Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 2 Article 5

February 2022

# Faculty and Advisor Advice for Cybersecurity Students: Liberal Arts, Interdisciplinarity, Experience, Lifelong Learning, Technical Skills, and Hard Work

Brian K. Payne
*Old Dominion University*, bpayne@odu.edu

Bria Cross
*Old Dominion University*, bcross@odu.edu

Tancy Vandecar-Burdin
*Old Dominion University*, tvandeca@odu.edu

# Faculty and Advisor Advice for Cybersecurity Students: Liberal Arts, Interdisciplinarity, Experience, Lifelong Learning, Technical Skills, and Hard Work


## Abstract

The value of academic advising has been increasingly emphasized in higher education. In this study, attention is given to the most significant types of advice that a sample of cybersecurity faculty and advisors from the Commonwealth of Virginia recommend giving to cybersecurity students. The results show that faculty and advisors recommended that students be aware of six different aspects of cybersecurity education including the value of experience, the need for lifelong learning, the importance of hard work, the need to develop technical skills, the interdisciplinary nature of cybersecurity, and the need to develop liberal arts or professional/soft skills. Implications of the findings include the need to embrace the advising of cybersecurity students, the importance of helping cybersecurity faculty and advisors deliver effective advising, and recognition that good advising is more than simply telling students which classes to take.



## Keywords

cybersecurity advising, mentoring, training

## Cover Page Footnote

This research is supported in part by the National Science Foundation under grant DGE1914613 and the Commonwealth Cyber Initiative.

# Faculty and Advisor Advice for Cybersecurity Students: Liberal Arts, Interdisciplinarity, Experience, Lifelong Learning, Technical Skills, and Hard Work

## Introduction

Dolly Parton once said, "If you don't like the road you're walking, start paving a new one." On the surface, the value of this comment may seem to be the message it conveys. Who could argue with the point that individuals should make decisions that would change their future options if they do not like their career paths? Imagine a cybersecurity major, for example, who indicates that they do not like their major. Surely it would make sense to have them consider other potential majors (Liu et al., 2020; Malgwi et al, 2005). Besides the practical utility of Dolly's quote, it also seems worth delving deeper into the nature of providing advice in the first place. Indeed, the very provision of advice is worthy of academic interest.

Several studies have explored advising. These studies have helped to shape our empirical understanding of the process of advising (Gortney et al., 2020; Loucif et al., 2020), its purposes (Alvarado & Olson, 2020; Bridgen, 2017), and its consequences (Zarges et al., 2018). Indeed, these studies have helped to shape what some have called an academic discipline or scholarship of advising (Troxel, 2018). Many areas of advising have been worthy of academic pursuit and these studies have provided useful insight into various dimensions of advising. Among other things, researchers have shown that advisors are expected to fulfill many different roles (Mier, 2018), faculty advisors face technological barriers and unclear expectations (Hart-Baldridge, 2020), and knowledge about advising improves the success of advising (Dillon & Fisher, 2000). Despite this growth in advising research, fewer studies have considered the specific types of advice given to students and, more specifically, advice that faculty and students would give to cybersecurity students. To fill this gap in the literature, this study explores the types of advice defined as the most important by cybersecurity faculty and advisors. Understanding the types of advice that faculty and advisors would give cybersecurity students has important implications for student success.

## Review of Literature

The majority of cybersecurity education research has focused on the strategies used to educate cybersecurity students. The past research has been valuable in shaping our understanding about teaching practices (Konak, 2018; Giannakas et al., 2015; Rege, 2019), learning styles (Chao et al., 2019; Kam et al., 2020), and curricular content (Mountrouidou et al., 2019; Taylor et al., 2017). Less research has considered aspects of advising as they relate to cybersecurity students' experiences. To fully understand the need to examine cybersecurity advising, a

review of the definitions of advising and the functions of advice is provided. Integrated into the discussion are themes merging advising literature with the cybersecurity education experience.

**Conceptualizing Cybersecurity Advising**

As one author notes, offering advice to students "is not a new phenomenon" (Stebleton, 2019, p. 163). From the days of Socrates advising Plato to today, learners have long looked to others for advice and mentoring related to their subjects of interest. While advising has been a mainstay of the learner/teacher relationship, the importance of advising has not afforded the level of significance warranted. In the words of one author, "good advising may be the single most underestimated characteristic of a successful college experience" (Light, 2001, p. B11).

Part of the reason that advising is not given the attention it warrants stems from varied definitions of advising. Consider the following definitions:

- "Academic advising is the process of advising students about the necessary classes and their sequence that should be taken to fulfill their collegiate graduation requirements" (Fisher et al., 2011, p. 45)
- "Academic advising is the process of selecting classes, to be taken by the student in the incoming semester" (Kowalski et al., 2008, p. 949)
- "Academic advising can be defined as an ongoing process, a dynamic relationship involving the academic advisor as the facilitator of communication, and helps students use educational institutions' resources to meet their special needs and aspirations" (Junita et al., p. 131).
- "Academic advising is defined as the process of assisting students with defining, clarifying, and planning their education and future" (Mondo, 2020, p. 125).
- "Academic advising [refers] to situations in which an institutional representative gives insight or direction to a college student about an academic, social, or personal matter" (Kuhn, 2008, p. 3).
- "Academic advising involves engaging students to think critically about their academic choices and make effective plans for their educations" (Schulenberg & Lindhorst, 2008, p. 43).

With so many different definitions of advising, it may be difficult to arrive at a succinct definition of the concept. However, when reviewing the above conceptualizations of advising, it seems that one commonality exists across all approaches. In particular, at its core, advising can be defined as the process of giving advice. For cybersecurity students, the advising process entails giving students advice that (1) teaches them about cybersecurity, (2) helps students select courses, (3) supports decisions about the various types of careers available in the

cybersecurity field, (4) better prepares them for among the half million cybersecurity jobs available (Cyberseek.org, 2021), and (5) develops students as mentees.

## Functions of Advising

Cybersecurity advising serves multiple purposes for students, institutions, and the community. Certainly, students benefit the most from successful academic advising. Four areas where students gain from advising include course preparation, major selection/confirmation, knowledge acquisition, and career preparation.

Regarding course preparation, as noted above one of the purposes of advising is to help students select the right courses (Fisher et al., 2011). Depending on the cybersecurity curriculum and student backgrounds, course selection is not always straightforward. Because they are familiar with stated and unstated prerequisites, advisors are able to help steer students into courses they are best prepared for. This is particularly important for cybersecurity courses that may have varying math or computing requirements. Enrolling in courses they are unprepared for will most certainly reduce the cybersecurity student's likelihood of succeeding in those courses.

A second function of advising is major selection/confirmation. The connections between major selection and advising are twofold: advisors help students decide what major to select initially and they help students decide whether to change their majors (Jaradat and Mustafa, 2017). The importance of this process cannot be understated for cybersecurity major selection. With the field of cybersecurity evolving, and students having little exposure to cybersecurity in high schools or from their parents, their decision to select cybersecurity may rest in large part on the advice they receive from advisors or others fulfilling an advising role. While advisors are in positions to help *new* students select cybersecurity as a major, given that more than half of all undergraduate students are believed to change their major (Marede & Brinthaupt, 2018), advisors are also in positions to help *current non-cyber students* change their major to cybersecurity.

A third function of advising is knowledge acquisition. Put simple, students can learn a great deal through the advising process. The phrase "advising as teaching" is used to characterize the way that students learn from advising. Looking at scholarship pointing to how advising helps to develop students (Crookston, 1972), the advising as teaching model defines advising as more than a service provided by advisors and faculty. Consider, for example, a survey of 611 students that concluded, "academic advising can vitally impact all facets of a student's academic experience, ranging from development of self-efficacy to practical applications of study skills." (Young-Jones et al., 2013, p. 15). Within this framework, advising is seen as a relational process that helps students grow. The advising process teaches

students about more than which courses to take and presumably helps students learn skills that will help them in their courses and in their subsequent careers. Those who point to the "advising as teaching" model hold that "effective advisors are also effective teachers" (Appleby, 2010, p. 3). Relative to cybersecurity, one might add that advisors have knowledge beyond cybersecurity-specific knowledge that can be shared with students through the advising process.

Career preparation is another function of advising which goes beyond simply advising about career selection. Instead, advising, when done well, should help to give students the tools they will need to thrive in their future careers. One author writes that advising should "encourage students to acquire human capital—the skills that will make them efficient and productive in the workplace. The primacy of acquiring human capital and skill development is also premised on the observation that the average American switches careers several times in their lifetime" (Atuahene, 2021, p. 80). Human capital refers to professional skills, such as communication, teamwork, and problem solving, that would serve students in multiple careers. There is no reason that cybersecurity graduates would be any different than others in terms of career switching. In fact, with so many careers in cybersecurity, and the field constantly changing, it is plausible that there will be even more opportunities for career switching in cybersecurity in the years to come.

Besides benefitting students, advising also serves important functions for academic departments and institutions. In recent years, funding for public institutions have been increasingly connected to retention, progression, and graduation rates. Research consistently shows that effective advising can improve student success, which subsequently enhances retention, progression, and graduation rates and funding stability (Glennen et al., 1996; Thomas & McFarlane, 2018). At the same time, the close one-on-one interactions that advisors have with students provides an opportunity for the department to learn about its curriculum. Students will share all sorts of information with advisors – whether courses are offered frequently enough, whether the prerequisites are appropriate, which teaching strategy works best, and so on. Of course, anecdotal comments from students during advising should not be the sole source of data for decision making. However, this informal feedback gives the department and institution information that can be considered for further review.

The community-at-large also benefits from effective advising. Since advising improves student success, the community benefits from a better prepared workforce. Further, given the way that advisors help students select the majors, they also have a role in shaping the size and diversity of the workforce. With many calls for increasing the diversity of the cybersecurity profession, it seems that advisors may, in fact, be one of the keys to helping to improve diversity and inclusion in the cybersecurity workforce.

By its very nature, advice is intended to improve the outcomes of those receiving the advice. It is common to ask experts about advice they have for students (see Ackerman, 2020; Patel, 2020; Tan, 2020; Wilkins et al., 2019), though fewer studies have focused on advice that experts have specifically for cybersecurity students, perhaps partly because of the comparative novelty of the cybersecurity profession. Assessing the types of advice that advisors and faculty would give cybersecurity students has important implications for the field. In particular, such advice can serve as a model for future cybersecurity learners.

## Methods

Cybersecurity faculty and advisors who work with cybersecurity students at four-year institutions and the community colleges in the Commonwealth of Virginia were invited to participate in a web-based survey in the 2020 fall semester. To recruit cybersecurity faculty, we used a non-random purposive sampling strategy seeking to acquire input from individuals we anticipated would be familiar with cybersecurity advising. Specifically, emails were sent through contacts at the Commonwealth Cyber Initiative, an initiative promoting cybersecurity research and workforce development throughout Virginia. To recruit the advisors, emails were sent to advising contacts across the Commonwealth. Those receiving the emails were asked to share the invitation with other cybersecurity faculty and advisors.

A total of 75 faculty/advisors participated. About one in five respondents (21.6%) were advisors and 78.4% were faculty. The amount of time respondents had been working in this role ranged from 2-400 months. Faculty and advisors were asked to provide the single most important piece of advice they could give to cybersecurity students. In this context it was assumed that the faculty were responding as faculty advisors and the advisors were responding as professional academic advisors.

Responses to the question about the single most important piece of advice were content analyzed using standard rules of latent and manifest content analysis. This entailed reading the comments and categorizing them according to themes and patterns that arose from their comments. This type of qualitative methodology is helpful in many different types of social science research studies. It is also important to note that qualitative methods are increasingly embraced in cybersecurity studies (Fujs et al., 2019).

## Findings

The content analysis revealed six themes regarding the single most important piece of advice that the respondents would give to students. These themes included

experience, liberal arts, lifelong learning, interdisciplinarity, work ethic, and technology. Each of the themes are addressed below.

**Theme 1: Experience**

Faculty and advisors both equally agreed that students having experience is important when it comes to majoring in or pursuing a career in cybersecurity. Experience is important because it shows that students are able to actually apply the knowledge that is being learned outside of the classroom setting. Faculty members and advisors suggest that having experience will allow students to gain education and training along with the experience. One respondent highlighted the importance of focusing on the connections between these areas stating, "Education, Experience and Training (Certifications) are the keys to success in the cybersecurity career - be sure a good balance."

When considering experience, other respondents also focused more on the value of certifications. Here are a few comments respondents made about the value of credentials:

- Earn as many credentials as you can along with your degree.
- Get certified
- Invest in completing and passing certification exams.

Respondents also highlighted the importance of building connections and relationships with those in the field as important to students' success in the cybersecurity field. One respondent advised students to "Get hands on experience and connect with a potential future employer." These comments were echoed by another respondent who suggested that students "Spend time in networking with other folks in the field. Take advantage of internships, clubs, and, and organizations in your area." A third respondent pointed to the importance of connections in the educational institution and outside the institution telling students "To remain connected to faculty and organizations in the field."

**Theme Two: Liberal Arts**

In addition to focusing on experience and connections, faculty and advisors advised that students having the basic knowledge or foundational skills related to liberal arts. In particular, they suggest the importance of emphasizing liberal arts or critical thinking perspectives when it comes to communicating and forming relationships with individuals in the field. One respondent addressed it this way*:* "People skills will make or break a career. In your career, 75% of long-term job success depends on people skills, while only 25% on technical knowledge." As an example of the people skills, another respondent advised students to "Always communicate, with fellow teammates, faculty and advisors." In terms or communication, some respondents encouraged students to ask questions advising

students to "Listen well and ask clarifying questions" and "Be curious and ask questions and constantly be ready to learn on a daily basis."

Other comments related to the liberal arts theme often included recommendations that students enhance their analytical, critical thinking, and problem-solving skills. For instance, one respondent said that students should "Pay attention to detail and make sure you are able to communicate clearly to those you work with and for." Others were more succinct and offered suggestions such as "[pay] attention to detail and critical thinking," "learning critical thinking skills," and "Develop problem solving and communications abilities." As will be shown below, these skills relate to lifelong learning in that they are skills that would be helpful throughout the cybersecurity student's entire career, or careers if they change careers.

**Theme Three: Lifelong learning**

Another theme that surfaced is lifelong learning. Respondents noted that students should realize that cybersecurity is a field requiring a commitment to continuing education. One respondent advised students to "Always continue learning and practicing," while another said, "Continue to learn - you can't stop once out of school; Continue to learn, read, study, and grow; It is a never ending learning process due to constant change; Prepare for life long learning." Grounded in this theme of lifelong learning were ideals of passion and commitment. Consider the following comments from two respondents:

- Always seek out knowledge. You don't have to know everything in cyber. You need to be resourceful and know where those resources are. Seek out those you work with and ask questions when you do not know or understand something. Always be humble. Education is a life long journey and you should seek out every opportunity to learn new things each day.
- To be totally passionate about this as a career, not just a job. To make a commitment to cybersecurity as a lifelong learning process knowing that the technology changes as fast or faster than they can learn.

Some focused on the need to stay current as part of the lifelong learning process. For example, one respondent remarked, "This field is nebulous and constantly evolving and many degree/training programs reflect this." Others advised students "To stay on top of changes in the market and make sure you relate content to everyday living" and "Stay current on trends in intrusion and protection." Another respondent explaining the need for being current and emphasized, "Keep in mind that the cyber hacker never sleeps and will constantly try a new approach until successful, thus this field is always changing." The constant changing nature of cybersecurity stems, in part, from the interdisciplinary nature of the field which balances many different technological and social science fields.

**Theme Four: Interdisciplinarity**

A fourth theme that surfaced was interdisciplinarity. While somewhat related to liberal arts, the notion of interdisciplinarity encourages balancing both technological and social dimensions of cybersecurity. Respondents made comments that emphasized the need to think broadly about cybersecurity. It is important to note that just one respondent actually used the academic term related to interdisciplinarity. This respondent offered as the single most important piece of advice this bit of wisdom: "Be interdisciplinary." While not using the word interdisciplinary, another respondent focused on disciplinary themes and suggested the following: "Understand that cyber threats are not only a technical challenge, but a human problem. They need to be able to work with professionals from other *disciplines* to reduce the organizational cyber risk effectively" (italics added).

Others made reference to needing to know about topics other than cybersecurity. For example, one respondent advised students to "Develop skills beyond technical skills" and another said, "Understand the businesses needs and how to apply security to them." In a similar way, a respondent advised students to "learn how to design, implement, and evaluate your computing solutions considering both technical and non-technical stakeholders." Two other respondents provided detailed advice that appear to be grounded in ideals of interdisciplinarity. These included:

- My approach to teaching is that good cyber hygiene is everyone's business. In non-cyber classes I discuss cyber threats as they relate to the current topic being taught (i.e. a lecture on the Internet, I will discuss the importance of changing default accounts on home routers, how to recognize phishing, and several other security related topics). I recognize and constantly stress attention to detail which is crucial in all aspects of life but especially in the IT/cyber security realm.
- While your technical/computer skills are valuable, they will only get you to a certain point. To reach management level positions, you must develop your verbal, written, and presentation skills. You must also be a consummate reader. Lastly, understand that the problems you are asked to solve are complex, and you will rarely have all the knowledge to accomplish the task. Therefore, you must understand how to work on teams that leverage the collective knowledge of the group.

**Theme Five: Work Ethic**

The interdisciplinary focus identified by the respondents was bolstered by the respondents' suggestions that it is crucial for students to have a hard work ethic in the field of cybersecurity. Some were direct in highlighting the importance of a strong work ethic, making comments such as:

- Students having a hard work ethic can only set themselves up to be successful and become the best version of themselves in cybersecurity.
- Go the extra mile.
- You need to have a strong work ethics with solid cybersecurity technical skills; Increase knowledge in the area of software and hardware.
- Work diligently; Work hard, ask questions, think through problems, and know what you don't know.

Others made comments inferring the value of a hard work ethic. Consider the advice offered by the following three respondents:

- Have a passion for solving complex puzzles and do not get discouraged by mundane tasks; Never give up on a problem or solving a vulnerability
- That it is a competitive field, but one that will only grow with the interconnection of the global economy. You are not just working to pass your classes but are competing with every other cyber security student for a potential job once you have completed your degree.
- You get out of the program what you put in. If you do the bare minimum you will receive the bare minimum. If you strive to do more you will achieve more.

**Theme Six: Technology**

While respondents commonly described the above themes as important, some also highlighted the importance of knowing about technology. The constantly changing nature of technology does not mean that students need to know about specific technologies; rather, the implication is that students need to know the basics of technology and they need to have the skills to learn about technology. One respondent advised that students need a "solid understanding of computer hardware and software" and another recommended "Learn as much technical content and computer science foundation as you can. Also, thoroughly understand how to set up a complete network. You can use that to build on."

Some respondents integrated technology with other types of advice when identifying their single most important piece of advice. For instance, one respondent indicated that they would advise students to "Start with a strong technical background and apply sound analytical skills [and] Continuously learn and refresh your skills and experiences with new technologies and new vulnerabilities." Another respondent similarly stated the following: "The cybersecurity field needs individuals with the drive to effectively protect information systems and enterprise computing platforms. Students need good technical skills coupled with a desire for further knowledge and understanding of protective security measures." A third respondent agreed advising students to "Get an internship, get hands-on experience, and hard technical skills."

## Discussion

These findings identified six different themes that captured the most significant pieces of advice faculty and advisors would give to students. Faculty members and advisors stressed the importance of students gaining as much experience as they can while pursuing degrees in cybersecurity. From this perspective, the higher education cybersecurity experience is more than just learning the material inside of the classroom. Instead, the implication from our findings is that successful cybersecurity students must utilize and expand resources, networks, training, and skills outside of the classroom. At the same time, the faculty and advisors highlighted the importance of a broad interdisciplinary education that balanced technical skills and liberal arts skills and embraced lifelong learning. Collectively, several important implications stem from our findings.

To begin, it is important to note that the advice had very little to do with telling students what courses to take. As noted earlier, narrow definitions of advising tend to emphasize that advising is helping students pick their courses. Such definitions undervalue the true importance of advising (Sabay and Wiles, 2000). If faculty, advisors, and administrators follow a shallow definition of advising, they risk failing to meet students' needs. For cybersecurity students in particular, it seems important to stress that advising should not be simply characterized as course selection.

In defining cybersecurity advising, one can point to two underlying themes that cut across the themes identified in this study. First, when considering the value of experience, lifelong learning, a hard work ethic, and liberal arts skills, the theme of social development arises. So, rather than telling students what classes to take, when asked to provide advice to students, faculty and advisors provided information that would help students to develop as students and professionals. Second, when considering the ideals of interdisciplinarity and technical skills, in many ways the respondents were drawing attention to the way that "advising is teaching." Combining these ideas together, it might be suggested that cybersecurity advising is teaching students about the skills they will need to succeed as students and future professionals.

On a related point, it is important that cybersecurity faculty and advisors recognize the value of the advising they provide their students. Because advising is underappreciated in many areas (Harrison, 2009), it is possible that some faculty may not be providing students the level of advising that would most effectively promote student success. Others have noted that professors receive little training about how to teach while they are in graduate school (Allgood et al., 2018). It seems also important to note that faculty likely receive little training about how to advise undergraduates while they are in graduate school.

Tied to the need to broadly define advising and to make sure that faculty are prepared for the advising process, it is equally important that administrators embrace the value of advising as well as the value of faculty and advisor perspectives (Dillon and Fisher, 2020). As our research shows, faculty and advisors have useful insight to provide when asked to provide advice for cybersecurity students. For advising to be appropriately resourced and rewarded, university administrators must be willing to lead as student success advocates.

It is also important to recognize the broad conceptualizations of cybersecurity offered by the faculty and advisors. The themes of interdisciplinarity, liberal arts, and technical skills draw attention to what is already known among cybersecurity scholars – the field is not easy to define. In this context, it is important that faculty and advisors help students to understand the broad interdisciplinary framework that is at the heart of cybersecurity. To some, cybersecurity is a part of computer science. To others, it is a part of computer engineering. And for some, it is a part of information technology. Others are increasingly recognizing that it is a field in its own right – one that draws upon these fields and other social science fields to educate students about technical and social strategies that can be used to secure cyberspace. In this context, it is important to note that the advising process is one part of the educational process where students can learn how to define cybersecurity.

Another important implication stemming from our findings has to do with the fact that no single piece of advice surfaced as the key ingredient to succeeding as a cybersecurity student. There is no magical silver bullet to success in cybersecurity, just as there is no silver bullet for succeeding in any academic major. Still, certain aspects of the advice were possibly unique to cybersecurity students. In particular, the focus on balancing technical skills and liberal arts skills within an interdisciplinary framework that values experience and lifelong learning seems to distinguish the kind of advice that one might give to a cybersecurity student versus students in the pure social sciences and pure STEM fields. In addition, the need for lifelong learning – which applicable to many different majors – takes on a different meaning when considering the interdisciplinary nature of cybersecurity. Also, while the value of liberal arts may be clear for certain types of academic majors, it's relevance to cybersecurity majors may need to be more clearly articulated.

**Limitations**

Our research is not without limitations. For example, our purposive sampling strategy meant that we only received responses from those who were truly interested in answering questions about cybersecurity education. In some ways, selection bias may have resulted in receiving responses from those faculty and advisors most willing to help. In addition, we focused on faculty and advisors in

one state, our findings might have been influenced by statewide factors related to either cybersecurity or the state culture of advising.

### Future Research

Despite these limitations, a number of questions arise for further research. Researchers should explore the most appropriate ways to advise cybersecurity students so they receive the most important components of advice. In addition, researchers should explore how advising cybersecurity students might vary from advising other types of students. Also, researchers should explore the most effective ways to prepare faculty and advisors to advice cybersecurity students.

The last avenue for future research is particularly important given the relative newness of the cybersecurity field. Because is it different from other fields, it is possible that the cybersecurity advising process has features that are unique to cybersecurity education. Another quote from Dolly Parton comes to mind, "I don't like to give advice, I like to give people information because everyone's life is different, and everyone's journey is different." Every discipline is different and one cybersecurity student's journey will be different from another's. It is critical that we understand those differences so we can best educate the future cybersecurity workforce.

## Acknowledgements

This research is supported in part by the National Science Foundation under grant DGE1914613 and the Commonwealth Cyber Initiative.

## References

Ackermann, S. (2020). The time I live in, and the work of Shyama Golden. *Art Education*, *73*(4), 48-54.

Allgood, S., Hoyt, G., & McGoldrick, K. (2018). Teacher training for PhD students and new faculty in economics. *The Journal of Economic Education*, *49*(2), 209-219.

Alvarado, A. R., & Olson, A. B. (2020). Examining the relationship between college advising and student outputs: A content analysis of the NACADA Journal. *NACADA Journal*, *40*(2), 49-62.

Appleby, D. C. (2008). Advising as teaching and learning. *Academic advising: A comprehensive handbook*, *2*, 85-102.

Atuahene, F. (2021). An analysis of major and career decision-making difficulties of exploratory college students in a Mid-Atlantic University. *SN Social Sciences*, *1*(4), 1-22.

Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal*, *37*(2), 9-20.

Chao, H., Stark, B., & Samarah, M. (2019, December). Analysis of learning modalities towards effective undergraduate cybersecurity education design. In *2019 IEEE*

*International Conference on Engineering, Technology and Education (TALE)* (pp. 1-6). IEEE.

Crookston, B. B. (1972). A developmental view of academic advising as teaching. *Journal of College Student Personnel*, 13, 12-17.

Dillon, R. K., & Fisher, B. J. (2000). Faculty as part of the advising equation: An inquiry into faculty viewpoints on advising. *NACADA Journal*, *20*(1), 16-23.

Fujs, D., Mihelič, A., & Vrhovec, S. L. (2019, August). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-10).

Fisher, W. W., Barman, S., & Killingsworth, P. L. (2011). Value stream mapping for improving academic advising. *International Journal of Information and Operations Management Education*, *4*(1), 45-59.

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015, November). CyberAware: A mobile game-based app for cybersecurity education and awareness. In *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)* (pp. 54-58). IEEE.

Glennen, R. E., Farren, P. J., & Vowell, F. N. (1996). How advising and retention of students improves fiscal stability. *NACADA Journal*, *16*(1), 38-41.

Gortney, J. S., Lahiri, M., Giuliano, C., Saleem, H., Khan, M., Salinitri, F., & Lucarotti, R. (2020). Evaluation of an instrument to assess students' personal and professional development during the faculty advising process. *American Journal of Pharmaceutical Education*.

Harrison, E. (2009). Faculty perceptions of academic advising: "I don't get no respect". *Nursing Education Perspectives*, *30*(4), 229-233.

Hart-Baldridge, E. (2020). Faculty advisor perspectives of academic advising. *NACADA Journal*, *40*(1), 10-22.

Jaradat, M. S., & Mustafa, M. B. (2017). Academic advising and maintaining major: Is there a relation?. *Social Sciences*, *6*(4), 151.

Junita, I., Kristine, F., Limijaya, S., & Widodo, T. E. (2020). A study of undergraduate students' perception about academic advising in an Indonesian university. *Humaniora*, *11*(2), 131-137.

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, *96*, 101875.

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 6.

Kowalski, K., Rodriguez, J. C., & Beheshti, M. (2008, November). Using XML in On-line Advising. In *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (pp. 949-954). Association for the Advancement of Computing in Education (AACE).

Kuhn, T. L. (2008). For the purposes of this chapter, academic advising will refer to situations in. *Academic Advising: A Comprehensive Handbook*, 3.

Light, R. J. (2001). The power of good advice for students. *The Chronicle of Higher Education*, *47*(25), B11.

Liu, V., Mishra, S., & Kopko, E. M. (2020). Major Decision: The impact of major switching on academic outcomes in community colleges. *Research in Higher Education*, 1-30.

Loucif, S., Gassoumi, L., & Negreiros, J. (2020). Considering students' abilities in the academic advising process. *Education Sciences*, *10*(9), 254.

Malgwi, C. A., Howe, M. A., & Burnaby, P. A. (2005). Influences on students' choice of college major. *Journal of Education for Business*, *80*(5), 275-282.

Marade, A. A., & Brinthaupt, T. M. (2018). Good and bad reasons for changing a college major: A comparison of student and faculty views. *Education*, *138*(4), 323-336.

Mier, C. (2018). Adventures in advising: Strategies, solutions, and situations to student problems in the criminology and criminal justice field. *International Journal of Progressive Education*, *14*(1), 21-31.

Mondo, C. B. (2020). Examining the practices and challenges of virtual academic advising in higher education during COVID-19. *The Journal of Student Affairs*, 124.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., ... & Yuen, T. T. (2019). Securing the human: a review of literature on broadening diversity in cybersecurity education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, 157-176.

Patel, P. (2020). Interview with Dr. Dawn Salvatore. *Gibbon Surgical Review*, *3*(1), 4.

Rege, A., Williams, K., & Mendlein, A. (2019, March). An experiential learning cybersecurity project for multiple STEM undergraduates. In *2019 IEEE Integrated STEM Education Conference (ISEC)* (pp. 169-176). IEEE.

Sabay, S., & Wiles, K. (2020). How Trio enhances equity for community college transfer students. *New Directions for Community Colleges*, *2020*(192), 109-119.

Schulenberg, J. K., & Lindhorst, M. J. (2008). Advising is advising: Toward defining the practice and scholarship of academic advising. *NACADA Journal*, *28*(1), 43-53.

Stebleton, M. J. (2019). Moving beyond passion: Why "do what you love" advice for college students needs reexamination. *Journal of College and Character*, *20*(2), 163-171.

Tan, X. T. (2020). The contemporary tax journal's interview with Mr. Steven K. Shee. *The Contemporary Tax Journal*, *9*(1), 10.

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017, April). Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1782-1789). IEEE.

Thomas, C., & McFarlane, B. (2018). Playing the long game: Surviving fads and creating lasting student success through academic advising. *New Directions for Higher Education*, *2018*(184), 97-106.

Troxel, W. G. (2018). Scholarly advising and the scholarship of advising. *New Directions for Higher Education*, *2018*(184), 21-31.

Wilkins, S., Neri, S., & Lean, J. (2019). The role of theory in the business/management PhD: How students may use theory to make an original contribution to knowledge. *The International Journal of Management Education*, 17(3), 100316.

Young-Jones, A. D., Burt, T. D., Dixon, S., & Hawthorne, M. J. (2013). Academic advising: Does it really impact student success?. *Quality Assurance in Education*.

Zarges, K. M., Adams, T. A., Higgins, E. M., & Muhovich, N. (2018). Assessing the impact of academic advising: Current issues and future trends. *New Directions for Higher Education*, *2018*(184), 47-57.