Cybersecurity Service Course at Radford University

Cole Daniels & Richard Joyce

Radford University

Radford, U.S.

Abstract:

This critique proposes the implementation of a cybersecurity awareness service course at Radford University designed specifically for non-technical students. As digital technologies become increasingly integrated into all aspects of personal and professional life, basic cybersecurity literacy has become essential for all university graduates, regardless of their field of study. Drawing from my dual background in Computer Science and Cybersecurity, this proposal addresses a critical gap in the current curriculum: the lack of accessible cybersecurity education for students outside technical disciplines. The proposed course would introduce fundamental concepts in cybersecurity, practical safety measures, and ethical considerations in a format accessible to students from all academic backgrounds. This critique evaluates the need for such a course through literature review, outlines potential learning outcomes, proposes lecture content, and presents an implementation timeline.

Literature Review:

The importance of cybersecurity awareness across disciplines is a well-documented discussion across academic literature. As of recent, it has become more of a conversation that securing systems includes and emphasizes the persons operating the system. The overarching goal of informing employees about various cybersecurity risks has become an extremely important concept in the workplace, no matter the role. This is ultimately due to the extreme implementation of technology in every career.

As discussed by Broadhurst et al. in [1], a quasi-experimental observation occurred at the Australian National University (ANU). This observation exposed 138 students to various forms of phishing attacks across several different platforms for a period of multiple months. A phishing attack is defined as the fraudulent practice of sending emails or other messages masked as a reputable sender in order to induce individuals to reveal personal information. This means that a person will receive an email saying they won a free trip to the Bahamas. Some instances of phishing are rather obvious the technologically literate individuals, however, there are various forms of phishing that can appear enticing to even the most informed of individuals. This study took place in an attempt to gauge the digital literacy of the college population at ANU. To elaborate on the various means of phishing, there are three in particular used in this study. There is generic phishing, tailored phishing, and targeted (spear) phishing. Each of these getting more and more specific to one person. In order to perform a spear phishing attack, research must be put into who the target is, and what kind of things they might be interested in signing up for. This process is also called social engineering, where someone attempts to befriend or act friendly towards the victim in order to gain extra information that would make the scam more likely to succeed.

The study found particularly significant data for our proposed course development. Most notably, they found that the overall complexity and specificity of the phishing attempts generated far more interaction from the user. To elaborate, it was found that the first year and transfer students suffered from dramatically more susceptibility than those in their later years of schooling. The underlying cause of this is almost impossible to attribute without more testing, but it could be hypothesized that the experience of being in an educational system and being exposed to conversations about cybercrimes occurred at an increased rate the longer someone has been in school. This is not a ridiculous concept as cybersecurity is becoming far more talked about, both in school and in the workplace. Students later into the degree would have likely experienced more of this conversation simply due to existing at that university for a longer period of time. Broadhurst et al. initiated the study by surveying the group and asking about their personal beliefs in their technologic literacy. With that said, 89.8% agreed that they would be able to spot the scams and ignore them accordingly. This is a ridiculously high number and can be a leading cause of susceptibility due to overconfidence. With that in mind, roughly 18 individuals actually fell for 0 scams. This means that while 89.8% said they would not fall for scams, in all actuality, that number was more like 13%. Ironically, the survey conducted after the study had concluded found that on average, individuals felt as if their IT literacy had increased. This is an incredibly concerning concept to me, and that is what fuels this idea of implementing a cybersecurity awareness service course.

Proposed Course Outcomes:

It is important to initially consider the desired knowledge gained throughout a course of this nature. With that being said, the proposed course outcomes would be as follows:

1) **Identify Common Security Threats**: Recognize phishing attempts, social engineering tactics, malware indicators, and other common security threats encountered in personal and professional contexts.
2) **Apply Basic Security Practices**: Implement fundamental security measures including strong password management, multi-factor authentication, secure data storage, and safe browsing habits.
3) **Evaluate Security Implications**: Assess the security and privacy implications of various technologies, applications, and online services before adopting them.
4) **Respond to Security Incidents**: Demonstrate appropriate response procedures when encountering potential security breaches or suspicious activities.

5) **Communicate Security Concepts**: Explain basic cybersecurity principles to peers and colleagues in clear, non-technical language.
6) **Recognize Legal and Ethical Dimensions**: Identify key legal regulations (such as GDPR, CCPA, HIPAA) and ethical considerations related to data privacy and security relevant to their field of study.
7) **Develop Security Mindfulness**: Integrate security awareness into daily technology use and decision-making processes.

If all of these outcomes are achieved, then the student would be well equipped to consider cybersecurity in their future endeavors, both school and career. This approach attempts to take into account various backgrounds that a service course would attract and then establish the connections between multiple thought processes about cybersecurity and all that is involved in the process. This approach also emphasizes applications of cybersecurity information rather than technical complexity.

Proposed Lecture Content:

The course would be structured throughout a full semester with lectures weekly along with practical exercises. It is important to note that the course would be worth three credits and graded as pass/fail. This is done in an attempt to promote outreach. The fear of being graded in a technical course might cause a lot of students to be turned away from the idea. Below is a proposed outline for what lectures might discuss:

Week 1-2: Foundations of Cybersecurity

- Introduction to cybersecurity concepts and terminology

- The cybersecurity threat landscape
- Why cybersecurity matters across all disciplines
- The human factor in security breaches

Week 3-4: Personal Digital Security

- Password management and authentication
- Secure use of personal devices
- Safe browsing and social media practices
- Protecting personal information online

Week 5-6: Social Engineering and Manipulation

- Recognizing phishing and social engineering
- Psychological aspects of security manipulation
- Case studies in social engineering attacks
- Practical defense strategies

Week 7-8: Data Privacy and Protection

- Fundamentals of data privacy
- Key privacy regulations and their implications
- Data collection practices and their consequences
- Tools and techniques for enhancing privacy

Week 9-10: Security in Professional Contexts

- Industry-specific security concerns
- Security in remote work environments
- Organizational security policies and compliance
- Professional responsibilities regarding security

Week 11-12: Emerging Technologies and Security

- Security implications of emerging technologies
- Internet of Things (IoT) security concerns
- Artificial Intelligence and security
- Future trends in cybersecurity

Week 13-14: Ethical Dimensions of Cybersecurity

- Ethical frameworks for security decisions
- Balancing security with accessibility and convenience
- Privacy as a fundamental right
- Security ethics across cultural context

Week 15: Review

- Discuss previous information.
- Answer questions that might have evolved throughout the semester.

Lecture Plans Week 1 & Week 2:

Week 1: Introduction to Cybersecurity Concepts and Terminology

Lecture Objectives:

- Define basic cybersecurity terminology (e.g., threats, vulnerabilities, exploits).
- Understand what cybersecurity is and why it matters to everyone.
- Recognize how cybersecurity connects to personal and professional life.

Lecture Outline:

1. **What is Cybersecurity?**
    - Definition: Protecting systems, networks, and data from digital attacks.
    - Cybersecurity vs. Information Security vs. Privacy.
2. **Core Concepts and Terms:**
    - Threats vs. Vulnerabilities vs. Risk.
    - Malware: viruses, worms, ransomware.
    - Phishing, social engineering, brute-force attacks.
    - Confidentiality, Integrity, Availability (CIA Triad).
3. **Cybersecurity in Everyday Life:**
    - Banking apps, smart devices, emails, social media.
    - Examples of personal cyber threats.
4. **Why You Should Care:**
    - Real-world consequences: identity theft, data leaks, reputational damage.
    - Non-technical roles still involve risky digital behavior.

Interactive Activities:

- **Discussion Prompt**: "What's the most cyber-risky thing you did today, knowingly or unknowingly?"

Week 2: The Cybersecurity Threat Landscape + Human Factor

Lecture Objectives:

- Understand the evolving nature of digital threats.
- Identify the most common attack vectors and their impact.
- Explore how human behavior can be the weakest link in security.

Lecture Outline:

1. **The Threat Landscape:**
    - Attackers: Hacktivists, nation-states, cybercriminals, insiders.
    - Trends: Ransomware, phishing, identity theft, zero-days.
    - Real-world stats: Cyberattack rates, costs to businesses, recent examples.
2. **Attack Vectors:**
    - Email, SMS (smishing), USB devices, public Wi-Fi, weak passwords.
    - Demo or screenshots of phishing emails and fake login pages.
3. **The Human Factor:**
    - Psychology of manipulation: trust, urgency, authority.
    - Case Study: The Australian National University phishing study (Broadhurst et al.)
    - Overconfidence bias and its dangers.
4. **How Awareness Helps:**
    - Recognizing red flags.
    - Building cyber mindfulness into routine decisions.

Interactive Activities:

- **“Spot the Phish” Exercise**: Analyze example emails, messages, and pop-ups.
- **Poll**: “Have you ever clicked on a suspicious link?” followed by a group discussion.

Survey Content:

Demographics

1. What year of study are you currently in?

   - A) First year
   - B) Second year
   - C) Third year
   - D) Fourth year
   - E) Transfer student
   - F) Graduate student

2. What is your primary field of study?
   - A) Arts and Humanities
   - B) Business
   - C) Education
   - D) Engineering
   - E) Health Sciences
   - F) Natural Sciences
   - G) Social Sciences
   - H) Other

Self-Assessment of Digital Literacy

3. How would you rate your overall technology literacy?
   - A) Very poor
   - B) Poor
   - C) Average
   - D) Good
   - E) Excellent
4. How confident are you in your ability to identify phishing attempts?
   - A) Not at all confident
   - B) Slightly confident
   - C) Moderately confident
   - D) Very confident

    - E) Extremely confident

5. I believe I would be able to spot and ignore online scams.
    - A) Strongly disagree
    - B) Disagree
    - C) Neutral
    - D) Agree
    - E) Strongly agree

Experience and Behavior

6. Have you ever fallen victim to an online scam or phishing attempt?
    - A) Yes
    - B) No
    - C) Not sure
7. How often do you check the sender's email address before clicking on links in emails?
    - A) Never
    - B) Rarely
    - C) Sometimes
    - D) Often
    - E) Always
8. Have you ever received formal training on cybersecurity awareness?
    - A) Yes
    - B) No
    - C) Not sure

Knowledge Assessment (with correct answers)

9. Which of the following is NOT a common indicator of a phishing attempt?
    - A) Poor grammar or spelling errors
    - B) Requests for personal information
    - C) Generic greetings (e.g., "Dear User")

    - D) Professional company logo ✓ (CORRECT ANSWER)
    - E) Sense of urgency or threat

10. True or False: If an email appears to come from your university administration, it is always safe to click on links within the email.
    - A) True
    - B) False ✓ (CORRECT ANSWER)
11. True or False: Phishing attempts are always obvious and easy to identify.
    - A) True
    - B) False ✓ (CORRECT ANSWER)
12. The most common motivation behind phishing attempts is:
    - A) Political activism
    - B) Financial gain ✓ (CORRECT ANSWER)
    - C) Personal revenge
    - D) Entertainment
    - E) Technical challenge
13. True or False: Using the same password across multiple accounts is safe as long as the password is complex.
    - A) True
    - B) False ✓ (CORRECT ANSWER)
14. When receiving an unexpected email claiming to be from your bank, the best action is to:
    - A) Click the link in the email to check your account
    - B) Reply directly to the email to confirm its legitimacy
    - C) Contact your bank through official channels (phone number on card or official website) ✓ (CORRECT ANSWER)
    - D) Forward the email to friends to see if they received it too

Self-Assessment After Exposure

15. After participating in this study, how would you now rate your ability to identify phishing attempts?

- A) Much worse than I thought
- B) Somewhat worse than I thought
- C) About the same as I thought
- D) Somewhat better than I thought
- E) Much better than I thought

Behavior Change

16. Has this experience changed how you will approach emails and online communications in the future?
    - A) Yes, significantly
    - B) Yes, somewhat
    - C) No change
    - D) Not sure
17. Which security measure would you be MOST likely to implement as a result of this study?
    - A) Double-check sender addresses
    - B) Hover over links before clicking
    - C) Verify requests through official channels
    - D) Use multi-factor authentication
    - E) Be more cautious with personal information

Behavior Change

19. Has this experience changed how you will approach emails and online communications in the future?
    - A) Yes, significantly
    - B) Yes, somewhat
    - C) No change
    - D) Not sure
20. Which security measure would you be MOST likely to implement as a result of this study?

   - A) Double-check sender addresses
   - B) Hover over links before clicking
   - C) Verify requests through official channels
   - D) Use multi-factor authentication
   - E) Be more cautious with personal information.

21. Which factor do you believe most contributed to your susceptibility to phishing attempts?
    - A) Lack of technical knowledge
    - B) Distraction or inattention
    - C) Trusting official-looking content
    - D) Time pressure
    - E) Curiosity about the offer
22. True or False: I would recommend that all university students receive formal training in cybersecurity awareness.
    - A) True
    - B) False
23. After this study, I believe the importance of cybersecurity awareness in my field of study is:
    - A) Not important
    - B) Somewhat important
    - C) Important
    - D) Very important
    - E) Essential

Conclusion:

The constantly developing integration of digital technologies into various careers inadvertently creates an ever-growing risk factor into those careers. In fields that never required forms of technology, there are now considerable threats from the cybersecurity realm. Due to the desire for better technologies and improved efficiency across all careers, there must be constant technical integration into those fields. This is exactly what I hope to achieve by implementing a course like this at Radford University. Offering a course that teaches the principles of online safety from a technical perspective, all while refraining from feeling as overbearing to the non-technical majors. This course would offer an education into what cybercrimes look like and how cybersecurity skills can be useful in every career, even in one's personal life. There is a clear disconnect between perceived skills and actual skills in accordance with Broadhurst [1]. Using interactive lectures and hands-on activities, we will be able to mitigate the gap between one's perceived skills and their actual competency. The goal is not to create security experts, but to foster a digitally responsible student population capable of acknowledging and not falling victim to various cyber threats.

Personal Reflection:

As a student in computer science and cybersecurity, this topic really resonates with me. I think that my education in various cybersecurity related aspects helped me understand what would be acceptable to include in an entry level class like this. It also helps me understand why there is such a gap between using a computer and understanding some underlying processes. I think that from an overarching perspective, there needs to be some kind of course like this that is offered to all majors. This is due to the inherent risks involved with using technology. Especially as my class, and other undergraduate classes enter the workforce, it becomes so much more important. This is because individuals are responsible for keeping their company safe, which affects many more people than just themselves.

In terms of what worked well in this project, it ultimately came down to my mentor Professor Joyce. Having his insight into what goes into creating a course and what ultimately proves that it is necessary was extremely helpful. Due to us creating a few lecture plans initially and creating a survey that could be used in the future at Radford University, we have done a lot of leg work for moving forward with this implementation. Additionally, there was really only one factor that went negatively. This would be not implementing the survey here at Radford University to see how similar the statistics would be to that as discussed in Broadhurst. Obviously, I could simply say that it came down to time, as I did not know how involved getting a survey approved would be. However, I think that the implementation of our survey would further create clear statistics as to how necessary this course would be.

References

[1] Broadhurst, R. G. (n.d.). *(PDF) phishing and cybercrime risks in a university student community*. Phishing and Cybercrime Risks in a University Student Community. https://www.researchgate.net/publication/326029318_Phishing_and_Cybercrime_Risks_in_a_University_Student_Community