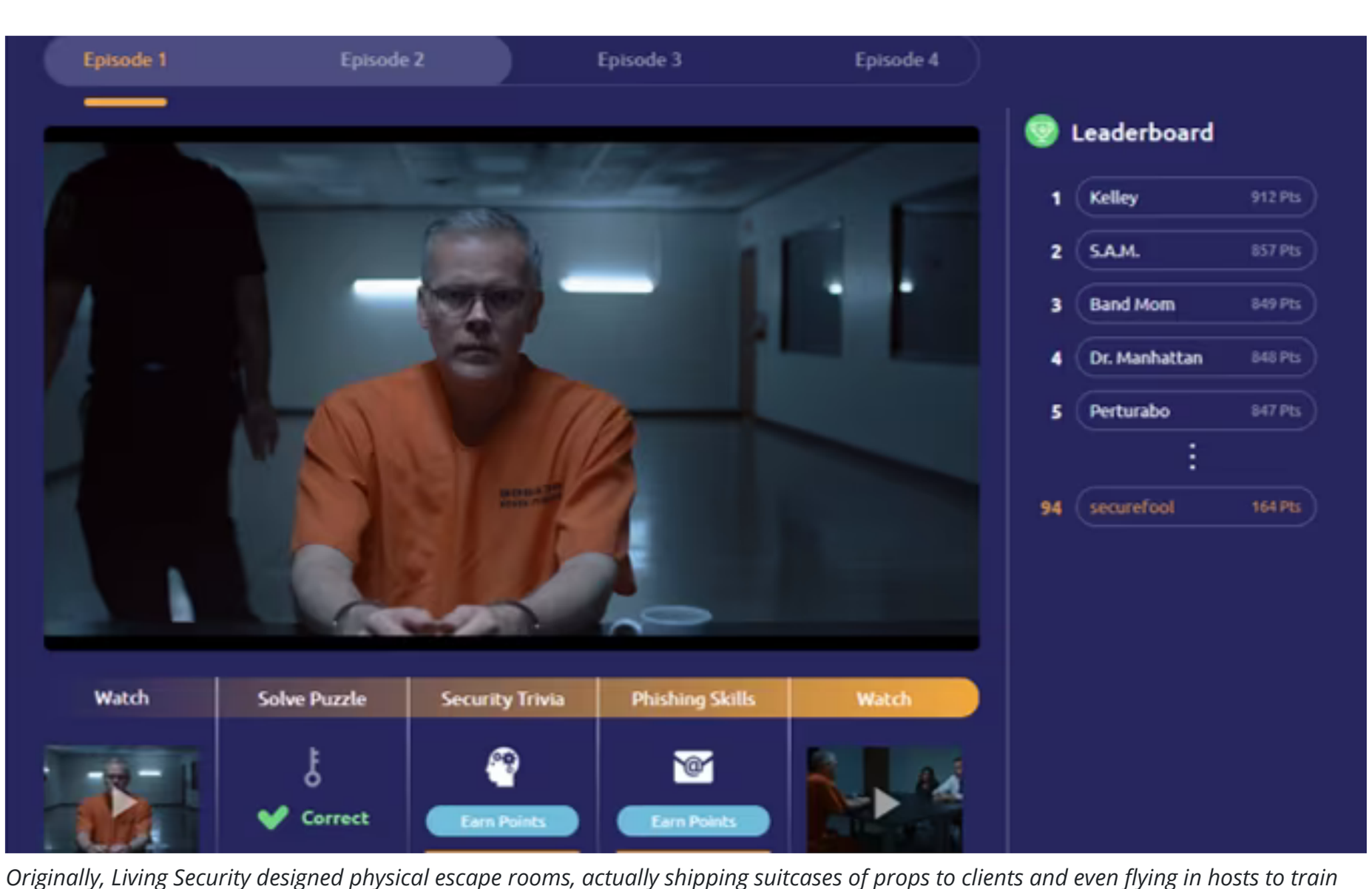
Malware, Network Security, Phishing

Cyber escape room locks in employees' security awareness. But can SC Media beat the clock?

Bradley Barth December 3, 2020



Originally, Living Security designed physical escape rooms, actually shipping suitcases of props to clients and even flying in hosts to train companies' security program leaders how to run exercises across their organizations. But like so many other organizations, Living Security was forced to pivot after COVID-19 forced lockdowns last March. Living Security)

You might say I'm a bit of an escape room fanatic.

Since 2015, I've successfully escaped from a sinking submarine, a bank vault (after robbing it, of course), Dr. Jekyll's laboratory and a magician's lair.

Regrettably, my record is far from perfect. I've also been cursed by a witch, bombed by enemy war planes, smashed up in a subway car collision and murdered by psycho killers three separate times.

But if there were ever an escape game that was built for me, it was "CriticalMass" – a cybersecurity-themed virtual escape room designed to train corporate employees how to be more secure by avoiding phishing emails, managing data responsibly and securing their networks.

The plot: identify and capture an insider threat within your organization before he or she is able to divert payroll funds.

CriticalMass is the first of several entries in the "CyberEscape Online" series created by Living Security, an Austin, Texas-based security training company founded in 2017 by CEO Ashley Rose and her husband, Security Awareness Creator Drew Rose.

The Roses both previously worked at a real estate investment trust company American Campus Communities (ACC), where Drew as information security manager was tasked with creating an internal security awareness program. It was around this time that he and Ashley signed up for a local escape room for a fun night out. This ultimately served as his inspiration.

"[Drew] came back and he was like, 'There are so many cybersecurity principles mixed into this escape room. You're trying to like pick locks and problem solve and there's encryption," said Ashley Rose, in an interview with SC Media.

Mr. Rose immediately set out to create an entirely paper-based escape room as a security training exercise for ACC employees. Mrs. Rose, who was serving in a marketing role at ACC, collaborated on the effort.

"I helped him create all these different escape room kits," said Mrs. Rose. "We had to make 100 of these things, because every time you ran through it, you'd have to throw everything away."

Living Security CEO Ashley Rose

The feedback from co-workers was effusive. "And that's really when that light bulb went off, and it clicked: Wow, if we can make people actually want to take cybersecurity training, then we're doing something better. We're doing something that can truly change behavior," Mrs. Rose continued.

And so the concept of Living Security was born. The Roses formed the company with a mission to create a security training program that embraces concepts such a gamification and experiential learning as a means to reduce human risk through behavioral change.

With normal training programs, "Typically you're checking a box; there's PowerPoint, there's questions and answers and [you're] done," said Mrs. Rose. But by introducing elements of fun and competition to employees, "you're actually getting them to completely change their mindset and shift the way that they think about security. [So] they think about the security team as more of a friend and an ally, and something that's positive versus the 'no team' or people that want to stop them from doing their job."

In fact, Living Security told SC Media that 90 percent of its surveyed escape room participants have said that they now feel more comfortable contacting their security team after going through the training exercise.

Mastercard is among the companies leveraging Living Security's immersive escape room content to train its global employees.

"We brought a competitive team to the session, so it was easy to stay engaged. We didn't want to miss a clue," said Amanda Gioia, vice president of technology risk management at Mastercard. "The story was compelling, and our team was racing against the clock to have the best score compared to the other teams on the leaderboard. Each of us learned something from each security-related challenge, and more about each other and how we approach challenges as well."

Originally, Living Security designed physical escape rooms, actually shipping suitcases of props to clients and even flying in hosts to train companies' security program leaders how to run exercises across their organizations. But like so many other organizations, Living Security was forced to pivot after COVID-19 forced lockdowns last March.

"Fifty percent-plus of our clients couldn't use our solution, and now all of their users were at home and open to even greater and different risks than they were in office," said Mrs. Rose. "And so we needed to figure out a way to get them trained and engaged in security while they're at home."

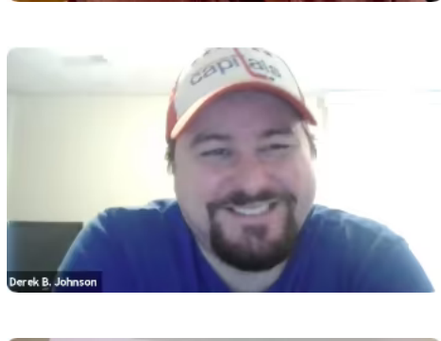
Within six weeks' time, the Living Security engineering and software teams devised a Zoom-based virtual version of their escape room program and brought it to market. Even some of the lesson content changed to reflect the current work-from-home realities. "I think ultimately we would have all gotten here [anyway] because companies are global and you were seeing this shift to remote workforces even pre-COVID," Mrs. Rose noted.

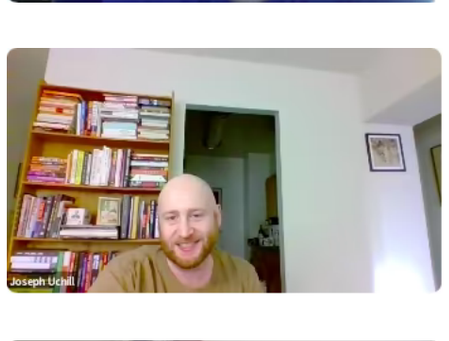
Meet the SC Security Ninjas

But what about SC Media's track of crack staff of reporters? Could we handle the challenge?

Considering the escape room doubles as a team-building exercise, it only made sense to invite several of my SC Media colleagues to play alongside me. Perhaps I was being generous… or perhaps I was just looking for a scapegoat to blame in case we lost.

The first step was to come up with a team name. So without further ado, I present to you the SC Security Ninjas: reporters Bradley Barth, Derek Johnson, Joe Uchill and Steve Zurier.





We were then shown a video setting up the situation: A detective warns us that an employee at our imaginary company is diverting payroll funds.

"Here's the crazy part: There are dozens of people across the organizations that can enter a payroll disbursement," the detective says. (Lesson number one: lack of privileged access is bad.) We have 40 minutes to shut down the rogue laptop. "You're going to have to work together as a team or this whole thing could go really bad," he says.

"All right, how are we feeling?" our live game host Dany Mares asked us immediately following the video intro.

"Very stressed out," said Johnson.

"My blood pressure is going up," said Zurier.

And with that, the clock started ticking.

To win, the Security Ninjas had to unlock a series of puzzles by answering various security-related questions correctly, such as how to define an insider threat. Answering a question correctly would open up a new puzzle or game. While the game doesn't operate precisely how an in-person escape room would work, it has many of the same elements – a high-stakes fictional mission, a time limit, a leaderboard to compare winning times, and clues and puzzles that must be solved in order to advance.

Living Security's escape rooms have multiple storylines to choose from, and the exercises are customizable according to what security concepts a company wants to emphasize, such as phishing or insider threats.

"Our clients really like to personalize the experience to fit their culture," said Mrs. Rose. "We have different storylines that map to these macro-level concepts at the highest level and then we have sub-concepts… that are baked into the puzzles." Companies can also can customize questions to incorporate their own actual internal policies.

One of the puzzles was a phishing exercise in which trainees must identify the reason why certain emails were classified as a phishing threat, by clicking on the telltale clues that made them suspicious, such as typos or an incorrect sender address. (In a related story, I was recently challenged to take a quiz in which I had to tell the difference between phishing emails and genuine emails. See how I did here.)

An interesting phenomenon, said Mrs. Rose, is that often employees who aren't confident about spotting phishing emails will pick up security tips from their own coworkers who know the answer. "They're really intrigued and are interested in what the rest of the team is doing. So now you're not just learning from training but you're learning from each other. So you're putting people in the role of a teacher," said Mrs. Rose. "It's more active learning than just passively watching something and it really gets everybody involved," she said.

In another round, the SC Security Ninjas used a company manual found in our digital evidence locker to look up our company's data classification rules to ascertain what company data was allowed to shared with the public (e.g. quarterly financials) and what was not (employees' personal data).

"I've seen a lot of employees struggling with data classification," said Mrs. Rose. "That's a huge challenge for a lot of organizations because these policy documents and policy statements are written so technically. It's not really written for people. And so most of the time you find people struggling or they didn't read it; they just kind of signed off on it."

In perhaps the most relevant exercise for 2020, the SC team was asked to view an illustration of a remote worker's home to click on any security risks or violations that could potentially threaten data. Living Security added this game specifically in light of the COVID-19 pandemic to deliver key lessons to remote worker, including the dangers of open Wi-Fi connections or Internet of Things devices within the home.

"One of the scenarios highlighted the importance of protecting your home router with a password," said Giola. "As someone who is working remotely right now this was a reminder to stay vigilant about security, regardless of where I'm working."

In the last stage, the Security Ninjas had to piece our clues together and identify the culprit. The final result: success! We caught the insider threat – in 29 minutes, 30 seconds, no less. Our imaginary company was saved, and our actual company didn't have to fire us for making it look bad.

Craving some hard-earned praise, I asked Mrs. Rose how we did.

"Twenty-nine minutes, that is definitely a good successful completion metric," she said, attributing our success to both solid teamwork and of course our knowledge of cybersecurity.

"Because there's a teamwork engagement element here we find that if [players] work well together as a team in other areas, then they can typically solve the challenges really well," she said. "For you to be able to pick up the concepts and materials and to be able to escape in 29 minutes is something that you should be bragging about," said Mrs. Rose.

Still, we were not record-breakers. We were informed that some cybersecurity professionals have completed the game in as little as roughly 25 minutes. But we were considerably faster than the average end user time of approximately 36 minutes (though times can vary based on game content).

But while trainees might be competitive about their final times, the more important result is that employees have learned valuable data and network security lessons, and are open to future instruction.

Indeed, 100 percent of polled Mastercard employees said they would agree to participate in a future Living Security escape room, and 95 said the exercise increased their awareness of security concepts. "All the exercises were helpful because they touched on different aspects of security, and served as good reminders for staying safe both at work and home," said Giola.

And to think that this all started with Ashley and Drew Rose spending a couple's night out in an Austin escape room. But here's the question I was wondering: Did they actually escape it?

"I'll tell you this: I was really bad," said Rose. "But then once I started building them, I was like, 'Oh, I have got your number… I know where this is gonna be hidden.'"

Bradley Barth
As director of community content at CyberRisk Alliance, Bradley Barth develops content for SC Media online conferences and events, as well as video/multimedia projects. For nearly six years, he wrote and reported for SC Media as deputy editor and, before that, senior reporter. He was previously a program executive with the tech-focused PR firm Voxus. Past journalistic experience includes stints as business editor at Executive Technology, a staff writer at New York Sportscene and a freelance journalist covering travel and entertainment. In his spare time, Bradley also writes screenplays.

RELATED

THREAT INTELLIGENCE
New Menorah malware bolsters OilRig APT's cyberespionage efforts
SC Staff October 2, 2023
Iranian advanced persistent threat operation OilRig, also known as APT34, Helix Kitten, Hazel Sandstorm, and Cobalt Gypsy, had its cyberespionage arsenal strengthened with the novel Menorah malware deployed in a spear-phishing campaign, which included a Saudi Arabia-based organization as one of its targets, reports The Hacker News.

MALWARE
New ASMCrypt malware loader detailed
SC Staff October 2, 2023
New ASMCrypt malware loader detailed Novel malware crypter and loader ASMCrypt has been developed by cybercriminals building upon the stealthy DoubleFinger malware loader, which was previously leveraged to facilitate GreetingGhoul cryptocurrency stealer deployment, according to The Hacker News.

MALWARE
LinkedIn Messaging used by APT to phish aerospace target and plant novel malware
Simon Hendery October 2, 2023
Hackers tricked an employee into downloading the previously unseen malware by claiming he was in the running for a job at Meta.

RELATED EVENTS
CYBERCAST
EMOTET Exposed: Inside the Cybercriminals' Supply Chain
ON-DEMAND EVENT