WHO ARE WE?

WE ARE FEDEX
WHAT IS FEDEX?
WHAT ARE ESCAPE ROOMS?
An escape room is a physical adventure game in which players solve a series of puzzles using clues, hints and strategy to complete the objectives at hand. Players are given a set time limit to unveil the secret plot which is hidden within the rooms. Escape rooms are inspired by "escape-the-room"–style video games. Games are set in a variety of fictional locations, such as prison cells, dungeons and space stations, and are popular as team building exercises.

- FROM WIKIPEDIA

And they’re getting more and more popular!
I can’t believe I ate the whole thing...

Okay, cool. Sounds like a jolly good time.

What does any of this have to do with Information Security Awareness?
AND NOW...

ESCAPE FROM SANS.
YOU ESCAPED!!!

NOW FOR MORE SLIDES
WHAT JUST HAPPENED?
TELL ME, AND I’LL FORGET.
SHOW ME, AND I’LL REMEMBER.
INVOLVE ME, AND I’LL UNDERSTAND.

Benjamin Franklin? Native American Proverb? Confucius?
不闻不若闻之，闻之不若见之，见之不若知之，知之不若行之

The quote comes from the Xunzi.

Xun Kuang was a Chinese Confucian philosopher that lived from 312-230 BC. His works were collected into a set of 32 books called the Xunzi, by Liu Xiang in about 818 AD. There are woodblock copies of these books that are almost 1100 years old.

Source: quora.com
“Not having heard something is not as good as having heard it; having heard it is not as good as having seen it; having seen it is not as good as knowing it; knowing it is not as good as putting it into practice.”

From Book 8, Chapter 11, John Knoblock translation
Escape rooms are intended to foster team-building, critical thinking and problem solving skills for groups of all kinds.

We build on that by designing puzzles and themes that reflect and reinforce beginner to intermediate Information Security principles.

And we hope that through some teachable moments, Information Security fundamentals and best practices become understood and formative in future decisions.
BUT WHAT ABOUT ADVANCED INFOSEC PRINCIPLES
Other options...

• Red Team / Blue Team exercises
• Hackathons
• Tabletop drills
HOW WE DO WHAT WE DO
Budget

Audience

Environment

THEME

Puzzles

Flow

Teachable Moments
BUDGET
- How much money to buy props, puzzles and other bells and whistles?

AUDIENCE
- Who is attending?
- What is their general IT exposure?
- How many are attending?
- Anything relevant to the group that can be used for a theme?

We strongly recommend dividing up into groups of no more than 10, for management and user experience.
ENVIRONMENT

- What kind of space is available?
- Does the room have anything unique that can be leveraged?
- How much prep time is available?
- Will the room be dedicated or shared from prep to finish?

Once these questions are answered, you can start planning in earnest.
THEME

This is where the fun in planning begins. Be creative, but be mindful of your audience. The more relevant, the more engrossing, the better the escape room. And of course, something to drive the clock (usually some threat of impending doom). Use a timer!!

Examples:

Cyberattack, crime scene investigation, heist, jailbreak
PUZZLES

As with themes, be creative, do some research, and try to make puzzles/challenges that are FUN but also build skills and reinforce best practices. This is the core of the escape room, so make them memorable!

Don’t be afraid to have your participants take on the role of an ‘attacker’ too. Some of the best lessons are learned by forcing oneself to view a situation through the eyes of an adversary.
PUZZLES

- Locks of all kinds
- Logins
- Scrambled / encrypted data
- Hidden objects
- Physical manipulation of objects
- Pre-staged computer issues
- Shredded documents
- External media devices
- Communication breakdowns
- More examples in the handout!!
FLOW

In other words, how the puzzles will chain together. This is largely dependent on the environment and puzzles chosen, but theme should also be considered. Rules or boundaries of the exercise should also be determined by this point.

Some tips...

• Keep a cheat sheet of all puzzles and solutions handy
• Fully test your puzzles in sequence multiple times
• Consider inserting red herrings in between puzzles to increase difficulty
• Allow for opportunities to provide groups with helps or hints
TEACHABLE MOMENTS

This are the moments where the puzzles, theme and/or flow are tied back to real-life Information Security best practices and principles.

These should occur both during the exercise AND be reinforced afterwards. Try to challenge your participants to identify the InfoSec themes on their own, and then provide your own explanations to compliment those self-learned lessons.

In many ways, a well designed escape room can represent an attack kill-chain and poor defense-in-depth. Each puzzle represents a vulnerability that the participant is exploiting, and if best practices were followed, the puzzle could not have been solved.
RECOMMENDATIONS & TIPS:

• Use puzzles / challenges that are appropriate for your audience
• Keep a timer visible
• Make sure to communicate your rules and caveats at the start
• Consider a “mini-victory” at the half-way point
• Have a live helper (or two) present to help with timing and flow to ensure the participants do not become bogged down / frustrated
• The more creative the puzzle, the better!
• Visit your local escape room(s) for some hands-on inspiration
## EXAMPLES

<table>
<thead>
<tr>
<th>Puzzle</th>
<th>Solution</th>
<th>Principle</th>
<th>Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password on shredded papers</td>
<td>Tape and patience</td>
<td>Secure disposition of sensitive data</td>
<td>Easy</td>
</tr>
<tr>
<td>Practice lock</td>
<td>Lock pick</td>
<td>Physical security</td>
<td>Medium</td>
</tr>
<tr>
<td>Phone “assistance”</td>
<td>Just say NO!</td>
<td>Phishing and critical thinking</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>USB drives</td>
<td>Just say NO!</td>
<td>Untrusted data</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>Email “assistance”</td>
<td>Just say NO!</td>
<td>Phishing and critical thinking</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>Brain teasers</td>
<td>Critical thinking</td>
<td>“Security” by obscurity / fun</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>Password hidden in jpeg</td>
<td>Text editor</td>
<td>Digital steganography</td>
<td>Hard</td>
</tr>
<tr>
<td>Combination in invisible ink</td>
<td>UV light</td>
<td>Physical steganography / fun</td>
<td>Easy</td>
</tr>
</tbody>
</table>
## EXAMPLES

<table>
<thead>
<tr>
<th>Puzzle</th>
<th>Solution</th>
<th>Principle</th>
<th>Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless networks</td>
<td>Secured only</td>
<td>Untrusted networks / data security</td>
<td>Medium</td>
</tr>
<tr>
<td>“Compromised” machine</td>
<td>Log files</td>
<td>Digital forensics</td>
<td>Hard</td>
</tr>
<tr>
<td>Combination lock with portion of combination provided</td>
<td>Brute force</td>
<td>Password complexity</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>Missing password, combination, or tool hidden in room</td>
<td>Physical searching</td>
<td>“Security” by obscurity / fun</td>
<td>Easy-Medium</td>
</tr>
<tr>
<td>Base-64 encoded passwords</td>
<td>Decoding tools</td>
<td>Weak encryption</td>
<td>Medium</td>
</tr>
</tbody>
</table>

VR and 3d printing offer untapped potential as well!
Questions?
Comments?
Bad jokes?

See you at the Show-n-Tell Table!