

## How to use this design journal:

During your final project, you will be working individually and collaboratively. All your work should be entered in the design journal here.

First, copy this into your Google Drive and share it with your teammates (only one person needs to do this for each team once).

Each assignment provided by your instructor in Brightspace should be entered here on its own page using “insert” > “page break”. The name or description of the assignment should be first on the new page and be a heading of an appropriate level (notice a few have been built as examples to modify and follow). The table of contents can be updated by hitting the refresh button that is evident in the table of contents section when you click on it.

Group assignments will have one entry here. Individual assignments will have one entry per person.

All submissions should be made chronologically.

To submit an assignment for grading in Brightspace: Make an entry in the design journal and then print only that entry’s pages as a PDF. Submit that PDF.

Begin with the format suggested here, but be creative in telling your story. The purpose is to document your journey this semester with this journal.

Delete this page prior to final submission.

Final Project Journal  
Purdue University

# Final Project Design Journal

Group #5

Group Members: Abhi Sunkara, Ishmeet Thethi, Seungchan Kim, Samuel Winiger, Derek Woodward

Purdue University  
Tech 120

Fall 2025

## Table of Contents

[Meet the Design Team](#)

[Team Contract](#)

[Executive Summary](#)

[Meeting 13 Tentative Problem Definition and Fieldwork Plans](#)

[Initial Problem Statement](#)

[Meeting 14 Feedback/Insights from Peers and Instructor](#)

[Meeting 15 - Benchmarking](#)

[Constraints and Criteria](#)

[Meeting 15 - Multicriteria Analysis](#)

[Meeting 17 - Before Class Fieldwork](#)

[Ethnographic Research - Interview 1](#)

[Ethnographic Research - Observation 1](#)

[Literature Review - Source #1](#)

[Meeting 17 In Class - Thematic Identification & Composite Character Profile](#)

[Meeting 18 - Before class ideation \[Individual\]](#)

[Meeting 18 - In-class ideation](#)

[Meeting 19 - Before class Solution Analysis](#)

[Meeting 19 - In-Class Solution Analysis](#)

[Meeting 20 - In-Class Prototype Development and Planning](#)

[Meeting 21 - Before Class Prototype Building](#)

[Meeting 21 - In-Class Prototype Feedback/Critique](#)

[Meetings 22 & 23 - Small Group Conference](#)

[Meeting 24 - Before Class Prototype Iteration](#)

[Meeting 24 - In-class Prototype Iteration](#)

[Meeting 25 - Before Class Prototype Finalization](#)

[Meeting 25 - In-Class Presentation Outline](#)

[Meeting 26 - Before Class Design Journal](#)

[Delete the instructions page \(in red\) from your design journal](#)

**Meet the Design Team**

Final Project Journal  
Purdue University

This section should include a professional picture of each group member along with a short bio that includes:

1. Name
2. Age (Year at Purdue)
3. Major
4. Main role in the group
5. Career aspiration(s)

\*Delete all text in red before final submission.

Abhi Sunkara  
20  
Cybersecurity  
Worker  
Security architect or chief officer of Cybersecurity

Seungchan Kim  
19  
Professional Flight & Aviation Management  
Worker  
Airline Pilot

Derek Wodoward  
18  
Cybersecurity  
Worker  
Security architect or some other similar job

Ishmeet Thethi  
18  
Cybersecurity  
Worker  
Already working at an ISP

## Team Contract

This section provides your team with a framework to set your own expectations to help establish a healthy and productive teamwork experience. Edit and revisit this as you go - refer to it during moments of success and challenging times.

Teamwork is essential to this course, but also for your work in campus organizations and future careers. Learning how to function as an effective team member and leader are prerequisite to administrative or management-level positions in any institution, organization, or company.

**Team Name:**

**Goals:** Our goal in this project is to...

These are the terms of group conduct and cooperation that we agree on as a team.

**Participation:** We agree to...

**Communication:** We agree to...

**Meetings:** We agree to...

**Conduct:** We agree to...

**Conflict:** We agree to...

**Deadlines:** We agree to...

## Executive Summary

This section should be completed at the end of the project BEFORE you submit it. Delete all text in red before submitting.

Instructions: The executive summary should be a maximum of one single-spaced page describing the final project. Items that should be included (as a bare minimum):

- How you reached your final POV statement
- Who your stakeholders are and why
- Your final solution idea
- Your prototyping sequence
- All feedback received
- Usability testing data

The executive summary should be a substantive outline that gives the reader a general idea of the events that transpired and should also give insight into the events ahead in the document.

## Meeting 14 Revised Problem Definition and Fieldwork Plans

Group Member Names: Samuel Winiger, Derek Woodward, Abhishek Sunkara, Seungchan Kim, Ishmeet Thethi

### Contact Information:

Derek Woodward: 5712178783 [derekwoodward22@gmail.com](mailto:derekwoodward22@gmail.com)

Ishmeet Thethi: 4809191176 / luumonix on Discord / [ithethi@purdue.edu](mailto:ithethi@purdue.edu)

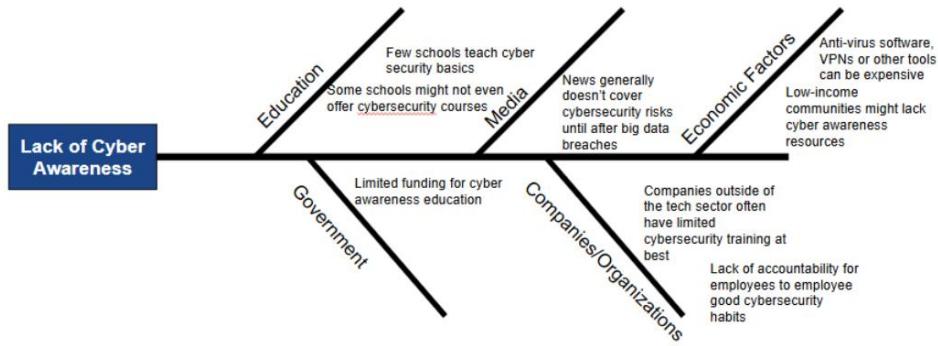
Samuel Winiger: 3177641811 [sambarca17@gmail.com](mailto:sambarca17@gmail.com)

Abhi Sunkara: 3149480081 [sunkara6@purdue.edu](mailto:sunkara6@purdue.edu)

Seungchan Kim : 9803712966 / [kim5171@purdue.edu](mailto:kim5171@purdue.edu)

### Fishbone Diagram (optional):

Take a picture and paste it. If no diagram, please provide the problem space your group has identified here:



### Potential Stakeholders (1 per group member)

Group Member	Stakeholder
Samuel Winiger	Purdue Cybersecurity Major Students
Derek Woodward	General College Students
Seungchan Kim	Professors

Final Project Journal  
Purdue University

Ishmeet Thethi	Purdue IT	
Abhishek Sunkara	Elders	
<b>Fieldwork Plans - Minimum 3 in each category &amp; a minimum of 3 per person</b>		
Literature (Member & What to look for)	Interviews (Member & Stakeholder)	Observations (Member & Location)
Ishmeet: Impact of weak passwords and MFA usage among students		Abhi: WALC Computer lounge
Ishmeet: Phishing and email-based cyber threats in universities	Abhi: Elders	Sam: Tarkington Hall
Sam: Cybersecurity awareness programs in school	Seungchan: Professors	
Abhi: Impact of weak passwords and MFA usage among students	Derek: Non-Purdue Students	Derek: Starbucks
Seungchan : Convenience tech habits and student cybersecurity risks	Sam: Purdue Students	Derek: Aspire Apartments
Seungchan : Public Wi-Fi security risks for students		

\*Further Fieldwork Plan details can be found in Meeting 17

### Initial Problem Statement

POV embedded in a paragraph describing the problem here. Include potential user groups, what those groups may need, and what makes the problem so surprising (insights). Additionally, since we have limited resources and time, discuss how you plan to interact with this problem. For instance, how will you be able to directly (and ethically) observe this problem happening, and who will you be able to talk to about this problem?

College students frequently neglect cybersecurity best practices despite being aware of the risks. Many rely on convenience, such as weak passwords or unsecured networks, which exposes personal and institutional data to potential attacks. Our group aims to explore why cybersecurity awareness doesn't translate into secure behavior among students and how Purdue can promote better digital safety habits.

### Meeting 14 Feedback/Insights from Peers and Instructor

\*Add more rows as necessary

Feedback/Insight	Is it something worth considering?	What needs to be changed?
Example: Interviewing students about road construction may not	Yes	Instead of interviewing students, we will seek out construction workers,

Final Project Journal  
Purdue University

give you sufficient information		city planners, or construction professors.
Think about solutions outside of generic online training courses	Yes	Creating a niche, interactive, and unique solution will make our solution more appealing, especially to students who are looking for an engaging way to learn about cyber awareness.
Try to find stakeholders who are more vulnerable to cybersecurity attacks like the elderly	Yes	By interviewing people who are most vulnerable to cyber threats, we can gain a better insight on the tactics people are implementing to illegally access victims' data and personal info. Further, interviewing people who lack cyber awareness will provide stronger data leading to a strong prototype
Make sure the scope isn't too large, so that you can complete it in the timeframe given	Maybe	Depending on our skillsets, we could either take on a larger scale project for our prototype or a lesser one. This will be decided depending on our group's skills and the assets that we have available to us

Apply any changes to the “Meeting 14 Problem Definition and Fieldwork Plans” template above and submit your revised plans and your feedback to the Meeting 14 in-class submission portal

## Meeting 15 - Benchmarking (Individual)

### TECH 120 Benchmarking

#### Solution 1

\*Note that all responses need to be in your own words\*

What solution was proposed? (Solution and detailed description)

Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.

How long does it take to implement? (From development to customer purchasing)

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

What environmental effects does the solution have? (Both positive and negative)

What economic effects does the solution have? (Both positive and negative)

How much does it cost? (Cost to the consumer)

What are some drawbacks of the product/service? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

#### About the Source

Overall Quality ("x" one):     High     Medium     Low

Citation in APA format (including URL if from Google):

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose. Answer the relevant questions)**

1. Authority: Who made the solution

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

2. Accuracy: The reliability, truthfulness, and correctness of the solution

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

3. Purpose: The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sale?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

**Solution 2****\*Note that all responses need to be in your own words\***

**What solution was proposed?**

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

How long does it take to implement? (From development to customer purchasing)

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

What environmental effects does the solution have? (Both positive and negative)

What economic effects does the solution have? (Both positive and negative)

How much does it cost? (Cost to the consumer)

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

**About the Source**

Overall Quality ("x" one):       High       Medium       Low

Citation in APA format (including URL if from Google):

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)

**1. Authority:** Who made the solution

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

**2. Accuracy:** The reliability, truthfulness, and correctness of the solution

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

**3. Purpose:** The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sale?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

### Constraints and Criteria

Choose your favorite/best benchmarked solution from above and read the definitions of *constraints* and *criteria*. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal

**Criteria:** What your solution has to do in order to be successful. A measure of success.

Example problem: increasing safety in manufacturing labs

Example constraints: Can the room layout stay the same? Are all walkways at least 4 feet wide? (Answering 'yes' would indicate a viable solution, 'no' would remove that solution from consideration)

Example criteria: provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

Solution:

Possible criteria (as many as possible):

Possible constraints (as many as possible):

\* Insert all benchmarking assignments from every group member. Delete this text prior to submitting.

**TECH 120 Benchmarking**

**Solution 1 - Ishmeet Thethi**

**\*Note that all responses need to be in your own words\***

**Keywords:** cybersecurity training, gamification, universities, phishing, student awareness, interactive learning, behavioral change

**What solution was proposed? (Solution and detailed description)**

Infosec IQ is a security awareness platform made specifically for universities. It has over 2,000 training resources in different formats and languages. The cool thing is they have pre-built training plans that universities can drop right into their academic calendar. It covers stuff like NIST cybersecurity topics and compliance things like FERPA. The platform can be customized for different groups - students get different training than faculty or IT staff. It includes phishing simulations, gamified content, and interactive modules to help people spot and respond to cyber threats.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

**How long does it take to implement? (From development to customer purchasing)**

Pretty quick actually - they give you a client success manager who helps set everything up. From what I found, schools can start using it within a few weeks. It integrates with university SSO systems which speeds things up. Full rollout with custom content takes 1-2 months from purchase to everyone on campus using it.

**Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)**

It's been successful at multiple universities. They measure success through training completion rates, how well people do on phishing simulations, actual reduction in security incidents, and behavior improvements. The platform won multiple awards including Expert Insights 2025 Security Awareness Award and G2's 2025 award for easiest setup. One verified user review said it's been crucial for their staff who haven't caught up with cybersecurity practices yet.

**What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)**

Just need internet and a device - computer, tablet, or phone. It's all cloud-based through a browser, no special software to install. For admins, you don't need to be a cybersecurity expert - they provide client success managers who help. It hooks into your existing LMS and university authentication. Regular users don't need any technical background since the training is designed to be accessible.

**What environmental effects does the solution have? (Both positive and negative)**

**Positive:** No printed materials needed, which saves paper. Also cuts down on travel emissions since you don't need to gather people in one place for training.

**Negative:** Uses data centers and cloud infrastructure, which consume electricity. But this impact is way smaller than traditional training and is shared across schools.

**What economic effects does the solution have? (Both positive and negative)**

Final Project Journal  
Purdue University

**Positive:** Can save massive amounts of money by preventing breaches. The average data breach in higher ed costs millions of dollars, and most universities have dealt with ransomware. Preventing just one incident pays for the platform many times over. The automation also saves staff time. Helps meet compliance requirements which avoids fines.

**Negative:** There's a subscription cost (pricing not public), initial setup time, and ongoing admin time, though the automation keeps this pretty minimal.

How much does it cost? (Cost to the consumer)

Not listed publicly - you have to contact them for a quote. Pricing is customized based on school size and features you want. Based on similar platforms, likely ranges from tens to hundreds of thousands annually depending on the university.

What are some drawbacks of the product/service? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Training fatigue is still possible if not done right. It's just awareness training, not technical security controls. Success depends on people actually engaging, which is tough in college where everyone's busy. Needs ongoing admin work to keep it relevant. The one-size-fits-all approach might not work for every department. Cost could be an issue for smaller schools.

**About the Source**

Overall Quality ("x" one):       High       Medium       Low

**Citation in APA format (including URL if from Google):**

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Infosec. (n.d.). Cybersecurity awareness training for higher education. Infosec.  
<https://www.infosecinstitute.com/solutions/cybersecurity-for-higher-education/>

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose. Answer the relevant questions)**

1. **Authority:** Who made the solution
  - Who is the creator of the solution? Is it a person, group of people, an organization?
  - Is he/she the original creator?
  - Is the person qualified? What are his/her credentials? What is his/her occupation?
  - Is the source sponsored or endorsed by an institution or organization?

Infosec created this platform and they're legitimate - they've been doing cybersecurity education for decades. They're qualified because this is what they specialize in. Research shows they've worked with thousands of organizations worldwide and have certified instructors developing content. The platform has won industry awards and has good ratings on G2 and Expert Insights. Universities also endorse the platform.

2. **Accuracy:** The reliability, truthfulness, and correctness of the solution
  - Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
  - Where does the information come from? Is it supported by evidence?
  - Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
  - Does the language or tone seem unbiased or free of emotion?

The source uses real statistics about cyber threats in higher ed. It's obviously promotional (they're selling their product), the threat info they cite is backed by actual industry research. They include testimonials from verified users on third-party review sites, which gives independent validation. The training is based on NIST frameworks and FERPA compliance, which are legal authoritative standards. The language is professional without being salesy. They acknowledge the broader cybersecurity context instead of claiming their product fixes everything.

3. **Purpose:** The reason the solution exists

Final Project Journal  
Purdue University

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

Main purpose is obviously to sell their platform, but they also provide educational value about cybersecurity in higher ed. They're transparent about being a commercial product but back up their claims with actual data. There's commercial interest since they're for-profit, but the solution addresses a real problem - breaches involve human error. The platform serves a genuine educational purpose beyond just making money, especially as it aligns with established frameworks like NIST.

**Solution 2 - Ishmeet Thethi**

**\*Note that all responses need to be in your own words\***

**What solution was proposed?**

Hoxhunt is a gamified cybersecurity training platform built on behavioral science. Instead of boring videos, it uses bite-sized, personalized phishing simulations tailored to your role and skill level. The gamification is sophisticated - points, badges, leaderboards, instant feedback, adaptive difficulty. Training scenarios are based on millions of real threat signals, so you're learning from actual current attacks. It's grounded in BJ Fogg's Behavior Model (Motivation + Ability + Prompt = Behavior). The adaptive difficulty adjusts as you get better, realistic simulations, immediate rewards for reporting threats, and detailed analytics tracking both practice and real threat detection.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

**How long does it take to implement? (From development to customer purchasing)**

Pretty fast - works with existing auth systems and can start training within weeks. AES Corporation saw engagement jump from 10% to 70% within months, so it can be rapidly effective. The adaptive system personalizes content immediately as you use it. Full organizational adoption with measurable behavior change happens in 3-6 months, but training starts sooner.

**Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)**

Real metrics: 6x improvement in phishing reporting accuracy in 6 months, 86% reduction in phishing incidents, and 10x increase in real threat detection within a year. User engagement went from 10% to 70% in some cases. They track actual behavioral statistics like phishing reporting rate and how fast people report threats (32% improvement in speed within a year). Organizations using it have won CSO50 awards. Studies show gamified programs boost completion by 60% and retention by 30-40%. On G2, Hoxhunt scores 9.7/10 for ease of setup and 9.5/10 for gamification quality.

**What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)**

Just need internet-connected devices - phone, laptop, tablet. Works great on mobile so you can do it on your commute. Cloud-based, browser-accessible, no special software. Admins just need basic IT knowledge. Integrates with email, Slack, Teams. No cybersecurity expertise needed for users - it's designed to be intuitive. The analytics dashboards are easy to read without being a data scientist.

**What environmental effects does the solution have? (Both positive and negative)**

**Positive:** Fully digital so no paper waste. Reduces need for in-person training (less travel emissions). Mobile-friendly design lets people train during commutes, making efficient use of existing travel time.

**Negative:** Needs cloud infrastructure and data centers which use electricity. But this impact is distributed across many organizations, so per-user impact is negligible compared to traditional training.

**What economic effects does the solution have? (Both positive and negative)**

**Positive:** Huge savings from preventing breaches. That 86% reduction in phishing incidents directly avoids the millions of dollars in average breach cost in higher ed. Automation cuts staff time significantly. Faster threat detection reduces damage when breaches do occur. Scales efficiently to large populations. 89% of employees report increased productivity with

Final Project Journal  
Purdue University

gamified training.

Negative: Subscription costs (not public), initial setup time, ongoing admin time for monitoring, albeit far less than a traditional approach.

How much does it cost? (Cost to the consumer)

Not public - you have to request a demo and get a quote. Customized based on org size, users, and features. Based on similar enterprise platforms, probably tens to hundreds of thousands annually for larger schools. Subscription-based with likely tiered pricing.

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Gamification helps a lot but can't completely eliminate training fatigue. Effectiveness depends on organizational culture and leadership support - can't create security culture on its own. Some people might view competitive elements negatively if leaderboards create pressure instead of motivation. Focuses mainly on phishing and social engineering, so you need other security controls as well. Needs consistent user interaction to work best, which is tough with irregular college schedules. Requires ongoing admin attention to review analytics. Cost might be prohibitive for smaller schools. Effectiveness depends on actual engagement, not just clicking through. Some privacy concerns with detailed behavior tracking, though they claim EU compliance.

About the Source

Overall Quality ("x" one):       High       Medium       Low

**Citation in APA format (including URL if from Google):**

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Hoxhunt. (2025, September 17). Does gamified cyber security training actually work? Hoxhunt.  
<https://hoxhunt.com/blog/gamified-cyber-security-training>

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)**

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

Hoxhunt created this platform - they're the original developers. They're qualified because they specialize in human risk management and behavioral change, with behavioral scientists, learning experts, and psychologists on staff. Their approach is grounded in BJ Fogg's Behavior Model from Stanford. They've worked with major companies like AES Corporation, Qualcomm, and TomTom. Multiple clients have won CSO50 awards using their platform. Third-party reviews on G2, Capterra, and Gartner rate them highly (9.7 for ease of setup, 9.5 for gamification), which provides external validation.

**2. Accuracy: The reliability, truthfulness, and correctness of the solution**

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

Strong accuracy backed by evidence. They're transparent about being promotional. They cite external research like the 2025 Verizon Data Breach Report, BJ Fogg's research from Stanford, and multiple studies on gamification. Specific metrics are provided with clear sources. Case studies use actual client names and measurable results, not vague claims. Links to external validation through G2 reviews and competitor comparisons. Language is professional and evidence-based. They even admit their bias at one point ('Are we biased? Absolutely. Is there real proof? Absolutely.') which shows honesty. Citations come from reputable sources like TalentLMS, Zippia, and published research.

**3. Purpose:** The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

Primary purpose is selling their platform, but there's substantial educational content about behavioral science in cybersecurity that goes beyond marketing. They present a balanced view by acknowledging gamification can't fix culture problems on its own. The detailed behavioral science explanations and extensive citations show genuine commitment to education. They explicitly admit commercial bias, which is refreshingly honest. While they're for-profit, the solution addresses a well-documented problem (60% of breaches involve human error per Verizon). The platform serves a real educational purpose in bridging the gap between awareness and actual behavior change.

### Constraints and Criteria

Choose your favorite/best benchmarked solution from above and read the definitions of *constraints* and *criteria*. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal

**Criteria:** What your solution has to do in order to be successful. A measure of success.

Example problem: increasing safety in manufacturing labs

Example constraints: Can the room layout stay the same? Are all walkways at least 4 feet wide? (Answering 'yes' would indicate a viable solution, 'no' would remove that solution from consideration)

Example criteria: provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

Solution:

I picked Hoxhunt because it actually addresses the core issue we found in our research - knowing about cybersecurity doesn't mean people actually do secure things. Traditional platforms like Infosec IQ have tons of content, but Hoxhunt specifically targets that gap between knowledge and action using behavioral science. The gamification isn't just superficial - it's based on actual psychology (BJ Fogg's Behavior Model, the Super Mario Effect). The results show relatively high improvement: 6x improvement in reporting and 86% reduction in incidents. That shows it creates lasting behavior change, not just temporary awareness. For college students specifically, this makes way more sense. The bite-sized, mobile-friendly format fits how students actually live. The adaptive difficulty keeps it challenging without being overwhelming, which addresses students tuning out when content is too easy or too hard. Plus, the focus on positive reinforcement instead of punishment creates a safe learning environment, which is important for students who may feel intimidated by cybersecurity-related topics or content.

Possible criteria (as many as possible):

User Engagement Rate: % of students completing training consistently. Target: 60%+ engagement.

2. Phishing Recognition: Pre vs post-training phishing identification. Target: 50%+ improvement.

3. Behavioral Sustainability: Tracking reporting behaviors over 6-12 months. Target: maintained or improved rates.

4. Knowledge Retention: Periodic assessments of retained info. Target: 70%+ retention at 3 months.

Possible constraints (as many as possible):

Budget: Must fit university tech budgets. Can we afford it? (Yes/No)

Technology Access: Must work on devices students own. Special equipment needed? (No)

Time Commitment: Must fit student schedules. Modules under 10 min? (Yes)

Privacy Compliance: Must meet FERPA and other regulations. Compliant? (Yes)

Scalability: Must handle thousands of users. Can it scale? (Yes)

Integration: Must work with campus SSO. Integrates? (Yes)

Accessibility: Must meet ADA requirements. Accessible? (Yes)

Language Support: Should support multiple languages. Available? (Yes)

Admin Overhead: Can't require excessive staff time. Minimal admin? (Yes)

Cultural Appropriateness: Must work for diverse backgrounds. Appropriate? (Yes)

## TECH 120 Benchmarking

Derek Woodward - Solution 1

**\*Note that all responses need to be in your own words\***

What solution was proposed? (Solution and detailed description)

Princeton University implemented a comprehensive cybersecurity awareness and culture-building program designed to transform how staff, faculty, and students think about information security. The initiative, led by Princeton's Information Security Office, focused on embedding security awareness into daily operations through continuous education, leadership engagement, and creation of departmental "security champions." The program included campus-wide communications, phishing awareness events, password-management campaigns, and partnerships with departments to tailor content to their specific risks. The goal was to make cybersecurity a shared responsibility and part of the university's culture rather than a technical afterthought.

Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.

How long does it take to implement? (From development to customer purchasing)

The cultural transformation process was launched over approximately one year. Initial planning and leadership engagement took 2-3 months, followed by content development and departmental coordination (3-4 months). Awareness events, workshops, and campus communications were rolled out continuously over the following academic year, with ongoing reinforcement and evaluation.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

The program achieved measurable results, including increased participation in security training, a noticeable rise in the number of phishing emails reported by users, and reduced account-compromise incidents. Princeton's information security team reported greater collaboration between IT and academic departments and higher adoption rates of secure tools such as password managers and multifactor authentication.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

Implementation required an internal information security team with expertise in cybersecurity education and communications, along with access to campus-wide communication tools (email systems, intranet, posters, and events). The university leveraged existing IT infrastructure and supplemented it with awareness-specific materials.

What environmental effects does the solution have? (Both positive and negative)

The environmental impact was minimal. Digital learning and communication materials replaced paper-based awareness flyers, slightly reducing paper use.

What economic effects does the solution have? (Both positive and negative)

Effects included a lower likelihood of costly breaches or downtime, resulting in savings on remediation and response. Financial investment was limited to awareness-program resources and staffing, making it a cost-effective prevention measure.

How much does it cost? (Cost to the consumer)

Costs primarily involved staff time and resources for creating and distributing awareness materials. Since Princeton used in-house personnel and existing tools, direct expenses were low.

What are some drawbacks of the product/service? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Challenges included maintaining engagement over time and measuring intangible cultural change. The program's success relied heavily on leadership support and consistent messaging.

#### About the Source

Overall Quality ("x" one):       High       Medium  
 Low

Citation in APA format (including URL if from Google):

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Blum, D., Sherry, D., & Schaufler, T. (2021). *Case Study: Transforming Princeton's security culture through awareness*. ISACA Journal, 1. Retrieved October 20, 2025, from <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/case-study-transforming-princeton-s-security-culture-through-awareness>

Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose. Answer the relevant questions)

<p>1. Authority: Who made the solution</p> <ul style="list-style-type: none"> <li>• Who is the creator of the solution? Is it a person, group of people, an organization?</li> <li>• Is he/she the original creator?</li> <li>• Is the person qualified? What are his/her credentials? What is his/her occupation?</li> <li>• Is the source sponsored or endorsed by an institution or organization?</li> </ul>
<p>This program was developed and implemented by Princeton University's Information Security Office, supported by ISACA, a global authority in cybersecurity and IT governance.</p>
<p>2. Accuracy: The reliability, truthfulness, and correctness of the solution</p> <ul style="list-style-type: none"> <li>• Is the bias of the creator obvious? Is the source trying to convince you of a point of view?</li> <li>• Where does the information come from? Is it supported by evidence?</li> <li>• Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?</li> <li>• Does the language or tone seem unbiased or free of emotion?</li> </ul>
<p>The solution is based on measurable outcomes and reported metrics in an industry-recognized publication.</p>
<p>3. Purpose: The reason the solution exists</p> <ul style="list-style-type: none"> <li>• What is the intended purpose of the solution: inform, teach, sell?</li> <li>• Does the point of view appear objective and impartial?</li> <li>• Are there political, ideological, cultural, religious, institutional leanings presented?</li> </ul>
<p>The purpose is educational and cultural improvement, not commercial promotion. It demonstrates credible, institution-backed change.</p>

### Derek Woodward - Solution 2

\*Note that all responses need to be in your own words\*

<p>What solution was proposed?</p> <p>Bridgewater State University adopted a phishing simulation and awareness training campaign to strengthen cybersecurity readiness among faculty, staff, and students. Partnering with KnowBe4, the university conducted regular simulated phishing exercises to test users' ability to recognize malicious emails. Individuals who fell for the simulations received targeted, interactive training modules to improve their awareness. Over time, this approach helped create a culture of accountability and proactive reporting. The program also included ongoing newsletters and metrics tracking to show improvement over successive simulations.</p>
<p>Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.</p>
<p>How long does it take to implement? (From development to customer purchasing)</p>

The initial rollout took about three months. The university selected a vendor, set up user groups, and ran the first phishing simulation to establish a baseline. Within the next 3-6 months, follow-up training, feedback, and performance tracking were implemented. Continuous campaigns are run every semester to maintain engagement.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

Bridgewater State University's program significantly reduced the percentage of users clicking on phishing links over time. The institution also reported higher completion rates of cybersecurity training and more incident reports from users recognizing suspicious messages. KnowBe4's case metrics documented measurable improvements after multiple campaign cycles, indicating behavioral change across the university community.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

Implementation required a phishing simulation and awareness platform (KnowBe4) and administrative access to campus email systems. No advanced in-house cybersecurity expertise was required beyond basic IT and training administration, as the vendor provided pre-built content and analytics.

What environmental effects does the solution have? (Both positive and negative)

Environmental impact is minimal, as all training and communications are digital.

What economic effects does the solution have? (Both positive and negative)

Positive effects include reduced risk of breaches, reputational harm, and recovery costs. Negative effects involve subscription or licensing costs for the awareness platform. However, the return on investment is strong compared to the potential cost of even a single successful attack.

How much does it cost? (Cost to the consumer)

Costs depend on the number of users. Vendor subscription pricing for phishing simulations and training platforms typically scales with enrollment, but total costs are modest compared to full-time staff or breach recovery expenses.

Final Project Journal  
Purdue University

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Drawbacks include reliance on a third-party vendor and the need to continuously update simulation templates to stay relevant. Some users may initially resist or misunderstand phishing tests, requiring clear communication.

About the Source

Overall Quality ("x" one):                    High                    Medium  
 Low

Citation in APA format (including URL if from Google):

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Bridgewater State University. (2024, September). *Case Study: Bridgewater State University Phishing Campaign & Awareness Training*. KnowBe4. Retrieved October 20, 2025, from [https://www.knowbe4.com/hubfs/KSAT-Education-Bridgewater-State-University-CS-2-en\\_US.pdf](https://www.knowbe4.com/hubfs/KSAT-Education-Bridgewater-State-University-CS-2-en_US.pdf)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)**

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

This case study was conducted by Bridgewater State University in collaboration with KnowBe4, a leading cybersecurity awareness vendor.

**2. Accuracy: The reliability, truthfulness, and correctness of the solution**

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

The source provides quantitative outcomes and details of implementation, offering a verified example of institutional success.

**3. Purpose: The reason the solution exists**

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The purpose is to educate and share a proven awareness model, not to market a product directly. The content is factual and based on actual results.

## Constraints and Criteria

Choose your favorite/best benchmarked solution from above and read the definitions of **constraints** and **criteria**. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal

**Criteria:** What your solution has to do in order to be successful. A measure of success.

**Example problem:** increasing safety in manufacturing labs

**Example constraints:** Can the room layout stay the same? Are all walkways at least 4 feet wide? (Answering ‘yes’ would indicate a viable solution, ‘no’ would remove that solution from consideration)

**Example criteria:** provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

**Solution:**

Bridgewater State University - Phishing Simulation and Awareness Training Program

Possible criteria (as many as possible):

- At least 90% participation rate in phishing simulations and follow-up training modules within the first year.
- Reduction of phishing click-through rate by 50% or more after three consecutive campaign cycles.
- Increased reporting of suspicious emails and phishing attempts by end users.
- Positive post-training feedback from staff and students (average satisfaction  $\geq 4$  out of 5).
- Documented improvement in cybersecurity awareness assessment scores year over year.

- Inclusion of the awareness campaign in the institution's broader IT security plan

Possible constraints (as many as possible):

- Limited budget for vendor subscription and staff time to manage campaigns.
- User resistance or fatigue from repeated testing or training sessions.
- Dependence on vendor tools (KnowBe4 platform or other) for analytics and training delivery.
- Varying technical skills among users, affecting comprehension and engagement.
- Need for administrative approval and IT coordination to send simulated phishing emails campus-wide.
- Data privacy and consent requirements for tracking user responses to simulations.
- Scheduling conflicts with academic calendars or faculty workload.
- Ongoing requirement to refresh content so simulations remain realistic and effective

### Solution 1 - Samuel Winiger

\*Note that all responses need to be in your own words\*

What solution was proposed? (Solution and detailed description)

Universities should real world cyber threats into their curriculum to better prepare students for what they may face in the real world.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

How long does it take to implement? (From development to customer purchasing)

This is more a matter of researching what specifically could be included in the new curriculum to help further education on cybersecurity, as such this may take weeks to months to research the best options to implement.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

The article focuses more on advocating for more universities to implement this type of education into their curriculum than it does focusing on where it has been used, it seems that success can be measured in how much more prepared students are for real world cyber threats after going through the new curriculum.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

Experts who are knowledgeable in the cybersecurity field and can research and implement these real life cyber attack scenarios will be needed to implement the solution.

What environmental effects does the solution have? (Both positive and negative)

The solution will require resources and investment from the university in order to implement this, so the environmental impact could be from needing to use energy and resources to make the solution, negatively affecting the environment.

What economic effects does the solution have? (Both positive and negative)

The solution will lead to better prepared people in the workforce who are less susceptible to cyber attacks which could save companies tons of money that would have otherwise went to dealing with the aftermath of cyber attacks on unprepared employees.

How much does it cost? (Cost to the consumer)

The cost would depend on the scale of the investment by the university into implementing the solution and how engaging and effective they want it to be, although I imagine it wouldn't be that expensive.

What are some drawbacks of the product/service? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

**The drawbacks of the solution is that success might be hard to measure when it is put into practice.**

Final Project Journal  
Purdue University

Overall Quality ("x" one):  High  Medium  Low

**Citation in APA format (including URL if from Google):**

Andersen, G. (2024, January 28). *The human element of cyber security: Raising Awareness in university settings*. MoldStud. <https://moldstud.com/articles/p-the-human-element-of-cyber-security-raising-awareness-in-university-settings>

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose. Answer the relevant questions)**

**1. Authority:** Who made the solution

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

The article was made by Grady Andersen who is a head IT consultant who specializes in no-code solutions to IT problems, and the article was published on Moldstud.

**2. Accuracy:** The reliability, truthfulness, and correctness of the solution

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

The information in the article seems to be fairly accurate although the article could be biased in that the creator of the article is also the one who created the solution they are presenting.

**3. Purpose:** The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The purpose of the solution and article seems to be a call to action to universities to change the way they educate students on cybersecurity.

**Solution 2 - Samuel Winiger**

**\*Note that all responses need to be in your own words\***

What solution was proposed?

This article recommends that colleges improve upon many different aspects of their security architecture.

Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.

How long does it take to implement? (From development to customer purchasing)

Because the article calls for various improvements to existing university cybersecurity protections, it would likely be a multi year process as changes are implemented incrementally to better see the improvements that come from each change

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

This article is more about what universities could do to improve cybersecurity rather than what they are doing but success could be measured in how many fewer cyber attacks happen on campus each year

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

Universities would have to bring in cybersecurity professionals who could oversee the changes being implemented

What environmental effects does the solution have? (Both positive and negative)

Because of the scale of the project there would likely be a significant carbon footprint involved with its implementation considering all the resources that would be needed to implement it

What economic effects does the solution have? (Both positive and negative)

The solution would go a long way in terms of saving the university from having to spend money on recovering from cyber attacks

How much does it cost? (Cost to the consumer)

Since the solution essentially involves a massive overall of universities security infrastructure it would be fairly costly to implement

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

**The drawbacks to the solution are that it hasn't been implemented so the impact is not really known**

#### About the Source

Overall Quality ("x" one):     High     Medium     Low

Citation in APA format (including URL if from Google):

Poremba, S. (2021, March 30). *Shift online exposed and expanded college cybersecurity vulnerabilities*. Higher Ed Dive. <https://www.highereddive.com/news/shift-online-exposed-and-expanded-college-cybersecurity-vulnerabilities/597451/>

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)

1. Authority: Who made the solution

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

The solution was made by a journalist building off of ideas from experts in the field and research.

2. Accuracy: The reliability, truthfulness, and correctness of the solution

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

Seeing as the article is not from someone with a cybersecurity background it might not be the most accurate however, they did do good research and sought the input from experts so I do believe it to be fairly accurate.

3. Purpose: The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sale?

- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The purpose of the solution is to improve the security controls on campuses across the country.

### Constraints and Criteria

Choose your favorite/best benchmarked solution from above and read the definitions of *constraints* and *criteria*. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal

**Criteria:** What your solution has to do in order to be successful. A measure of success.

Example problem: increasing safety in manufacturing labs

Example constraints: Can the room layout stay the same? Are all walkways at least 4 feet wide?

(Answering ‘yes’ would indicate a viable solution, ‘no’ would remove that solution from consideration)

Example criteria: provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

Solution:

Universities should real world cyber threats into their curriculum to better prepare students for what they may face in the real world.

Possible criteria (as many as possible):

Provide more hands on work dealing with real world issues rather than just learning about them and studying them.

Make the learning more practical than about memorization.

Provide access to the real world tools used to deal with or prevent cyber attacks.

Possible constraints (as many as possible):

Can all students handle working through and dealing with real world threats?

Will the solution be accessible for all students?

Will the solution make students think critically about cybersecurity?

### **What solution was proposed?**

The solution proposed was a modular curriculum called fiches for teaching cybersecurity and cyber safety in high schools.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

How long does it take to implement? (From development to customer purchasing)

The research mentions that teachers were given one month to prepare before utilizing the modules in class. The solution was utilized from the end of November 2022 to the beginning of March 2023 which is about 3 months.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

Yes. The authors reported positive feedback from students via surveys. The data showed that students increased their confidence, familiarity, and satisfaction other than their scores.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

In order for this solution to be proposed, the schools must have computer labs or students must have laptops with internet connectivity. Teachers should also be familiarized with the school devices.

What environmental effects does the solution have? (Both positive and negative)

The research does not mention environmental effects. However, we can assume that it can have some positive effects since no paper resources have to be printed out while computers can use higher electricity.

What economic effects does the solution have? (Both positive and negative)

Since the computers or laptops has to be purchased if there is not enough at the school, schools must spend time and money on teacher training and computer labs which can be negative economic effect for the school

How much does it cost? (Cost to the consumer)

The expected cost may vary, however, computer purchases and teacher training can be quite expensive. Students might be able to receive financial support from institutions, but if not, they would have to buy their own laptops which can cost over \$1,000 per student.

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Some drawbacks mentioned in the research are maintaining and updating external links/resources, variability in teacher expertise, differences in student background, and possible variability when scaling. Some other drawbacks can be the need for training time, lack of computers or budget, or outdated sources.

### **About the Source**

**Final Project Journal  
Purdue University**

Overall Quality ("x" one):      X High         Medium         Low

**Citation in APA format (including URL if from Google):**

**Blažič, A. J., & Blažič, B. J. (2024, November 15). Toward effective learning of cybersecurity: New curriculum agenda and learning methods | journal of cybersecurity | oxford academic.**  
[\*\*https://academic.oup.com/cybersecurity/article/10/1/tyae018/7900964\*\*](https://academic.oup.com/cybersecurity/article/10/1/tyae018/7900964)

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)**

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

The solution was created by Blažič, A. J. and Blažič, B. J. They are the original creators who developed the learning module themselves from the structure, design, and method. They are qualified since they both are cybersecurity researchers in Slovenia. The source is also published through Oxford Academic.

**2. Accuracy: The reliability, truthfulness, and correctness of the solution**

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

The author does not show bias in this research. They focus on data and observations that they conducted with their own developed solution which makes the source convincing. This research is published by Oxford academy and the language or tone is neutral and factual which makes it unbiased and free of emotion.

**3. Purpose: The reason the solution exists**

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The intended purpose of the solution is to inform and teach. The goal of the article is to share a new educational method that helps schools teach cybersecurity more effectively. The point of view is objective since it's talking about their research process and the result, not promoting a product or service. There aren't any political, cultural or religious learnings presented.

**Solution 2**

**\*Note that all responses need to be in your own words\***

**What solution was proposed?**

This research proposes several solutions which are developing digital literacy training, conducting workshops, developing communication channels, having public-private partnerships or developing a cybersecurity advice website.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

How long does it take to implement? (From development to customer purchasing)

The time it takes may vary based on the specific solution. For example, having partnership with cybersecurity companies can take a long time while conducting workshops can last from an hour to several years.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

Since this research did not lead to the result from the survey they took, it is not quite possible to measure the success. However, since they conducted surveys and proposed solutions based on the overall cybersecurity area, we can say that it was a successful research that shows the real world of cybersecurity risks.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

Smartphones, computers or digital devices were needed. In order to develop webs or apps for cybersecurity training, experts might need to build those technology tools.

What environmental effects does the solution have? (Both positive and negative)

A positive effect is that since some of them are digital solutions, they can reduce the use of paper. The negative effect is that more devices can cause higher electricity use.

What economic effects does the solution have? (Both positive and negative)

Some positive effects is that after these solutions are proposed, people will be aware of cybersecurity risks and will be more aware of cyber security. Some negative effects are that cities or institutions will have to spend money on training or development and low income communities might be unable to afford the cost.

How much does it cost? (Cost to the consumer)

The cost may vary based on the solution. For example, having cybersecurity workshops can be lower cost since we might be able to find some people who are willing to volunteer. On the other hand, developing apps or websites can be expensive since they will have to hire experts and spend on technologies.

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Some drawbacks of the product is that some of the solutions proposed can take time and money to set up. Also, some communities with lower budgets might not have access to digital devices or might be unable to afford the cost of the solutions.

**About the Source**

**Final Project Journal  
Purdue University**

Overall Quality ("x" one):        High      X Medium        Low

**Citation in APA format (including URL if from Google):**

**Sultan, A. (n.d.-b). *Improving Cybersecurity Awareness in Underserved Populations*. Berkeley CLTC White Paper Series. [https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC\\_Underserved\\_Populations.pdf](https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC_Underserved_Populations.pdf)**

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)**

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization?
- Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation?
- Is the source sponsored or endorsed by an institution or organization?

The author is Ahmad Sultan and he is the original creator who conducted the study and wrote the report. He is a master of public policy in UC Berkeley and associate director for research which proves his credentials. The source is published via the Center for Long Term Cybersecurity from UC Berkeley.

**2. Accuracy: The reliability, truthfulness, and correctness of the solution**

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view?
- Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

This study is based on several surveys containing over 100 responses. Results are supported by survey data, graphs, and comparison groups. This research is unbiased since its not a promotion of a product or service and the tone of the research is factual and unbiased.

**3. Purpose: The reason the solution exists**

- What is the intended purpose of the solution: inform, teach, sell?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The purpose of this research is to inform and teach people and city institutions to teach and learn how to protect people from cyber risks. The point of view is neutral and educational and there is no political, cultural, and religious bias.

## Constraints and Criteria

Choose your favorite/best benchmarked solution from above and read the definitions of *constraints* and *criteria*. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal

**Criteria:** What your solution has to do in order to be successful. A measure of success.

Example problem: increasing safety in manufacturing labs

Example constraints: Can the room layout stay the same? Are all walkways at least 4 feet wide?

(Answering ‘yes’ would indicate a viable solution, ‘no’ would remove that solution from consideration)

Example criteria: provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

Solution:

Modular curriculum (fiches) for teaching cybersecurity and cyber safety in high schools.

Possible criteria (as many as possible):

- Students will understand cybersecurity concepts
- Students will show more awareness in online safety
- Teachers will be able to use the modular curriculum as a support tool
- Program can be used by different schools and age groups
- Learning materials can stay up to date if updated
- Curriculum can be shared and reused for future classes or projects

Possible constraints (as many as possible):

- Schools must have enough computers or laptops
- Teachers will need training period
- Teachers who aren't used to digital devices might lack of usage
- Low income families might not be able to afford digital devices
- Developing modular curriculum can cost quite a lot based on the expert or tool that they use
- The project will depend on student and teacher participation
- Curriculum must be modified for students and teachers who are in different regions or who speak different languages

-Abhi Sunkara

**Solution 1**

**\*Note that all responses need to be in your own words\***

**What solution was proposed? (Solution and detailed description)**

The National Institute of Standards and Technology (NIST) proposed a Cybersecurity Awareness and Training Program designed to help organizations bridge the gap between knowing and doing when it comes to cybersecurity. The program promotes regular awareness campaigns, behavior-based training, and leadership involvement to build a lasting “security culture.”

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

**How long does it take to implement? (From development to customer purchasing)**

It will take about 3-6 months as developing materials, scheduling workshops, and deploying awareness campaigns will take up most of that time.

**Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)**

The solution from the source was successful. According to the source, organizations that followed the NIST framework reported huge improvements in user behavior, such as decreased phishing click rates, stronger password usage, and better reporting of suspicious activity.

**What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)**

Special equipment isn't necessary; however, certified cybersecurity trainer or IT staff who can deliver workshops and maintain training platforms like online modules or phishing simulator tools.

**What environmental effects does the solution have? (Both positive and negative)**

Some positives include that the solution promotes digital sustainability by reducing cyber incidents that cause downtime and wasted energy. The negatives are quite minimal but include increases in data storage or online activity for training materials

**What economic effects does the solution have? (Both positive and negative)**

Some positives include that the solution prevents financial losses from data breaches, reduces IT support costs, and increases institutional trusts. Some negatives include the solution requiring personal investments in staff time, training software which costs money and time, and communication campaigns.

**How much does it cost? (Cost to the consumer)**

It will depend on the seriousness and tools used for the cyber awareness program, but usually it would cost \$15-\$25 per student if they chose to enroll. The program won't use as many advanced tools so there is no need to over price for admission into it.

Final Project Journal  
Purdue University

What are some drawbacks of the product/service? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

Challenges include low student engagement, where students may find the training repetitive or uninteresting. Without creativity in assignments and lectures, participation rates can drop. Also, behavior change takes time, and measuring improvement in an academic environment takes time. However, the framework provides flexibility to adapt to student culture and integrate engaging digital learning.

**About the Source**

Overall Quality ("x" one): \_x\_ High        Medium        Low

**Citation in APA format (including URL if from Google):**

on, M., & Hash, J. (2003, October 1). Building an Information Technology Security Awareness and Training Program. CSRC. <https://csrc.nist.gov/pubs/sp/800/50/final>

10

Final Project Journal  
Purdue University

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose. Answer the relevant questions)**

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization? • Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation? • Is the source sponsored or endorsed by an institution or organization?

The solution was created by the National Institute of Standards and Technology (NIST), a highly respectable federal agency responsible for cyber threats. It was developed by cybersecurity experts so its reputable in terms of quality. Multiple government and academic partners are also involved. The source is an official U.S Department of Commerce agency, ensuing the source is authoritative and credible.

**2. Accuracy:** The reliability, truthfulness, and correctness of the solution

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view? • Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

The solution uses data driven and evidence based recommendations from security research and field studies. With this in mind, the language helps readers see that it is clear from bias and does not promote anything. The tone is unbiased and free of emotion as it is objective and instructional, providing frameworks and metrics for real implementation

**3. Purpose:** The reason the solution exists

- What is the intended purpose of the solution: inform, teach, sale?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The intended purpose of the solution is to inform and guide organizations on improving user cybersecurity behavior. The point of view does not appear to be objective or impartial as the info is coming from someone who is trying to spread information to help increase cyber awareness. And there are no political, ideological, cultural, or religious learnings presented; however, there are institutional learnings because the information is coming from a cybersecurity awareness based organization.

11

Final Project Journal  
Purdue University

**Solution 2**

**\*Note that all responses need to be in your own words\***

What solution was proposed?

The Stop.Think.Connect. Campaign, created by the U.S. Department of Homeland Security, is a national cybersecurity awareness and education initiative that encourages individuals – especially students – to make safer choices online. The campaign uses their slogan (“Stop. Think. Connect.”) to help users pause

before sharing information or clicking suspicious links. Thus, the campaign is focused mainly on phishing awareness and deciphering between safe and unsafe links.

**Specific Questions - answer all that apply. If you can't answer most of them, you might consider finding a new source as it might not be reliable or reputable.**

How long does it take to implement? (From development to customer purchasing)

The campaign should take between 2-4 months depending on how it is implemented. If implemented in schools and universities, it should take about 2 months. But for full integration into environments which include posters, toolkits, and events, the process should be about 3 months since the campaign is designed to help educational institutions and work spaces with awareness.

Was it successful? (How do you know, specifically?) How was success measured? (Earnings, revenue, valuation, etc.)

Yes. The campaign was successful as it's been widely adopted across schools, colleges, and international partners. Its success is measured by increased participation rates, the number of educational institutions using the toolkit, and surveys that showed higher cyber awareness between students. Success was measured by the amount of kids who adopted cyber awareness practices successfully through surveys and quizzes.

What special equipment or expertise is necessary? (Does the consumer need anything else to use it and why?)

No special equipment is necessary. However, the campaign will need certified IT staff and digital ambassadors to help in managing campaigns and running interactive workshops. The consumer will have stuff to download for free from the CISA website which include notes and activities that can be done.

What environmental effects does the solution have? (Both positive and negative)

Some positive environmental effects include most of the work being digital which limits the use of paper and anything tree related. Some negatives, which are minimal, include the printing of posters and forms which could cause minor environmental impacts due to the cutting of trees.

What economic effects does the solution have? (Both positive and negative)

Some positive effects include the campaign being free to use, saving institutions money if they choose to integrate the campaigns, and longer term benefits being seen from the teachings of the program. Some negative effects involve costs for the institution since they need to be the ones supplying the paper and printing materials and the potential of the campaign not succeeding, leading to a waste of resources.

How much does it cost? (Cost to the consumer)

There is no cost since the campaign is free to consumers; however, institutions will need to funnel in some money for promotional events and printing materials.

Final Project Journal  
Purdue University

What are some drawbacks of the product? (Will this work for your problem space? What are things that should be considered when evaluating the product/service?)

The campaign is reliant on voluntary participation so impacts from the campaign will depend on the students. Engagement. And with the integration, some institutions may need to change how the campaign is laid out so that it integrates cleanly with the specific environment and student body.

**About the Source**

Overall Quality ("x" one): \_x\_ High        Medium        Low

**Citation in APA format (including URL if from Google):**

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/>)

Cybersecurity Awareness Program | CISA. Cybersecurity & Infrastructure Security Agency. (n.d.).  
<https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program>

**Why is this a good solution? (Use ideas from the evaluation checklist, e.g. Authority, Accuracy, Purpose)**

12

Final Project Journal

Purdue University

**1. Authority: Who made the solution**

- Who is the creator of the solution? Is it a person, group of people, an organization? • Is he/she the original creator?
- Is the person qualified? What are his/her credentials? What is his/her occupation? • Is the source sponsored or endorsed by an institution or organization?

The CISA (Cybersecurity and Infrastructure Security Agency) is a part of the U.S Department of Homeland security and is the creator of the campaign idea. The creators are a group of educators, security professionals, and communication specialists. It's an official U.S government initiative, making it credible and trustworthy.

**2. Accuracy: The reliability, truthfulness, and correctness of the solution**

- Is the bias of the creator obvious? Is the source trying to convince you of a point of view? • Where does the information come from? Is it supported by evidence?
- Is the publication in which the item appears published, sponsored, or endorsed by a political or other special interest group?
- Does the language or tone seem unbiased or free of emotion?

The information is based on verified cybersecurity practices endorsed by national standards from various organizations such as the NIST. The information here is similar to various other sites that have aimed to prompt cybersecurity campaigns. The language is clear and factual, making it unbiased and the campaign from the site uses evidence-based strategies that can be implemented in the campaign. Some of these strategies include password hygiene and phishing prevention. The tone is unbiased and uses facts rather than emotions to get its point across.

### **3. Purpose: The reason the solution exists**

- What is the intended purpose of the solution: inform, teach, sale?
- Does the point of view appear objective and impartial?
- Are there political, ideological, cultural, religious, institutional leanings presented?

The purpose of the source is to inform and educate, and not to sell. It aims to create a culture of cybersecurity through awareness and easy habits that can be applied everyday. The point of view is objective as it avoids any political and commercial influence. And there are no political, ideological, or specific learnings present since the source is aimed as proving a campaign idea that can help people be better prepared for cybersecurity threats.

## **Constraints and Criteria**

Choose your favorite/best benchmarked solution from above and read the definitions of **constraints** and **criteria**. Consider how success was measured in that solution and what limitations the designers had when creating it. Hint: This information can be extrapolated from the questions you answered above. Then list out possible constraints and criteria for the solution chosen. You will use this information in class.

**Constraints:** Requirements and limitations that need to be addressed in order to accomplish a goal  
**Criteria:** What your solution has to do in order to be successful. A measure of success.

**Example problem:** increasing safety in manufacturing labs

**Example constraints:** Can the room layout stay the same? Are all walkways at least 4 feet wide?

(Answering ‘yes’ would indicate a viable solution, ‘no’ would remove that solution from consideration)

**Example criteria:** provide greater access to PPE, provide proper storage for student belongings, provide access to tools for cleaning work areas, promote a distraction-free environment, equipment use information is intuitive.

**Solution:**

The National Institute of Standards and Technology (NIST) proposed a Cybersecurity Awareness and Training Program designed to help organizations bridge the gap between knowing and doing when it comes to cybersecurity. The program promotes regular awareness campaigns, behavior-based training, and leadership involvement to build a lasting “security culture.”

**Possible criteria (as many as possible):**

Final Project Journal  
Purdue University

For this solution to be successful, it is crucial that IT staff and cyber experts are recruited to ensure proper teachings. Distribution of materials and a proper teaching setting is needed to ensure the campaign is successful. Materials will also need to be supplied by the institution that chooses to adopt this particular cyber campaign but other than that, following these protocols will work.

Possible constraints (as many as possible):

Does the environment for the campaign have to be academic? Will size limits matter for consumers? Can people with just IT certifications be employed?

## Meeting 15 - Multicriteria Analysis

<b>Group Members:</b>	Samuel Winiger, Derek Woodward, Abhishek Sunkara, Seungchan Kim, Ishmeet Thethi						
<b>Initial POV Statement</b>							
<<This is your initial POV statement derived from your benchmarking and any fieldwork completed at this time>>							
College students frequently neglect cybersecurity best practices despite being aware of the risks. Many rely on convenience, such as weak passwords or unsecured networks, which exposes personal and institutional data to potential attacks. Our group aims to explore why cybersecurity awareness doesn't translate into secure behavior among students and how Purdue can promote better digital safety habits.							
<b>Multicriteria Analysis</b>							
<<Insert a picture of your completed Multicriteria Analysis here>>							
<<Be sure that all elements of your analysis are legible>>							
Solution	Cost Savings	Time to Implement	Effectiveness	Scalability	Available to everyone regardless of their location/background?	Is it engaging?	Total
Weight	0.2	0.15	0.25	0.15	N/A	N/A	
Online training course	10	6	4	10	Yes	No	5.4
Cyber threat practice	10	8	10	6	Yes	Yes	6.6
Gamified cyber awareness training	10	8	10	10	Yes	Yes	7.2
Phishing simulation	10	8	6	10	Yes	No	6.2
Cyber awareness campaign	6	4	10	8	No	Yes	5.5
"Yes" is positive, "No" is negative   scale of 1-10 with 10 being the best							
<b>Constraints and Criteria</b>							

<<Briefly describe each of your constraints and criteria and how you intend to measure (test) them>>

- Cost savings: cost required for tool purchase
- Time to implement: How long will it take to implement the solution? Will be measured in the amount of time it takes to make.
- Effectiveness: Is it unique? Will people be able to learn and memorize for a long time?
- Scalability: Is it able to a large number of people? Can we keep the data up to date?
- Availability: Is it available to everyone regardless of their location and background (language...etc)?
- Engaging: Is it a hands-on experience? Will people get actual opportunities to experience?

### **“Best” Existing Solution and Gaps Identified**

We decided on a gamified cyber awareness solution being the best option. This solution is innovative, and it works well with our end goal. The reason the issue is still around is that this solution is not commonly used, with less engaging solutions being used far more frequently.

<<Why is it the best? Is it innovative? Why doesn't it work for you? If it's good, why does the problem still exist?>>

## **Meeting 17 - Before Class Fieldwork**

\*Remember the minimum requirement for each person and each category. See Brightspace for details\*

Final Project Journal  
Purdue University

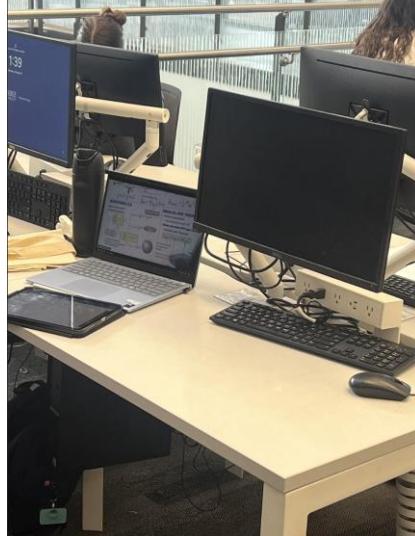
<b>Interviewer Name:</b>	Abhishek Sunkara	<b>Date:</b>	10/27/25
<b>Interviewee Name:</b>	Sandy Galloway	<b>Time</b>	3:30PM
<b>Interviewee Description:</b>	The interviewer is in her 50s and is a person who works at the WALC on the second floor. She mentioned how she isn't as knowledgeable about cybersecurity but will try her best to answer the questions		
<b>Question/Describe-to-Me Statement 1:</b>	Why do you think many students choose convenience (like staying logged in or using public Wi-Fi) over secure online practices?		
<b>Question/Describe-to-Me Statement 2:</b>	What types of cybersecurity habits do you personally follow when using your laptop or phone on campus?		
<b>Question/Describe-to-Me Statement 3:</b>	What has been your experience like when dealing with a cybersecurity threat		
<b>Question/Describe-to-Me Statement 4:</b>	Describe to me the steps you would implement if you were presented with a cybersecurity risk?		
<b>Question/Describe-to-Me Statement 5:</b>	How do you think the older generation is handling the way newer cyber risks are occurring and with them being the target for scams.		
<b>Link to Recording:</b>	<a href="https://drive.google.com/file/d/1KNco2WW9_V4TPZRNbZQC2stnHVL8L1_U/view?usp=sharing">https://drive.google.com/file/d/1KNco2WW9_V4TPZRNbZQC2stnHVL8L1_U/view?usp=sharing</a>		

**Notes, Thoughts, and Observations:**

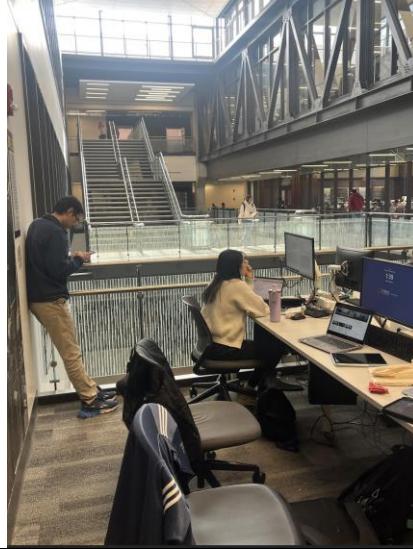
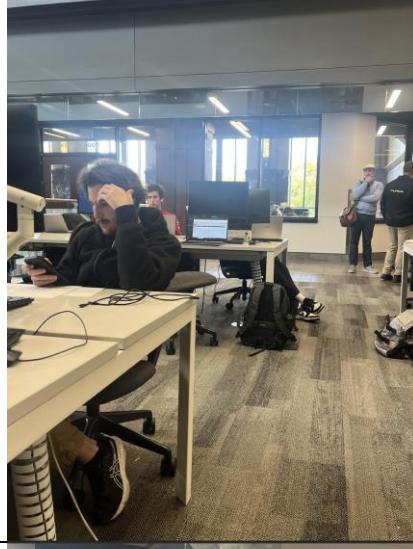
< include personal notes, insights, interesting observations here>

Personal notes - The interviewer tried their best to answer the questions; however, they weren't as knowledgeable. And that is expected because they are of the elder stakeholder group and most older generations won't be as sufficient in the growth of newer technologies

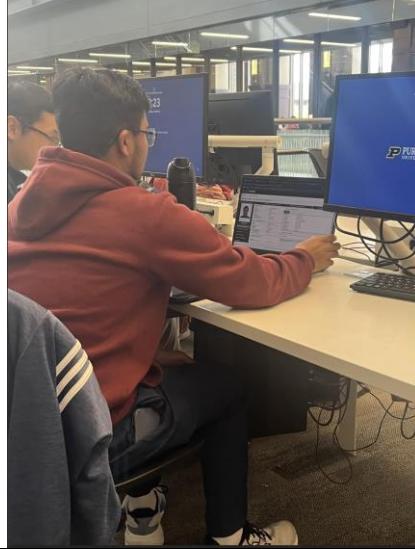
Insights - It was interesting to see how Sandy as an elder would call IT support and not try to deal with the cybersecurity questions on her own

<b>Ethnographic Research - Observation 1</b>		<b>Tech 120</b>	<b>Spring 2024</b>
*note that one observation assignment includes 5 different observations documented in the table below			
<b>Observer Name:</b>	Abhishek Sunkara	<b>Date:</b>	10/27/25
<b>Location Name:</b>	WALC Computer Lounge	<b>Time</b>	1:30PM
<b>Description of Location at the Time of Observation:</b>	The WALC computer lounge is usually crowded with various kids completing their assignments, utilizing the computers in the lounge, and working together on projects. The atmosphere is quiet at times, and the area is a great place to document cybersecurity related work		
<b>URL to Recording/ photo of observation site(s):</b>			
	<b>What?</b> (What are they doing?)	<b>How?</b> (How are they doing it?)	<b>Why?</b> (Why are they doing it this way? Take a guess!)
1	They are leaving their stuff unattended with their computer open and not turned off	The student is not present at their workspace	They are doing it possibly because they feel their stuff is in a secure area and that no one would want to steal their electronics considering it's a library
			

Final Project Journal  
Purdue University

2	A student is seen taking a phone call and leaving their computer open to brightspace	The student is to the side, in the blue shirt, and is on the phone and having his personal brightspace exposes	The student does this because he believes being near his computer is fine enough and so he leaves it on to prevent the process of logging in again		
3	A student has his printer app open but actively left quickly to get his printout	The student left the screen open and didn't close his computer when he left	The student does this because he believes that he is in a safe space and that the destination of the printer isn't far enough to where he would need to turn off his laptop		
4	A student is completing a task on his phone; however, he is leaving his laptop to his side	The student has his computer to the side and is ignoring the fact that his laptop can easily be grabbed	The student is likely doing this because he doesn't suspect that his stuff can be stolen considering stealing laptops isn't a common thing in most colleges		

**Final Project Journal  
Purdue University**

5	A student has his personal dashboard open in a public space	The student is on his dashboard and is trying to view his personal information through myPurdue	The student is likely doing this because he believes no one would attempt to see his personal info considering it has no value to a college student		
< add as many rows as you need >					

<b>Possible problems observed:</b>	Some problems observed include the opening of personal laptops in public spaces and leaving laptops unattended in public spaces. These are common issues most students will do which cause serious cybersecurity risks.
<b>Quantitative data related to problem:</b>	2/5 students leave their laptops unattended, which leads to 40% of students. 5/5 of the students left their screens unlocked when not using them, which led to 100% of students.

<b>Notes, Thoughts, and Observations:</b>
<p>It was interesting to see how almost all of the students in the WALC computer lounge left their laptops unattended. It was also crazy to me how 2 out of 5 of the students left their laptops unattended which poses serious cybersecurity risks. Another thing was seeing people act comfortable viewing personal information in public spaces</p>

### Literature Review - Source #1

**\*Note that all responses need to be in your own words and detailed enough that anyone could understand the source without reading it\***

#### Summarize the source.

The article by Gupta and Shukla (2023) explores how college students create and manage passwords as well as how often they use multi-factor authentication (MFA) to protect their online accounts. The researchers in the study by the article surveys hundreds of students from different universities to measure their understanding of password security, password habits, and their willingness to use MFA

#### What were the findings?

The study found that most students continue to use weak or repeated passwords across multiple platforms such as email, social media, and university portals. Around 68% reused the same password for three or more accounts. Even though over 80% of students were aware that MFA increases security, only 37% actually used it regularly. Major reasons identified by the researchers as to why students skipped the MFA setup was due to convenience, time, and lack of urgency.

#### What is the source saying about your problem?

The source supports the idea that weak passwords and low MFA adoption are serious cybersecurity problems among students. It provides quantitative evidence showing that students often trade convenience for proper security, which leaves them at a higher risk of cyber breaches.

#### What did you learn from the source in regards to your problem?

Based on the source, I learnt that even when students know about cybersecurity best practices, they often fail to apply them in their daily lives. This alone shows how awareness isn't enough to cause change and how behavioral change must be done in order for better cybersecurity practices to be used.

Overall Quality ("x" one):  High       Medium       Low

Citation in APA format (including URL if from Google):

Roberts, L. (2021, June 18). *Who Uses Multi-Factor Authentication?*. BYU ScholarsArchive.  
[https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1187&context=studentpub\\_uht](https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1187&context=studentpub_uht)

Final Project Journal  
Purdue University

<b>Ethnographic Research - Interview 1</b>	<b>Tech 120</b>	<b>Spring 2024</b>
--	-----------------	--------------------

<b>Interviewer Name:</b>	Samuel Winiger	<b>Date:</b>	10/27/2025
<b>Interviewee Name:</b>	Fallyn Ranek	<b>Time</b>	7:30am
<b>Interviewee Description:</b>	Fallyn is a student at Purdue majoring in Cybersecurity who might be able to offer some insight into the problem we are researching as both a student and someone who is knowledgeable in cybersecurity.		
<b>Question/Describe-to-Me Statement 1:</b>	How aware do you think most students are about cybersecurity risks on campus?		
<b>Question/Describe-to-Me Statement 2:</b>	Why do you think cybersecurity is or isn't important for college students to understand?		
<b>Question/Describe-to-Me Statement 3:</b>	Have you ever received any cybersecurity training from Purdue outside of classes?		
<b>Question/Describe-to-Me Statement 4:</b>	On a scale of 1-10 How aware are you on common cybersecurity threats like phishing emails or scams?		
<b>Question/Describe-to-Me Statement 5:</b>	Describe to me the steps you usually take to protect your information while browsing online		
<b>Link to Recording:</b>	<a href="https://drive.google.com/file/d/1LZ2iABvULI7Yb5dDjw3NNljLLTD bq8h/view?usp=sharing">https://drive.google.com/file/d/1LZ2iABvULI7Yb5dDjw3NNljLLTD bq8h/view?usp=sharing</a>		

<b>Notes, Thoughts, and Observations:</b>
---

Of the opinion that most college students are generally aware of the importance of cybersecurity even if they don't know specifics

Thinks it is important that college students know more about cybersecurity, they are for the first time going through life without adult supervision for all their important matters, and they need to know how to keep that important information safe by themselves.

Always be skeptical of sites when browsing the web, especially when you're being asked to offer up sensitive information like credit card details for instance.

Tech 120

Spring 2024

### Ethnographic Research - Interview 2

<b>Interviewer Name:</b>	Samuel Winiger	<b>Date:</b>	10/27/2025
<b>Interviewee Name:</b>	Quan Phan	<b>Time</b>	11:30am
<b>Interviewee Description:</b>	Quan is a student at Purdue majoring in First Year Engineering and can offer some insight into what an average student/a STEM major at Purdue knows about online safety or cybersecurity which can be helpful to know what we should focus on in our solution.		
<b>Question/Describe-to-Me Statement 1:</b>	How aware do you think most students at Purdue are on cybersecurity risks?		
<b>Question/Describe-to-Me Statement 2:</b>	On a scale of 1-10, how secure would you say you feel when connected to Purdue-run wifi connections?		
<b>Question/Describe-to-Me Statement 3:</b>	How confident do you feel in trying to recognize scamming or phishing emails? Why or why not?		
<b>Question/Describe-to-Me Statement 4:</b>	Describe to me what comes to mind when you think about the word "Cybersecurity"		
<b>Question/Describe-to-Me Statement 5:</b>	If you found out that your school account had been hacked or compromised, what would your first steps be? Do you know what your first steps would be?		
<b>Link to Recording:</b>	<a href="https://drive.google.com/file/d/11Xneivyl2xVXXk4mcDJPATphOATnJ8AY/view?usp=sharing">https://drive.google.com/file/d/11Xneivyl2xVXXk4mcDJPATphOATnJ8AY/view?usp=sharing</a>		

### Notes, Thoughts, and Observations:

Thinks that most students probably know a lot about cybersecurity at Purdue

Final Project Journal  
Purdue University

Is more worried/concerned with school administrators being able to access things from students while connected to school wifi than he is concerned about a threat actor  
 Admits that he has trouble identifying scam emails and especially was when he first started getting them  
 Says he would benefit from some form of cybersecurity training from the school  
 Associates cybersecurity with the idea of protecting users from dangers online.  
 Would contact Purdue IT Helpdesk if he found his school account to be compromised  
 Identified that he has a bad habit of accepting all cookies on websites no matter what and he thinks that could be potentially dangerous

### Literature Review - Source #1

**\*Note that all responses need to be in your own words and detailed enough that anyone could understand the source without reading it\***

Summarize the source.

The source first goes into why cybersecurity is such an important topic for college students nowadays, and then goes into some measures college students can take to help reduce risks of cyber attacks and other general good online safety habits.

What were the findings?

Some of the findings that the source mentions are that around 60% of attacks in education come from people's logins being stolen or guessed. It also goes on to identify five key things for college students to be on top of in terms of cybersecurity, securing their devices, using communal workstations safely, setting secure passwords, ensuring site safety when browsing the web, and preventing phishing and other scams.

What is the source saying about your problem?

The source reaffirms the idea that college students are particularly vulnerable when it comes to cyber attacks and it further offers some steps to take to help college students protect themselves from their potential vulnerabilities.

What did you learn from the source in regards to your problem?

It was helpful in both learning some potential points to implement in our solution and also is valuable for gaining insight into what Purdue already is trying to get students to focus on when it comes to cybersecurity, so those things might be things we focus on reinforcing in our solution.

Final Project Journal  
Purdue University

Overall Quality ("x" one): X High      Medium      \_\_\_\_\_ Low

Citation in APA format (including URL if from Google):

(APA Format: <http://owl.english.purdue.edu/owl/resource/560/07/> or in Academic Search Premier, choose "Cite" on the right when viewing an article if using an academic source)

*Internet safety and cybersecurity awareness for college students.* Purdue Global. (2020, September 17). <https://www.purpleglobal.edu/blog/student-life/internet-safety-cybersecurity-college-students/>

Website URL: <https://www.purpleglobal.edu/blog/student-life/internet-safety-cybersecurity-college-students/>

Starbucks

Starbucks			
WHAT (What are they doing specifically? Be as detailed as possible)			
HOW (How are they doing it?)			
1	Connected to Starbucks Wi-Fi	Joined the public Wi-Fi at Starbucks	They most likely did not have access to any other Wi-Fi networks but wanted connection so they chose to join the public one.
2	Walked away from their computer.	They walked away from their open, logged in computer and walked down the hallway.	Most likely it was to use the restroom or to get water, and they didn't shut their computer for convenience.
3	Opened a QR code that was on the wall outside the store	They used their phone's camera app to scan and open a QR code	They were either curious to where it led or already knew and wanted to go to whatever site the QR code would lead.
4	Charged phone using a public USB outlet	Plugged their phone into a public USB charging port near a table or counter.	Their battery was low and they didn't have a wall charger, unaware of potential "juice jacking" risks.

Final Project Journal  
Purdue University

5	Downloaded a file from an unfamiliar website	Clicked a link on social media or email while connected to Starbucks Wi-Fi and downloaded a file.	They were multitasking and didn't verify the source, thinking the file was harmless.
---	--	---	--

KNOY

	WHAT (What are they doing specifically? Be as detailed as possible)	HOW (How are they doing it?)	WHY (Why are they doing it this way? Take a guess!)
1	Left their laptop unattended	Walked away from their logged-in laptop to grab a drink or talk to a friend.	They assumed it would be safe since it's a familiar environment.
2	Shared files over Airdrop	Accepted the files that were sent to them	They thought it was a classmate or trusted device.
3	Used an unpatched campus computer	Logged into a shared workstation that hadn't been updated.	They just needed quick access to print or check something, ignoring updates.

Final Project Journal  
Purdue University

4	Reused the same password for multiple logins (could tell by password length)	Logged into university and personal accounts using the same credentials.	It's easier to remember one password than several.
5	Downloaded software from an unofficial source	Installed a free version of a program for a class project.	They wanted to save money or time and didn't realize it might contain malware.

Final Project Journal  
Purdue University

**Ethnographic Research - Interview 1**

**Tech 120**

<b>Interviewer Name:</b>	Derek Woodward	<b>Date:</b>	10/14/2025
<b>Interview Setting Description:</b>	Virtual	<b>Time</b>	5:20 PM 10/15
<b>Interviewee Description:</b>	Name: Ethan Odom Major: Civil Engineering		
<b>Question 1:</b>	What is your opinion on public Wi-Fi? a. Would you join them? b. Why do you feel that way?		
<b>Question 2:</b>	If a file was airdropped to you in public, what would your response be? a. Why?		
<b>Question 3:</b>	Do you personally reuse passwords? a. Why? b. Are you aware of the risks of doing this?		
<b>URL to recording or screen capture of discussion:</b>	<a href="https://voca.ro/14BzB4pM9bID">https://voca.ro/14BzB4pM9bID</a>		

Final Project Journal  
Purdue University  
**Literature Review - Source #1**

### 1. Seungchan Kim - Convenience tech habits and student cybersecurity risks

**Summarize the source :** This research mainly focuses on cybersecurity problems in education and why it is important to teach students about cyber safety. It examined 25 research articles, over 100 survey responses and 4 interviews from cybersecurity experts. It discusses why students are getting cyber attacks and how we can prepare them so that they are aware of cybersecurity in the future. This research also talks about why cybersecurity in education matters and what colleges and governments are doing to raise the awareness of cybersecurity issues.

**What were the findings :** The study finds that 42% of the survey participants think that cybersecurity is very important and 28% of them think it's moderately important. However, 73% of the survey participants have never attended any programs related to cybersecurity awareness at their school and 81% of them never received formal cybersecurity training. Additionally, only 45% of them felt that they are confident about understanding the basic cybersecurity principles. The interviews from the experts showed what the real problem was. The real issue was that over 70% of the cybersecurity companies say that more than half of the graduates don't have the skills needed for cybersecurity jobs and only 27% of them are qualified. The main issue was that they had a lack of hands-on training experience and they had a lack of IT knowledge. They also said that there is a lack of qualified professors who can teach students about real cybersecurity and the budget for cybersecurity programs are insufficient which makes students now get enough access to proper equipment for cybersecurity education.

**What is the source saying about your problem?** The source is saying that students choose convenience over security when they use digital technologies. Today, students use their devices a lot for education, socializing and more but they don't receive proper and enough training on how to stay safe online. The research says that COVID 19 made things worse since the use of digital devices has increased dramatically during that period without students understanding the cyber threats. The source also says that the current education system does not provide enough hands-on training experience and the teachers themselves are not aware of the cybersecurity risks. Moreover, it states that schools also struggle with adapting additional cybersecurity courses and tools due to lack of their budget.

**What did you learn from the source in regards to your problem?** From this source, I learned that preferring convenience and ignoring the safety risk can cause big problems. I also learned the reality of cybersecurity risk awareness since most of the students didn't have any cybersecurity training or knowledge training. Another thing that I learned was the job market for the cybersecurity field. I learned that the lack of cybersecurity training leads to less students being aware of the basic knowledge, which makes less people apply and actually qualify for cybersecurity job positions.

Overall Quality ("x" one):  High       Medium       Low

Citation in APA format (including URL if from Google):

Shelim, R. (2024, August). *Montclair State University Digital Commons*. Cybersecurity in Education .

<https://digitalcommons.montclair.edu/>

**Website URL:** <https://digitalcommons.montclair.edu/cgi/viewcontent.cgi?article=2445&context=etd>

## Literature Review - Source #2

### 1. Seungchan Kim - Public WiFi Security Risks for Students

**Summarize the source :** This source focuses on the danger of using public wifi networks in locations such as airports, cafes, or hotels. The course explains how these networks are often unsecured and open to people allowing easy access to personal data that puts users in danger. The article explains that hackers can exploit public wifi networks to get personal data and inject harmful software into our devices that steal sensitive information regularly. It also proposes some methods and solutions to this issue to keep users safe from cyber attacks.

**What were the findings :** This article identified 4 main risks of public wifi. First risk found was man-in-the-middle attacks in which the hackers can position themselves between our devices and the wifi network and intercept our communications and steal personal data. The second risk found was data theft which means that unsecured wifi and websites can expose our activities and data and hackers can capture this information. Third risk found was the malware injection which Attackers can exploit vulnerabilities in public Wi-Fi to inject malware into connected devices. This malware can steal data, damage your system, or even give hackers remote access. Fourth risk found was the rogue hotspots which the cybercriminals can create fake wifi networks and monitor devices that are connected to those. After these risks, the study also proposed some solutions and how to stay safe from public wifi. It said that using VPN can help us protect personal data and enabling multi factor authentication can make it harder for hackers to access our information. It also mentioned using https websites, turning off sharing features, disabling auto connecting features, keeping our software updated, and using a firewall.

**What is the source saying about your problem?** The source is saying that the public wifi can create serious cyber security problems for students and anyone who uses these networks since they are easier for hackers to get our information. The article emphasizes that knowing how to stay safe on a public network is important for protecting our personal data. The main problem of public networks is that they don't have built in security measures which makes it easier for cybercriminals to spy on users, steal our data, and trick them into connecting fake networks. This source argues that people should understand and know these specific threats and take action to protect themselves from these risks.

**What did you learn from the source in regards to your problem?** From this source, I learned that public wifi has a lot of differences compared to private networks. I did not know the real difference between those 2 and used to use public wifi more than private wifi when I am out of home. From this source I learned specific issues and risks of using public wifi. Moreover, I could learn lots of ways to prevent myself from getting into cyber attacks. I learned about the usage of https websites and VPN for safety and features such as sharing features and auto connection features that can increase the danger of cyber risks.

Overall Quality ("x" one):  High  Medium  Low

Citation in APA format (including URL if from Google):

*Understanding the Risks of Public Wi-Fi and How to Stay Safe.* Understanding the risks of public wi-fi and how to stay safe. (n.d.). <https://tdx.vanderbilt.edu/TDClient/33/Portal/KB/PrintArticle?ID=286>

Website URL: <https://tdx.vanderbilt.edu/TDClient/33/Portal/KB/PrintArticle?ID=286>

Ethnographic Research - Interview 1	Tech 120	Fall 2025
-------------------------------------	----------	-----------

<b>Interviewer Name:</b>	Seungchan Kim	<b>Date:</b>	October 24th, 2025
		<b>Time</b>	11:07pm
<b>Interviewee Description:</b>	His name is Woohyun Kim and he is a freshman at University of Maryland majoring Mechanical Engineering.		
<b>Question/Describe-to-Me Statement 1:</b>	Do you use public wifi at locations such as hotels, airports, or cafes?		
<b>Question/Describe-to-Me Statement 2:</b>	Do you know what specific risks there are using a public network?		
<b>Question/Describe-to-Me Statement 3:</b>	Have you ever been educated about cybersecurity or public network risks? Have you ever been offered to participate in a related program?		
<b>Question/Describe-to-Me Statement 4:</b>	What kind of resource or training do you think will be helpful for students to be more aware of these risks? - describe me statement (personal opinion)		
<b>Question/Describe-to-Me Statement 5:</b>	How do you think college can help you gain experience about cybersecurity or public network risk? - describe me statement (personal opinion)		
<b>Link to Recording:</b>	<a href="https://drive.google.com/file/d/1o44IxhvYQ4wWbLNDF_rAOYuy_Lt09W2C/view?usp=sharing">https://drive.google.com/file/d/1o44IxhvYQ4wWbLNDF_rAOYuy_Lt09W2C/view?usp=sharing</a>		

Notes, Thoughts, and Observations:
<ol style="list-style-type: none"> <li>1. He said that he uses public wifi often at public locations since they are easy and free to connect when he is lack of mobile data.</li> <li>2. He knows that public wifi allows hackers to access our personal information such as passwords easily.</li> <li>3. He hasn't really been educated about cybersecurity since his school did not offer. He also does not have any program experience.</li> <li>4. He thinks that short videos, workshops, games, or quizzes will help students be aware of cybersecurity and public networks.</li> <li>5. He thinks that colleges can offer more courses about cyber safety and teach safety for their devices when connected to public wifi.</li> </ol>

Final Project Journal  
Purdue University

Overall, his interview shows the current situation about cybersecurity. It seems like there is a lack of education and resources available to students. Additionally, he proposed some solutions to increase cybersecurity awareness.

### Literature Review - Source #1

**\*Note that all responses need to be in your own words and detailed enough that anyone could understand the source without reading it\***

**Summarize the source.**

**What were the findings?**

**What is the source saying about your problem?**

**What did you learn from the source in regards to your problem?**

Overall Quality ("x" one):     High                       Medium                       Low

Citation in APA format (including URL if from Google):

Website URL:

## Meeting 17 In Class - Thematic Identification & Composite Character Profile

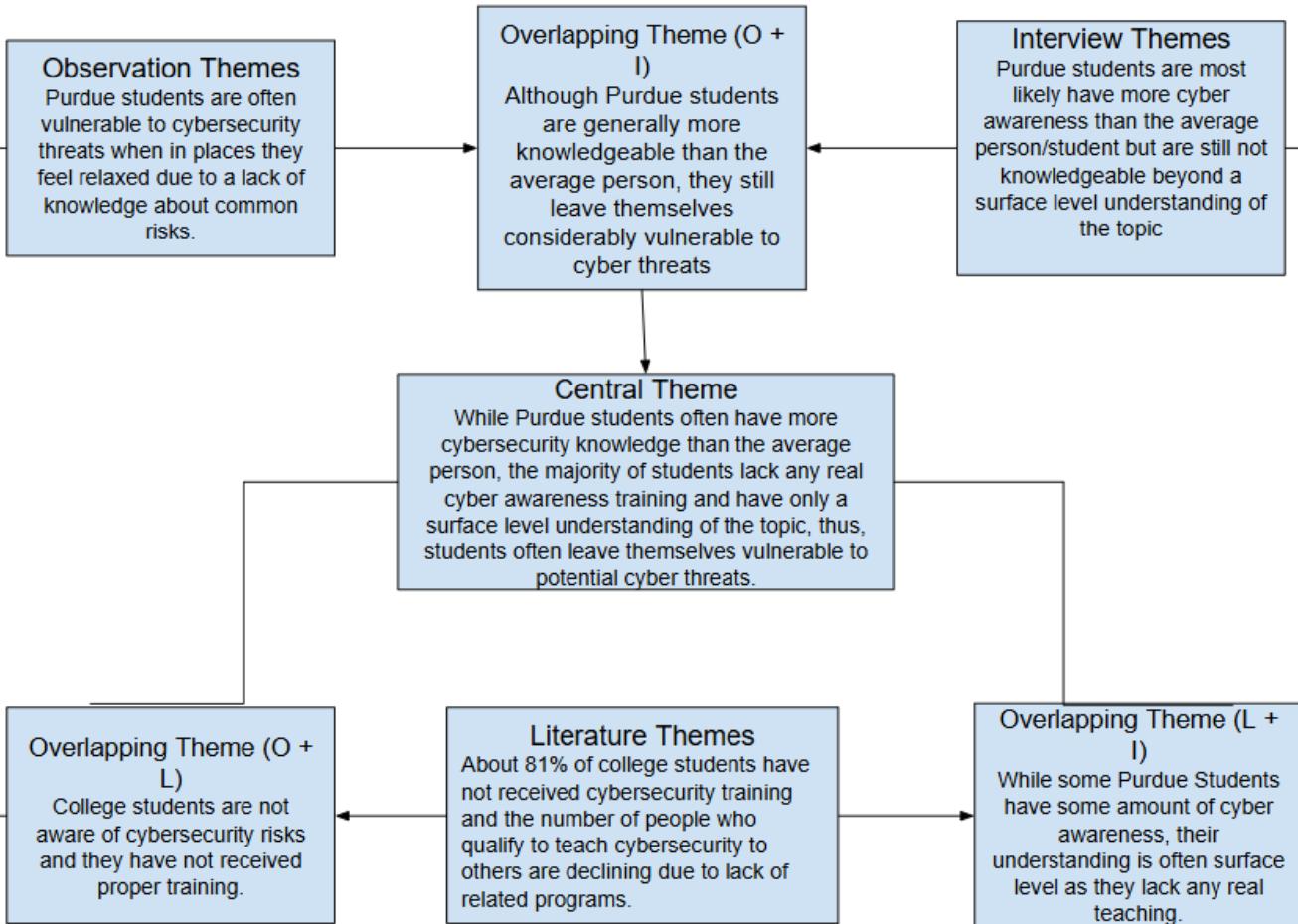
**Names:** Samuel Winiger, Derek Woordward, Seungchan Kim, Abhishek Sunkara, Ishmeet Thethi

**Initial POV Statement:**

College students frequently neglect cybersecurity best practices despite being aware of the risks. Many rely on convenience, such as weak passwords or unsecured networks, which exposes personal and institutional data to potential attacks. Our group aims to explore why cybersecurity awareness doesn't translate into secure behavior among students and how Purdue can promote better digital safety habits.

**Thematic Identification:**

**Final Project Journal**  
**Purdue University**



**Revised POV Statement:**

While Purdue students often have more cybersecurity knowledge than the average person, the majority of them lack any real cyber awareness training and have only a surface level understanding of the topic, thus, students often leave themselves vulnerable to potential cyber threats.

**Composite Character Profile**

Final Project Journal  
Purdue University

Picture of User:



Source : Gemini generated

Characteristics related to the problem space and fieldwork results:

Individual: Ryan Ma

- Freshman
- Political Science major (Not cybersecurity major)
- Purdue student
- High School didn't have cybersecurity program
- Uses technology a lot, especially for school related activities
- Has not had prior cybersecurity training
- Often uses public Wi-Fi at college, instead of secure net (PAL/eduroam)

\*Note: Your composite character is the person that represents your user group. That group is who you'll do your prototype testing and data collecting on\*

## Meeting 18 - Before class ideation [Individual]

\*Each group member's ideas should be put here. Include the member's name with the ideas.

Samuel Winiger:

**Functions:**

**Educate students**

- **Make cybersecurity awareness videos**

**Make learning engaging**

- **Gamified learning material to help reinforce ideas**
- **Host cybersecurity education/awareness events with related clubs**

**Involve knowledgeable students**

- **Have Cybersecurity Students educate their peers for a project (Like a presentation for example)**

**Reinforce good online habits:**

- **Develop a phishing identification simulator with a simple reward system**

Derek Woodward

**Functions:**

- Educate students on real-world cyber risks.
  - Develop short, scenario-based modules featuring real Purdue student stories.
- Engage students in interactive, memorable training experiences.
  - Build a gamified training app with points, levels, and badges.
- Encourage secure digital behaviors (password management, phishing awareness, data privacy).
  - Provide a browser extension or app that gives real-time feedback on risky actions
- Motivate consistent participation and long-term retention of cyber-safe habits.
  - Offer rewards: certificates, dining credits, or resume badges.
- Assess and reinforce progress in understanding and behavior
  - Periodic quizzes and feedback dashboards.

Abhi Sunkara

**Functions:**

- Gamify cybersecurity with a campus-wide “Hack Me If You Can” competition.
- Create a dessert stand where people can receive free sweet treats if they answer some questions about cyber risks
- Have campus-wide “Cyber Safety Week” events with prizes, memes, and workshops.

Final Project Journal  
Purdue University

- Offer bonus points or dining dollars for students who complete cybersecurity training.
- Launch a “Cyber Fails” board where anonymous funny cybersecurity mistakes are shared to educate others.

Seungchan Kim

Ideas :

- Cybersecurity app with point awarding system
- Daily mission app with daily quiz/activity + reward
- Vouchers for cybersecurity task completion
- Pop up cybersecurity knowledge test before connecting to public network
- Game designed cybersecurity app

1. List of Ideas

- Game designed cybersecurity app
- Point system cybersecurity app
- Online training website
- Cybersecurity workshop
- Cybersecurity poster
- Public network pop up message system

2. Criteria 1 : Is it hands-on experience?

3. Narrow down:

- Game designed cybersecurity app
- Point system cybersecurity app
- Cybersecurity workshop

4. Expand:

- + Daily Mission app that with daily quiz/activity + reward per rank

5. Additional Criteria : Does it benefit participants / has a hook?

6. Narrow Down :

- Game designed cybersecurity app
- Point system cybersecurity app
- Daily Mission app that with daily quiz/activity + reward per rank

## Meeting 18 - In-class ideation

Peturbation Method

1. List of Ideas

- Cybersecurity poster competition
- Food /Drink coupon/voucher reward system for daily cybersecurity task completion

2. Repeating...

- Cybersecurity knowledge test before connecting to public wifi
- Add watching requirement before connecting wifi

lock completion

Final 5 solutions

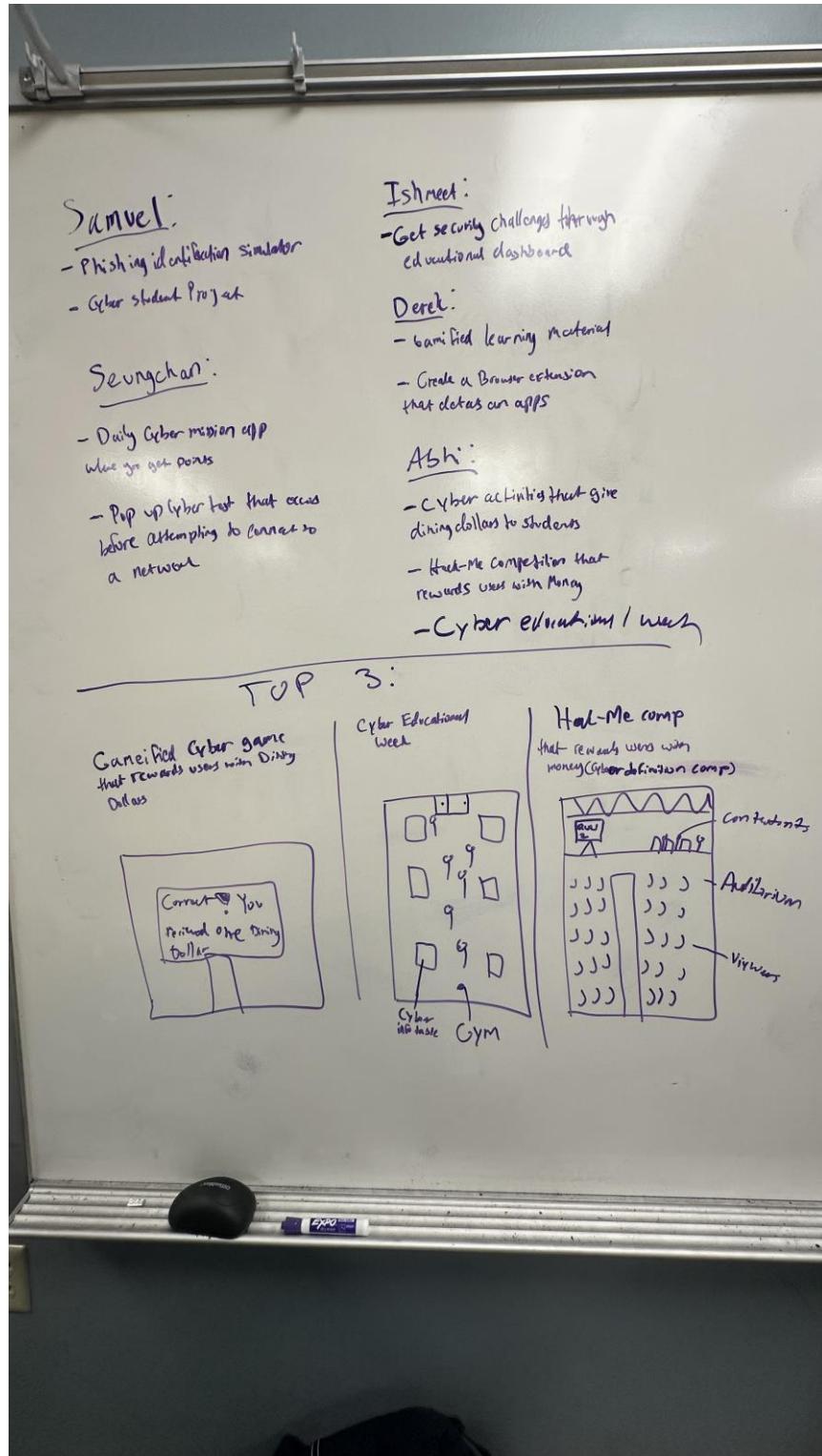
- Game designed cybersecurity app
- Point system cybersecurity app
- Daily Mission app that with daily quiz/activity + reward per rank
- Food /Drink coupon/voucher reward system for daily cybersecurity task completion
- Cybersecurity knowledge test before connecting to public wifi

<b>Names: Samuel Winiger, Derek Woodward, Seungchan Kim, Ishmeet Thethi, Abhishek Sunkara</b>
---

<b>POV Statement:</b> While Purdue students often have more cybersecurity knowledge than the average person, the majority of them lack any real cyber awareness training and have only a surface level understanding of the topic, thus, students often leave themselves vulnerable to potential cyber threats.
---

**Final Project Journal**  
Purdue University

Ideas developed (remember who you're designing for:



**Three grouped ideas to mock up from the above list OR from before class:**

1. Gamified cyber game that rewards users with dining dollars
2. Cyber educational week
3. Hack me competition that rewards with money

**Next steps - In class Meeting 18 (After you choose the top 3 ideas from before class OR in class)**

1. Determine a plan of who will create the mock-ups of all 3 ideas and how they will be built (refer to Meeting 19 before class as well)
  - a. Mock-ups are VERY quick representations of ideas
  - b. Typically made of paper, readily available materials, or computer models

Abhi Ishmeet - **Gamified cyber game that rewards users with dining dollars**

Samuel, Derek, Seungchan - **Cyber educational week diagram & Hack me competition that rewards with money**

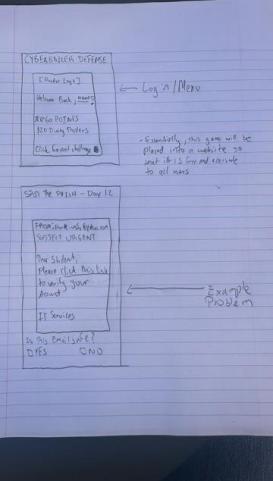
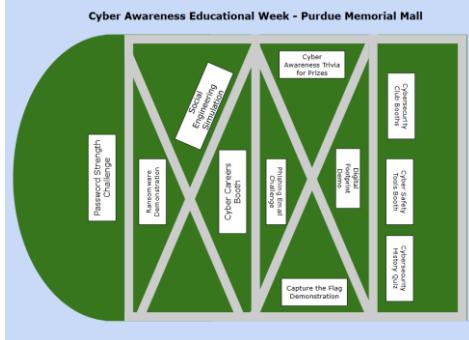
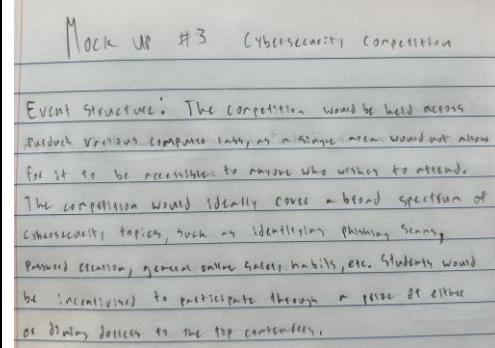
The gamified cyber game will be created through a computer model. Possibly through a software of some sorts

The Cyber educational week diagram & Hack me competition that rewards with money will be represented through a layout of how we envision the week/competition to be run.

## Meeting 19 - Before class Solution Analysis

2. Create/build the 3 mock-ups before class
3. Develop a short pitch of:
  - a. Why each idea is viable to your problem
    - i. What your problem space is
  - b. How the solutions are innovative
  - c. How closely do they align with your constraints and criteria

**Final Project Journal**  
**Purdue University**

Mockup #1	Mockup #2	Mockup #3
 <p><b>Cybersecurity Defense</b></p> <p>Log A/Memo</p> <p>What's your name? Rebecca Roberts Rebecca Roberts Click Event Survey</p> <p>It's probably that game will be placed into a website so send it to me and I will do all the work.</p> <p>SURVEY - Day 12</p> <p>How much do you know about cybersecurity? Very Little Some A lot Know everything It's not important?</p> <p>Do you think it's important? YES NO</p> <p>Example Problem</p>	 <p align="center"><b>Cyber Awareness Educational Week - Purdue Memorial Mall</b></p> <ul style="list-style-type: none"> <li>Physical Challenge</li> <li>Maintenance Competition</li> <li>Social Engineering Station</li> <li>Cyber Careers Booth</li> <li>Photo Op</li> <li>Capture the Flag Demonstration</li> <li>Cybersecurity Awareness</li> <li>Photo Op</li> <li>Cybersecurity Awareness</li> <li>Photo Op</li> <li>Cybersecurity Awareness</li> </ul>	 <p align="center"><b>Mock Up #3 Cybersecurity Competition</b></p> <p><b>Event Structure:</b> The competition would be held across multiple locations (competition lobby, main lounge, etc.). It would not allow for it to be accessible to anyone who wishes to attend. The competition would ideally cover a broad spectrum of cybersecurity topics, such as identifying phishing scams, password cracking, general online safety habits, etc. Students would be incentivized to participate through a prize of either \$100 or \$500.</p>

<p>while fitting student schedules and requiring no special equipment.</p> <p><b>How mock-up represents the solution</b></p> <p>Our mockup shows two screens: the home dashboard displays progress, and dining dollars earned, driving engagement through visible rewards. The phishing challenge shows interactive learning where students practice identifying real threats.</p>	<p>able to engage a large amount of students that any students could come and learn from at their own convenience, however with it being a large event that lasts a fairly long time, about a week, it might not be ideal when it comes to cost and preparation time so some concessions would have to be made in those aspects of our constraints.</p> <p><b>How the mock-up represents the solution:</b></p> <p>This solution would be an event that takes place on campus, so the mock-up is a diagram or layout of said event which shows some potential booths or activities that could take place at the event throughout the week that give a general idea of what we see as being important for Purdue students to be knowledgeable of.</p>	<p><b>Mockup:</b></p> <p>Our third solution was to create a cybersecurity competition with a prize of either dining dollars or cash. Due to our solution being an event, a physical mockup wasn't possible. Due to this, our mockup is an explanation of the event's structure, allowing one to quickly understand how the event would work.</p>
--	---	--

\*Bring mockups to class and be ready to present the information above to half of the class to gather feedback on your most viable solution idea.

**Names:** Ishmeet Thethi, Abhishek Sunkara, Derek Woodward, Seungchan Kim

**Feedback/Critique received after pitch:**

- Offer certificates to incentivize students to participate in the hackathon event
- Make it usable on the phone (The gamified cybersecurity training)
- Compare your progress with other students (Like a competition function of the game)

**What more do you need to know (action items)?**

Research the feasibility of integrating dining dollars as rewards through university systems

Determine the technical requirements for developing a mobile-compatible game

Investigate what types of certificates or credentials would be valuable to students

Explore gamification features that enable peer comparison and competition

Assess budget requirements for prize money/rewards for the competition format

**Which solution idea is your group choosing? Why?**

Our group is choosing the Gamified Cyber Game that rewards users with dining dollars (Solution #1).

It directly addresses our revised POV statement by providing the "real cyber awareness training" that students currently lack, and the feedback from our interviews specifically mentioned that students want "games and quizzes" for learning. Once built, it can continuously engage students without requiring recurring event planning, and also furthermore aligns best with our constraints: engaging, accessible to everyone, requires no special equipment, and can be implemented within our timeframe.

*Think about the future. You will have to build a more detailed prototype, develop a usability test with clear testing conditions, and test functions of your solution with your user group (composite character profile). Look ahead in Brightspace for further details.*

**Reflect:**

Does the solution you picked solve your problem? Can your solution be implemented? Will you be able to prototype and test your solution to see if it works? How do you know?

Yes. Our problem is that Purdue students have surface-level cybersecurity knowledge but lack real training, leaving them vulnerable. This gamified solution provides the hands-on, engaging training they're missing. By using Purdue-specific scenarios from our observations (like the WALC situations where students left laptops unattended), we're addressing real behaviors we documented. The solution can be implemented as a mobile web app or native app. We can start with a basic prototype using available development tools and platforms. The dining dollar integration will of course require partnership with Purdue Dining, but this is supposed to be a prototype, not an entire app.

We know this will work because we're able to test this with students matching our character profile (non-cybersecurity majors, freshmen with limited training) by having them complete scenarios and measuring:

- Engagement time and completion rates
- Knowledge improvement (pre/post scenario questions)
- User feedback on interface and experience
- Behavioral intent changes

And in return, we will get measurable statistics doing so (roughly matching our research).

## Meeting 20 - In-Class Prototype Development and Planning

Names: Samuel Winiger, Ishmeet Thethi, Derek Woodward, Abhi Sunkara. Seungchan Kim

Develop a plan for your prototyping building and testing sequence by addressing the points below. Record your responses on the document. Notice the rubric before starting.

1. Think backward: if your solution was complete, how many functions would it have? For instance, your smartphone has biometric support, a few cameras, a touch screen, speakers, microphones, and so much more. As a group, make an exhaustive list of all of the functions your solution would have - be as detailed as possible.

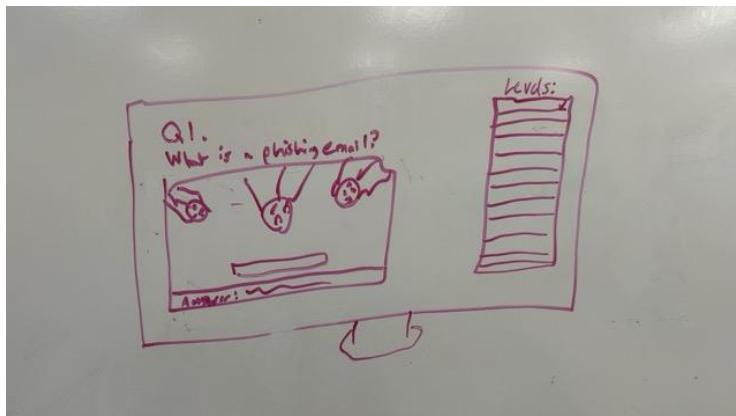
### Functions:

- Incorporation of a reward system (Points system)

- Displays questions randomly
  - Question Database
  - Is accessible from a variety of devices/locations
  - Dashboard/Start Menu
  - Leaderboard/Keep track of scores
  - Website has a URL
2. Then, as a group, decide how many of those functions you can properly build and test and then commit to that - you don't have to do it all if there's a lot. Consider a few things: 1) take a risk! If you go for the big thing and it fails, you can learn from that failure and do it better next time; 2) if you have a larger group, take on more functions; 3) think of the capabilities of each group member and what their skills are; 4) think about how much time you each have and what can work in your schedules (if you have more time, take on more functions); 5) think about how your prototype will be made (e.g., 3D printing takes hours, Amazon ships in 2 days, etc.), and 6) what are your higher priority design requirements?
- Most of the functions are things that we can reasonably accomplish, but if we were to aim to focus on the most important tasks, the main priority would be having a question database that can display questions randomly. The second most important goal would be to incorporate a reward system to keep participants engaged. The website URL would be auto generated by GitHub, and the least important goal among our functions would be having a publicly displayed leaderboard.
3. Think about and choose which digital tool you might use if you haven't already

We will be using GitHub to store our code. A webserver will be provided by one of our group members to host the instance. It is likely we are going to utilize Python in the back-end systems for development and then some sort of JS full-stack platform (i.e. NextJS) for the front-end.

4. Draw detailed sketches of what your prototype might look like



5. Plan out your prototype test. Consider the following:

- a. Simply surveying your user group does not fit the requirement of a prototype test.
- b. How will your solution be used in the real world? Consider replicating those conditions for your users.

Users will access the prototype on their own devices (phones/laptops)  
They'll complete it in a natural setting (dorm room, library, between classes)  
Time pressure similar to real decisions (5-10 min total)  
Scenarios based on actual Purdue situations we observed

c. What do you want your users to do?

Create an account/login  
Complete 5 cybersecurity scenarios  
Receive immediate feedback on each  
See their points accumulate  
Complete a brief post-test questionnaire

d. How long will the test take?

Core prototype interaction: 8-10 minutes  
Post-test questionnaire: 3-5 minutes

e. How many users should you test on to see how well/not well your prototype work?

Number of users: Target: 10-20 users (minimum 10)

f. What are your higher-priority design requirements and what sort of test aligns with them?

Design Requirement	Test Method
Engagement	Track completion rate, time spent, voluntary continuation
Effectiveness	Pre/post knowledge questions on each scenario
Ease of use	Task completion rate, error tracking, SUS score
Behavioral change	Post-test questions about intent to change habits

g. What makes sense to test based on what you're building?

Can users navigate the interface intuitively?  
Do the scenarios feel relevant to Purdue students?  
Does the point system motivate continued use?  
Do users learn from immediate feedback?  
Would users recommend this to their peers?

h. What data do you need to collect to learn about your prototype efficacy?

**Quantitative Data:**

1. Completion rate (% who finish all 5 scenarios)
2. Time spent per scenario
3. Correct answer rate (pre vs. post similar questions)
4. Points earned
5. Click patterns/navigation paths

**Qualitative Data:**

1. Open-ended feedback questions:
  - a. "What did you like most?"
  - b. "What was confusing?"
  - c. "Would you use this again? Why/why not?"
2. Observation notes during testing
3. Specific feature feedback (points, scenarios, design)

\*Be sure to take pictures of your group building the prototype for future use

\*\*Extract only the necessary page(s) for submission

## Meeting 21 - Before Class Prototype Building and Testing Development

\*Your prototype is not due yet. We are looking at your progress so far\*

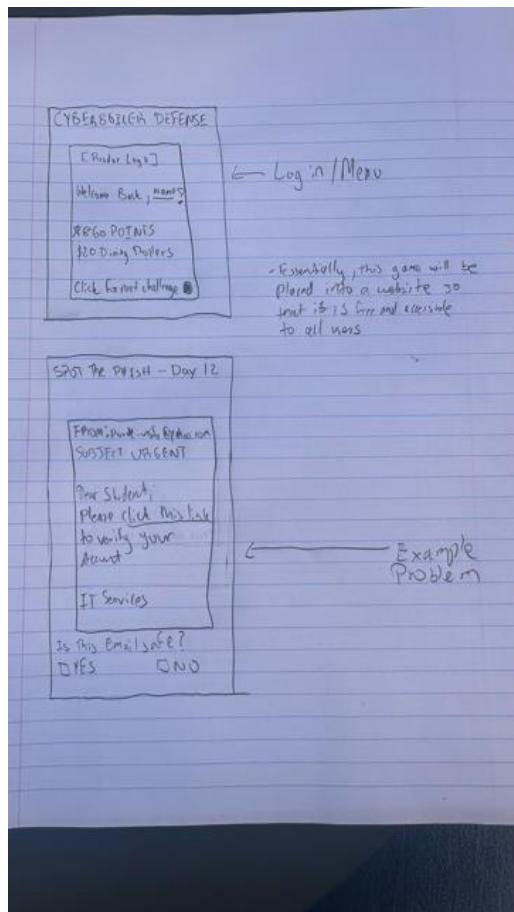
Names: Samuel Winiger, Abhi Sunkara, Ishmeet Thethi, Derek Woodward, Seungchan Kim

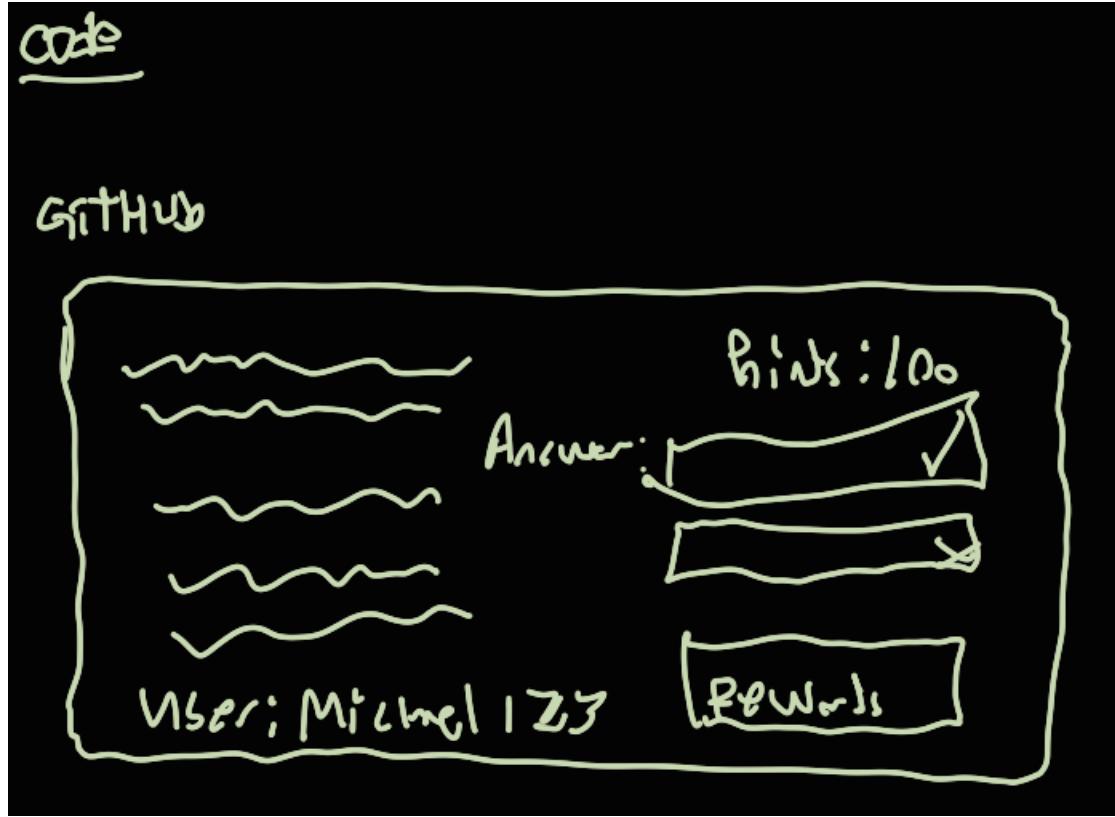
Provide all details and descriptions of your group prototype building below. Notice the rubric before starting!

- Description of the prototype (how you will make it, what it will be made of, etc.)

The prototype will be made/coded by our group on Github, it will be a rough model of an educational cybersecurity game with the most important functions present such as a menu, points/reward system, and some game functionality like a leaderboard and cybersecurity questions pulled from a question database.

- Preliminary sketches of prototype





- Description of the functionality(ies) being investigated by the prototype

The menu of our prototype will allow users to input a username and password for their “account” and continue on to the game. The game will consist of asking the user cybersecurity questions, pulled from a list of questions, that will then explain to the user why the correct answer is correct, and save their point total which can then be stored with a leaderboard and used as part of the “reward” system allowing users to gain something like dining dollars for answering questions correctly.

- Description of relevant test conditions
  - Which constraints/criteria will be tested?

We want to make sure the game is engaging for users, so they learn from the experience. In addition, the game should be easily accessible for all students, including not requiring any special equipment beyond what you’d expect a university student to have, a computer. We also want our solution to be relatively quick to implement so that students can engage with it as soon as possible. Our idea is to test our solution on Purdue students who don’t have much advanced knowledge on cybersecurity topics and survey them before and after so we can get an idea of how helpful our solution can be for the average student at the school. We would like to test students with our prototype, getting them to make an “account” and answer questions and receive instant feedback on their answers from the prototype, save their point total and ask them questions ourselves about their experiences afterwards.

\*Be sure to take pictures of the prototype while being built for future use

\*\*Extract only the necessary page(s) for submission

## Meeting 21 - In-Class Prototype Feedback/Critique

Names: Samuel Winiger, Abhi Sunkara, Ishmeet Thethi, Derek Woodward, Seungchan Kim

Description of design being presented: Cybersecurity game (website) such as wordle that users can enjoy daily.

There will be a reward system that you can get each time you participate, and you will be able to convert those to vouchers or dining dollars. The daily questions/tasks will be randomized every night.

### Solicit feedback for your prototype and testing plans

Positive Feedback	What Still Needs Work?	Suggestion for Improvement
Having reward system	Consider if you'll need to collaborate with Purdue to make the solution successful	Alternative rewards, ideally non-monetary such as bragging rights or in-game titles/rewards.
Easy accessibility for users is necessary	Will you be making this a website vs app?	Explore making the game more competition focused
New tasks/questions everyday	How would we prevent cheating?	Consider testing the prototype on more than just Purdue students.
	What will be the conversion rate from points to dining dollars?	Survey testers on the engagement felt from the prototype.
	How will questions be generated?	Consider making questions random for each user to prevent answer sharing.

\*Add more rows as necessary

Select the top 5 feedback items for your **prototype** AND the top 5 feedback items for your **testing** and respond to them below. Be sure to include a plan to address each feedback item.

Alternative rewards:

- The issue here is finding a reward that is non-monetary while also large enough that users are motivated to be engaged with the game. Due to this, many rewards such as in-game titles would likely be too small of a motivator to keep students engaged with the product. Overall, the ideal reward would likely have to be monetary but at a ratio where a significant number of points are required to claim the rewards.

Explore making the game more competitive:

- We have considered including some sort of leaderboard or way to keep track of scores so students can compete against other students or against their own highest score. Perchance points could be based on correct answers and time taken per question.

Do you need collaboration with Purdue?

- Unless we decide to have dining dollars as a reward system, we might not need collaboration. However, it is encouraged since Purdue might be able to support us to afford the rewards.

How would you prevent cheating?

- We can set a time limit for each question to ensure that they don't really have time to move onto another tab and search for the answer. We can additionally randomize questions for each user, so users cannot share answers or find them online.

Will you be making this a website or app?

- We can make a website since there will be no need for the users to download, which takes another step. However, individuals who decided to participate in the reward system would be required to make an account to save progress.
- We will utilize software such as python for the back end of our game and for the front end we can use Next J S

Consider testing the prototype on more than just Purdue students:

- We could potentially test our prototype with non-Purdue students, however since our target audience or user group would be Purdue students, it might still just be best to test it on Purdue students as they presumably would be the only ones to use it.

Survey testers on engagement:

- We will be asking our testers about how engaging it felt for them to do the questions and asking them if they would do this daily.
- We will also get feedback from users for future rewards and see what type of reward they are looking for.

\*\*Extract only the necessary page(s) for submission

## Meetings 22 & 23 - Small Group Conference

Type a list of action items from your instructor and create a tentative plan of who will address them and when they need to be completed. Submit only the relevant pages for the assignment.

### Ideate and create start/main menu

- Think of how the start/main menu will look and what specifically can be put on it, i.e. potentially a login (to save their progress and points), start game button, and then put your ideas into practice by making the menu.
- Addressed by: Ishmeet Thethi, Abhi Sunkara

### Create question base

- Make/acquire a large set of cybersecurity fundamentals questions that can be informative to the average Purdue student which your game can draw from. Potentially consider different levels of question difficulty if we want to go down that route. Also consider potentially adding hints for after questions are incorrectly answered
- Questions can be about basic cybersecurity knowledge, phishing emails, risks of using public networks, solutions to those risks, and more.
- Addressed by: Seungchan Kim, Samuel Winiger

### Create question answering method

- Create the actual method in which users can play the game by answering cybersecurity questions and determine potentially which questions will be given.
- There can be a variety of levels, and each level will be awarded different points. However, the total number of questions and points the users can get will be the same among the users.
- Addressed by: Samuel Winiger, Abhi Sunkara

### Create method of keeping track of points/score and leaderboard

- Keep track of their score, also think about how the score/points will be measured (ie just correct or wrong or perhaps also factor in time, can you get a fraction of the points for getting on second, third attempt?)
- Addressed by: Derek Woodward, Ishmeet Thethi

### Create design/layout

- Come up with what the game will look like aesthetically and layout wise, what will the theme be, where are buttons, questions or indicators going to be?
- Addressed by: Seungchan Kim, Samuel Winiger, Derek Woodward

## Meeting 24 - Before Class Prototype Iteration

1. Respond to peer feedback as a group (from Meeting 21)

Final Project Journal  
Purdue University

2. Compile evidence that shows your prototype will function
3. Compile evidence that demonstrates you will perform a suitable usability test
4. Bring all evidence and prototype to class

Note: Your prototype test cannot solely be a survey of interest (would you use it? does this seem useful?). That information is only marginally useful and doesn't tell you if your solution works.

\*There is no submission before class Meeting 24. Please bring your prototype evidence with you to class.

## Meeting 24 - In class Prototype Iteration

Document the feedback your group received in class. Paste the pictures of your prototype iteration below.

## Meeting 25 - Before Class Prototype Finalization

- First prototype (from Meeting 21 before class assignment)
  - description of the prototype (how you made it, what it's made of, etc.)
  - preliminary sketches of prototype
  - one or more pictures of the prototype
  - description of the functionality investigated by the prototype
  - description of relevant test conditions

Final Project Journal  
Purdue University

- which constraints/criteria were tested?
- Finalized prototype (i.e., descriptions of changes made based on peer feedback; after Meeting 21)
  - description of the prototype
  - picture of the new prototype iteration
  - discussion of what changes will be incorporated based on the results of /findings made by testing your prototypes and peer feedback
  - Pictures of most comparable existing product; differences described
  - Pictures/videos of usability testing
  - Logical organization of testing data
    - What did you test?
    - What functionalities were tested?
    - What constraints and criteria were tested against?
    - How did you do it?
    - Who was your user group (composite character profile)?
    - What units of measurement did you use?
    - How long did the test(s) take?
    - How many participants did you test on?
  - Conclusions drawn from testing - what were your findings? (Hint: don't make these up. Another hint: testing CANNOT solely be a survey of interest. Surveys can only be administered AFTER a usability test).
  - Reflection

## Meeting 25 - In Class Presentation Outline

Final Project Journal  
Purdue University

## Meeting 26 - Before Class Design Journal

- Delete the instructions page (in red) from your design journal
- Fill in Title Page
- Update your Table of Contents. Each heading and subheading should have a working link from the table of contents
- Complete the "Meet the Design Team" section
- Complete the Executive Summary
- Check to make sure fonts are the same
- Consider feedback to date.
- Changes to the document should reflect feedback.

**\*Delete this section once you've completed the items above.**