Lt Col Mark A. Reith, AFIT/ENG
U	U	U	UU	91	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636 x4603 mark.reith@afit.edu

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.