Cybersecurity Escape Room

Highlights

Save the Date – to Escape!

A hacker is trying to break into your devices using social engineering, phishing, malware and other cybercriminal tactics … and the clock is ticking!

It’s up to you to beat the hacker at their own game by working with a group and putting your cyber-knowledge to the test to solve 15 cybersecurity puzzles.

Personas

- Escape Room was designed for participants that are:
  - Curious
    - Enjoy solving puzzles and riddles
  - Adventurous
    - Digging around areas, finding hidden items/lockboxes/clues
  - Preferred interdependence
    - Working as a team to solve the problem
  - Social Contact
    - Must interact and work together to solve puzzles
  - Competitive
    - Event is timed and best time wins a prize
- Employees encouraged to use the event as team building, but could attend independently and be added to a team.

Game Mechanics

- Game Mechanics put into the Escape Room:
  - Achievement
    - “I Escaped” sticker given at the end
    - Picture taken with escape time
  - Advance Priming
    - Video shared story/why of the room
  - Communal Discoveries
    - Some puzzles required multiple participants to track clues to find the answer
  - Puzzle Guessing
    - Had to discover the clue(s), answers and corresponding lockbox that were not always near each other
  - Unlocking
    - Box must be unlocked to get the next clue
  - Hints
    - Team could receive hints from the facilitator, but it would cost them 30 seconds
  - Competition
    - Team with the best escape time featured in company newsletter and received a certificate

The Project

Learning Themes:

- Use strong passwords
- Turn on MFA
- Recognize and report phishing
- Update software
- Overall cybersecurity knowledge

Goal:

Reinforcement training for the company on top human risks.

Metrics:

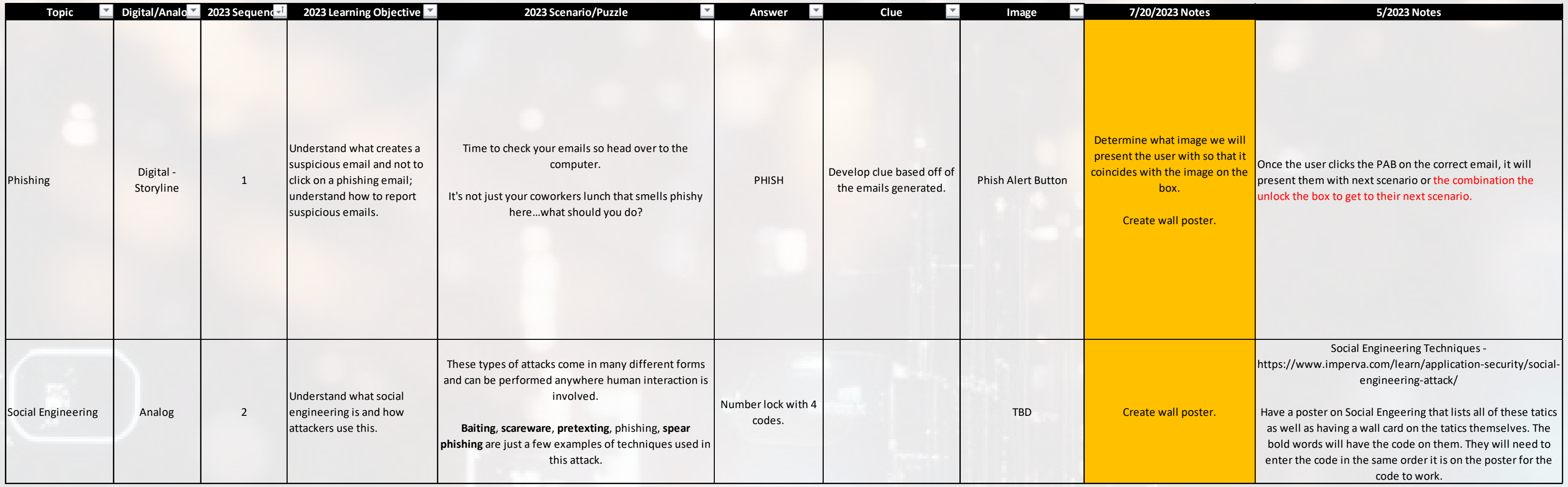
Before and after phishing metrics of participants (90 days prior and 90 days post)

The Project

Other considerations:

- Planning committee
  - Used volunteer employees to help plan scenarios and to facilitate the escape room
- Timeline
  - Project management of deliverables, print materials, digital materials, playtest, room set-up, each team's escape, room tear-down
- Registration
  - Microsoft Forms sign-up
    - Placed into preferred timeslots
    - If timeslot is filled (over 10 participants) given a choice to take another timeslot
    - All timeslots filled by September (9 am, 10,11, 12, 1, 2, 3, 4pm)
- Items needed/already have for the room
  - Lights, props, locks, UV markers, etc.
- Marketing
  - Internal marketing
    - Employee Newsletter
    - Electronic Kiosk
    - Cybersecurity newsletter
    - Intranet
    - In-Person events
- Evaluation
  - Electronic and In-Person
  - Evaluation of learning objectives during escape room
  - Evaluation of escape room after the event

Project Development



Topic	Digital/Analo	2023 Sequenc	2023 Learning Objective	2023 Scenario/Puzzle	Answer	Clue	Image	7/20/2023 Notes	5/2023 Notes
Phishing	Digital - Storyline	1	Understand what creates a suspicious email and not to click on a phishing email; understand how to report suspicious emails.	Time to check your emails so head over to the computer. It's not just your coworkers lunch that smells phishy here...what should you do?	PHISH	Develop clue based off of the emails generated.	Phish Alert Button	Determine what image we will present the user with so that it coincides with the image on the box. Create wall poster.	Once the user clicks the PAB on the correct email, it will present them with next scenario or the combination the unlock the box to get to their next scenario.
Social Engineering	Analog	2	Understand what social engineering is and how attackers use this.	These types of attacks come in many different forms and can be performed anywhere human interaction is involved. **Baiting**, **scareware**, **pretexting**, phishing, **spear phishing** are just a few examples of techniques used in this attack.	Number lock with 4 codes.		TBD	Create wall poster.	Social Engineering Techniques - https://www.imperva.com/learn/application-security/social-engineering-attack/ Have a poster on Social Engeering that lists all of these tatics as well as having a wall card on the tatics themselves. The bold words will have the code on them. They will need to enter the code in the same order it is on the poster for the code to work.

- Built out scenarios for each topic/learning objective with answers, clues and box images
- Added sequence of events to make sure there was enough variety (not spending too much time in one area)
- Escape Room Activity must be completed within 30 minutes, puzzles must be tricky enough to be engaging but not so tricky that a team would get lost
- Red herrings added, but must not take too long
- “Hacking music” used in background to pump/pressure participants

Surprise and Delight

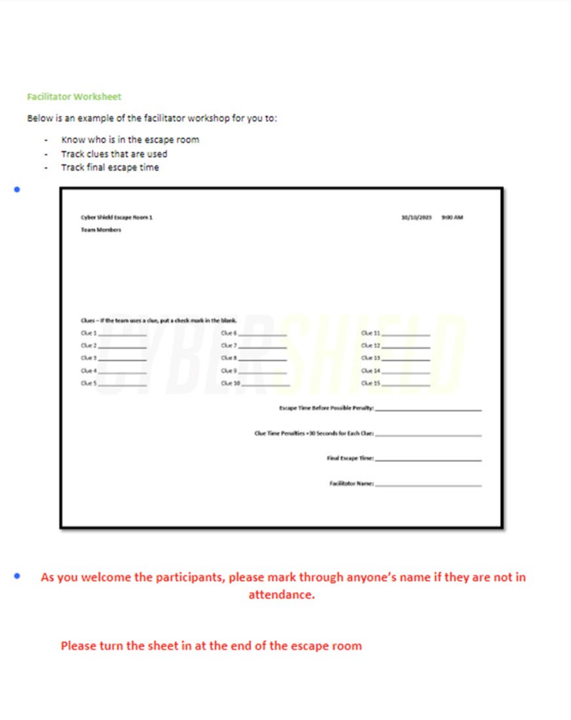
- Puzzle Answer “369” refers to a song
  - Yes, people did sing it during the event
- Puzzle Answer “2468” refers to “Who do we appreciate?”
- Puzzle Clue “Who You Gonna Call?” refers to GhostBusters (and our cybersecurity team)

Escape Room Review

Attendees go through 3 stages

- Pre-room
  - Discuss any accommodations needed
  - Icebreaker (attendance)
  - Video introduction of story
- Walk through to Escape Room
  - Quick breakdown of rules
  - Explanation of digital vs. analog puzzles
  - Set the timer
- Debrief Room
  - Discuss areas of struggle
  - New information the team discovered
  - Pictures/congratulations

Facilitator Guide Examples



Facilitator Worksheet

Below is an example of the facilitator workshop for you to:

- Know who is in the escape room
- Track clues that are used
- Track final escape time

Cyber Shield Escape Room 1 10/10/2023 9:00 AM

Team Members

Clues – If the team uses a clue, put a check mark in the blank.

Clue 1 ____________ Clue 6 ____________ Clue 11 ____________
Clue 2 ____________ Clue 7 ____________ Clue 12 ____________
Clue 3 ____________ Clue 8 ____________ Clue 13 ____________
Clue 4 ____________ Clue 9 ____________ Clue 14 ____________
Clue 5 ____________ Clue 10 ____________ Clue 15 ____________

Escape Time Before Possible Penalty: ____________________

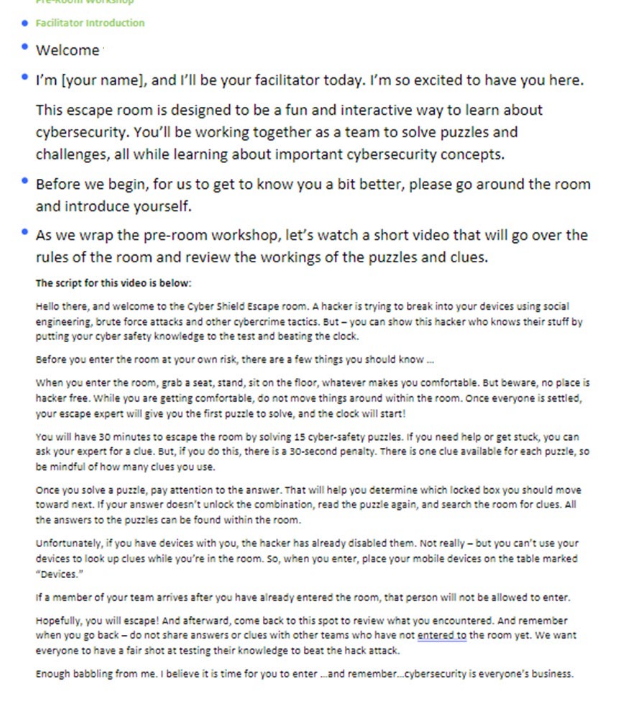
Clue Time Penalties +30 Seconds for Each Clue: ____________________

Final Escape Time: ____________________

Facilitator Name: ____________________

- As you welcome the participants, please mark through anyone's name if they are not in attendance.

Please turn the sheet in at the end of the escape room



Pre-Room Workshop

- Facilitator Introduction
- Welcome
- I'm [your name], and I'll be your facilitator today. I'm so excited to have you here.

  This escape room is designed to be a fun and interactive way to learn about cybersecurity. You'll be working together as a team to solve puzzles and challenges, all while learning about important cybersecurity concepts.
- Before we begin, for us to get to know you a bit better, please go around the room and introduce yourself.
- As we wrap the pre-room workshop, let's watch a short video that will go over the rules of the room and review the workings of the puzzles and clues.

The script for this video is below:

Hello there, and welcome to the Cyber Shield Escape room. A hacker is trying to break into your devices using social engineering, brute force attacks and other cybercrime tactics. But – you can show this hacker who knows their stuff by putting your cyber safety knowledge to the test and beating the clock.

Before you enter the room at your own risk, there are a few things you should know …

When you enter the room, grab a seat, stand, sit on the floor, whatever makes you comfortable. But beware, no place is hacker free. While you are getting comfortable, do not move things around within the room. Once everyone is settled, your escape expert will give you the first puzzle to solve, and the clock will start!

You will have 30 minutes to escape the room by solving 15 cyber-safety puzzles. If you need help or get stuck, you can ask your expert for a clue. But, if you do this, there is a 30-second penalty. There is one clue available for each puzzle, so be mindful of how many clues you use.

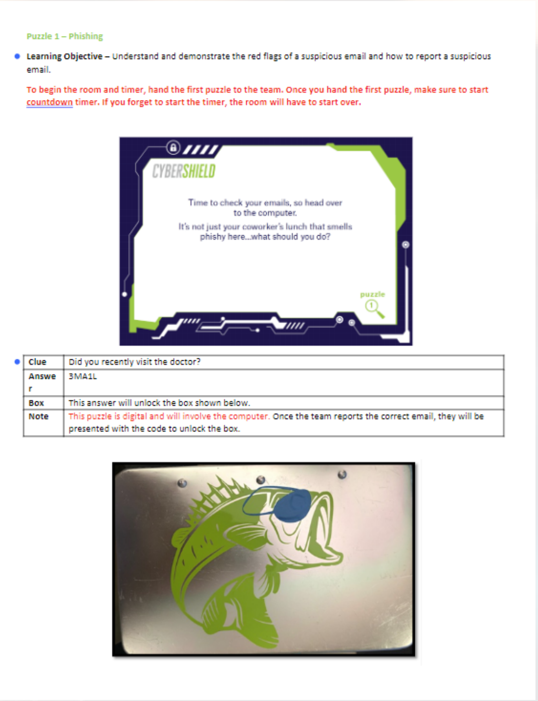
Once you solve a puzzle, pay attention to the answer. That will help you determine which locked box you should move toward next. If your answer doesn't unlock the combination, read the puzzle again, and search the room for clues. All the answers to the puzzles can be found within the room.

Unfortunately, if you have devices with you, the hacker has already disabled them. Not really – but you can't use your devices to look up clues while you're in the room. So, when you enter, place your mobile devices on the table marked "Devices."

If a member of your team arrives after you have already entered the room, that person will not be allowed to enter.

Hopefully, you will escape! And afterward, come back to this spot to review what you encountered. And remember when you go back – do not share answers or clues with other teams who have not entered to the room yet. We want everyone to have a fair shot at testing their knowledge to beat the hack attack.

Enough babbling from me. I believe it is time for you to enter …and remember…cybersecurity is everyone's business.



Puzzle 1 – Phishing

- **Learning Objective –** Understand and demonstrate the red flags of a suspicious email and how to report a suspicious email.

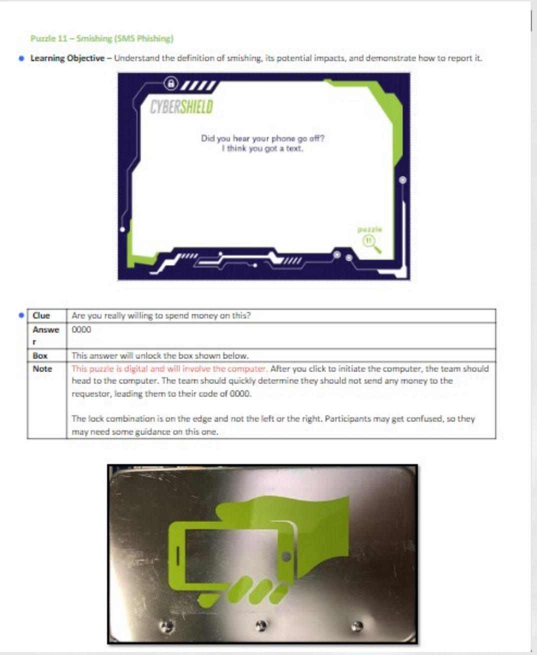
To begin the room and timer, hand the first puzzle to the team. Once you hand the first puzzle, make sure to start countdown timer. If you forget to start the timer, the room will have to start over.

CYBERSHIELD

Time to check your emails, so head over to the computer.

It's not just your coworker's lunch that smells phishy here…what should you do?

Clue	Did you recently visit the doctor?
Answer	3MA1L
Box	This answer will unlock the box shown below.
Note	This puzzle is digital and will involve the computer. Once the team reports the correct email, they will be presented with the code to unlock the box.



Puzzle 11 – Smishing (SMS Phishing)

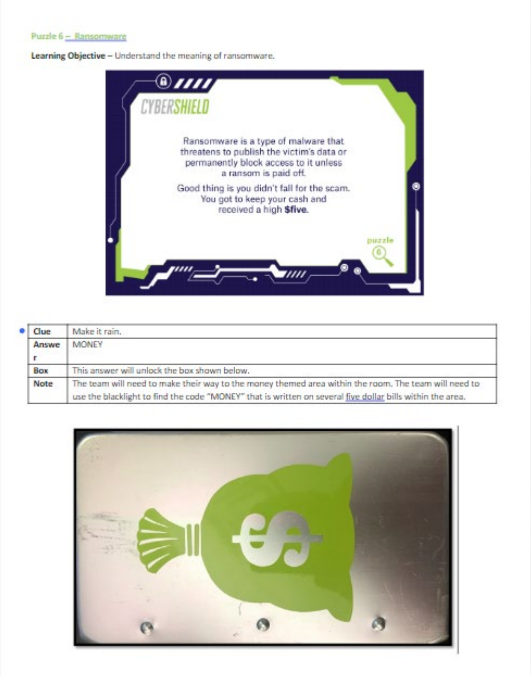
- **Learning Objective –** Understand the definition of smishing, its potential impacts, and demonstrate how to report it.

CYBERSHIELD

Did you hear your phone go off?
I think you got a text.

puzzle
11

Clue	Are you really willing to spend money on this?
Answer	0000
Box	This answer will unlock the box shown below.
Note	This puzzle is digital and will involve the computer. After you click to initiate the computer, the team should head to the computer. The team should quickly determine they should not send any money to the requestor, leading them to their code of 0000. The lock combination is on the edge and not the left or the right. Participants may get confused, so they may need some guidance on this one.



Puzzle 6 – Ransomware

Learning Objective – Understand the meaning of ransomware.

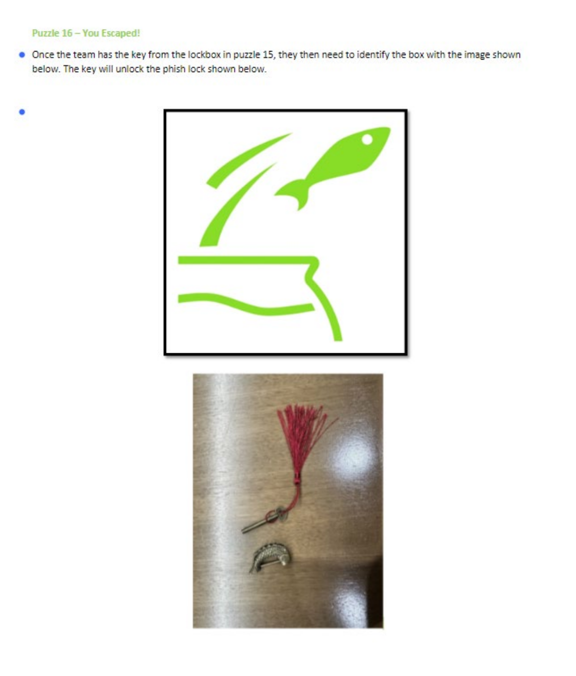
CYBERSHIELD

Ransomware is a type of malware that threatens to publish the victim's data or permanently block access to it unless a ransom is paid off.

Good thing is you didn't fall for the scam. You got to keep your cash and received a high **$five.**

puzzle
6

Clue	Make it rain.
Answer	MONEY
Box	This answer will unlock the box shown below.
Note	The team will need to make their way to the money themed area within the room. The team will need to use the blacklight to find the code "MONEY" that is written on several five dollar bills within the area.

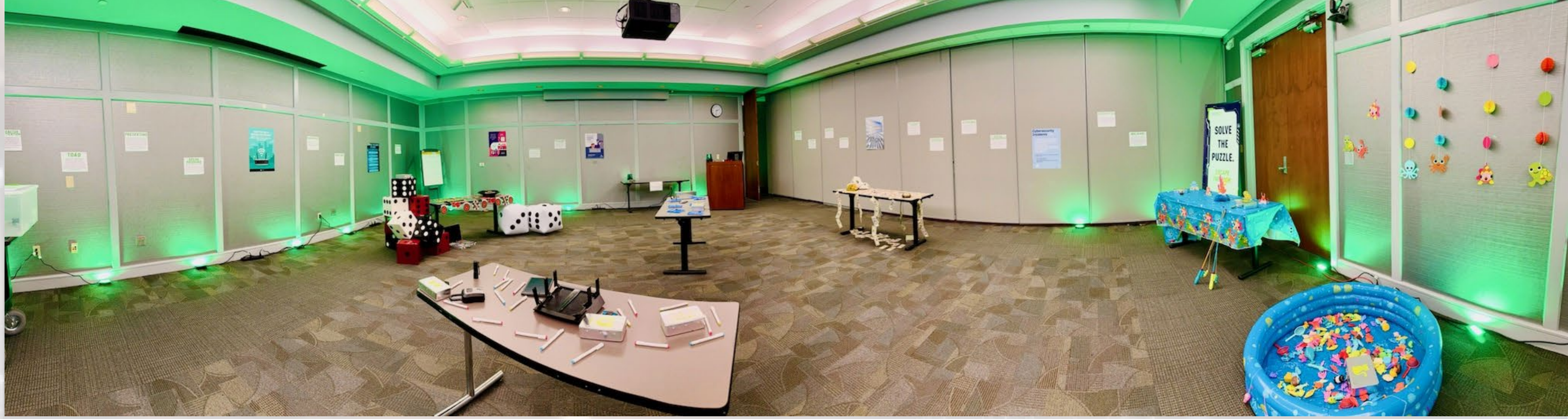


Puzzle 16 – You Escaped!

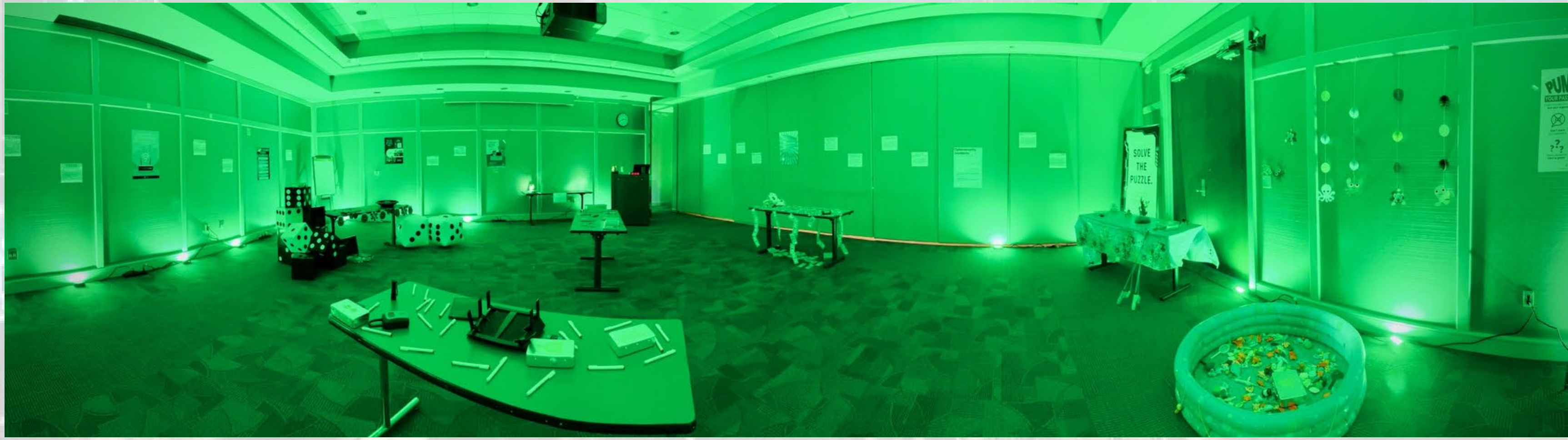
- Once the team has the key from the lockbox in puzzle 15, they then need to identify the box with the image shown below. The key will unlock the phish lock shown below.

Escape Room Signage

Escape Room Pictures

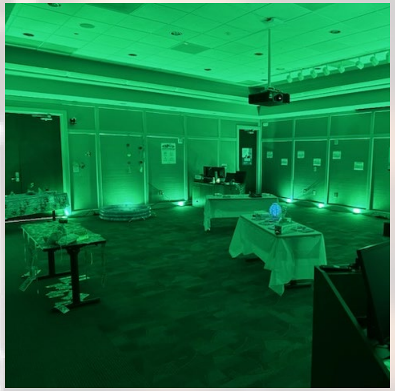


Initial set-up of escape room with lights on

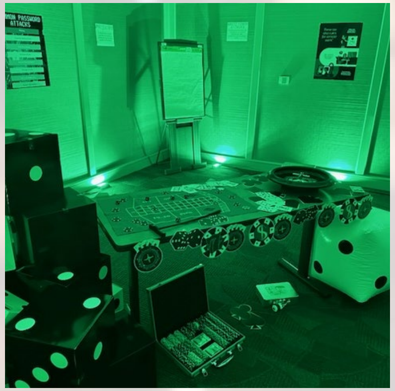


Initial set-up of escape room with lights off

Escape Room Pictures



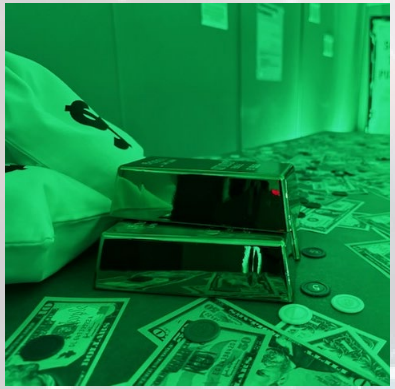
Wide-shot of room



Mobile Security puzzle

IoT puzzle

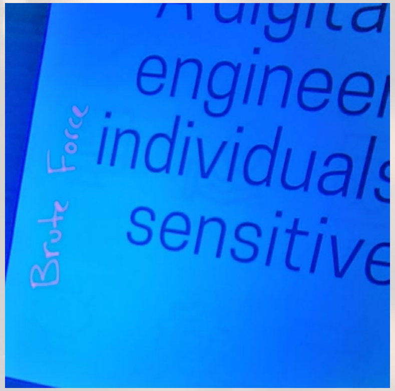
Vishing puzzle



Ransomware puzzle

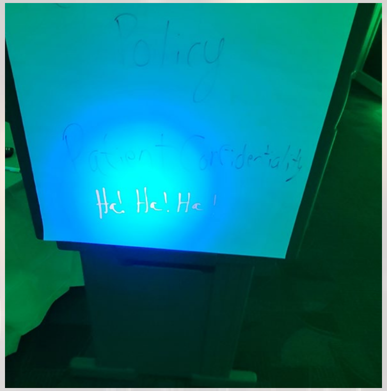
Lockboxes

Escape Room Pictures

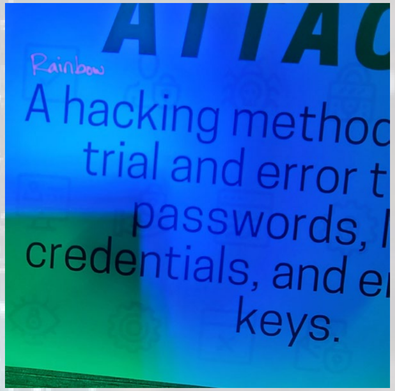


Puzzle Clue using UV Light

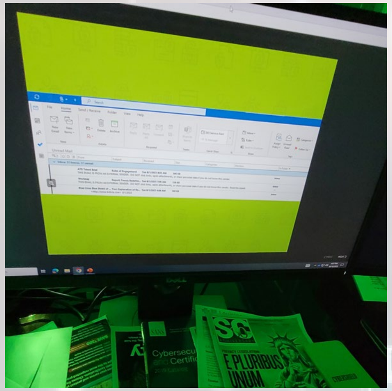
Red Herring puzzle using UV Light



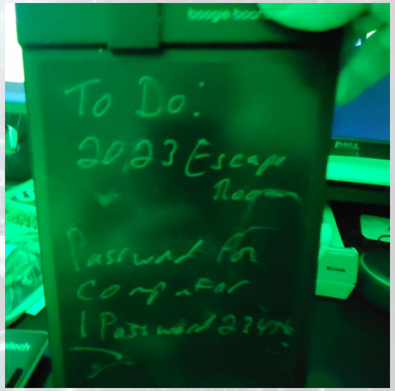
Red Herring using UV Light



Puzzle Clue using UV Light



Digital Phishing puzzle



To Do:
2023 Escape Room
Password for computer
1Password23456

Red Herring for password puzzle

Debrief

Puzzle 1—Phishing
Untargeted, mass emails sent to many people asking for sensitive information, such as bank details, or encouraging them to visit a fake website. Use the Phish Alert Button in Outlook to report suspicious emails.

Puzzle 2—Social Engineering
Manipulating people into carrying out specific actions or divulging information that is of use to an attacker.

Puzzle 3—Security Incident
A security incident is defined as any event that results in the loss of the confidentiality, integrity or availability or e-PHI and/or other sensitive information. ***How to contact the company***

Puzzle 4—Malware
Malicious software including viruses, trojans, worms or any code or content that could have an adverse impact on organizations or individuals.

Puzzle 5—Encryption
A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

Puzzle 6—Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Puzzle 7—MFA
The use of multiple components to verify a user's claimed identity.

Puzzle 8—Password Attack Vector
One of the most common password attack vectors is via phishing attacks.

Puzzle 9—Passwords
Company's policy on Passwords

Puzzle 10—Device Secutity
Never leave your device unattended in a public setting. Devices should always be locked when not in use. Be aware of your surroundings to mitigate shoulder surfing.

Puzzle 11—Smishing
Avoid SMS phishing to safeguard your privacy and prevent potential identify theft or financial loss.

Puzzle 12—Remote Workspace
Smart speaker devices are not allowed in a remote workspace as they may capture and record conversations and activities.

Puzzle 13—Internet of Things
Refers to the ability of everyday objects, other than computers and devices, to connect to the internet. Examples include fridges and televisions.

Puzzle 14—Confidential Documents
Confidential information should never be shared via personal email, text, or uploaded to storage sites.

Puzzle 15—Vishing
Vishers use fraudulent phone numbers, voice-altering software, text messages and social engineering to trick you into taking action.

During debrief the escape room facilitator:

- Debriefed puzzles the team had trouble answering
- Went over anything the team wasn't sure of (new words, concepts, etc.)
- Discussed things the team learned during the session

Project Evaluation

Microsoft Forms Evaluation sent after event:

1. Overall, rate this session on a scale of 1 (low) to 5 (high):
2. What is one thing you learned at this event?
3. Would you attend another Escape Room?
4. Do you prefer hands-on or computer-based training?
5. How can we improve our Escape Room?
6. Do you have any additional comments, questions or feedback you would like to provide?