M+E JOURNAL

It's Showtime!

Innovation explodes across every workflow as technology emerges from the pandemic.

Where are you in this accelerated evolution?

DIVERSITY & INCLUSION
In the office, behind the camera, and on the screen, diversity is crucial

SECURITY
Remote productions create new security concerns, with assets under siege

SMART CONTENT
Artificial intelligence and machine learning are being applied in new, exciting ways

NEW WORKFLOWS
The cloud is delivering on its promise, powering the future of productions

21.01

HOW FUN AND GAMES CAN REDUCE YOUR CYBER RISK

Cybersecurity training doesn't have to be a snore

ABSTRACT: Traditional methods of cybersecurity training don't work well, mostly because they're boring. Your team will retain more cyber awareness over the long term if they have fun in the process.

By Meera Mehta, CEO, Xcapism Learning

Picture the scene: 5 p.m. on deadline day, and you still haven't finished your mandatory cybersecurity training.

You know you have to do it, open what you've been assigned, skim through information on how to spot a phishing attempt, how to protect your data, all the rest … and you keep hitting "next" over and over, as fast as possible. Then you guess most of the answers for the test.

You've finished for another year, and pretty much forget about it. And that's the key: how much have you really retained?

According to a study by the National Training Laboratories

> *DEPENDING ON YOUR ORGANIZATION'S CULTURE, the tone needs to be widened to make cybersecurity training as simple and relatable as possible.*

Institute for Applied Behavioral Science, most of the traditional methods of training and awareness — from posters, watching videos, reading articles and annual training — results in as little as 30 percent retention of the information you're being given.

Not a great return on your investment, right? And certainly not helpful in reducing the risk of someone in your company clicking on a bad link or falling for fraud. Even at a live cybersecurity demonstration or event, many people will be interested, but I've seen a few people playing games on their phones.

There's nothing wrong with the content traditional methods of cybersecurity training offer. It's the delivery that's lacking. If you're not fully engaged, you don't remember as much. Which means you're unlikely to change your behavior.

The National Training Labs study goes on to say that by being immersed in a subject will see you retain up to 75 percent of the information offered. Even better, if the experience is truly engaging and immersive, you'll retain 90 percent, and be more likely to pass on your new-found knowledge onto others.

LEARNING THROUGH DISCOVERY

But how do you achieve this successfully? Think about applying a combination of gamification with "practicing doing" to your cybersecurity training, meshing the mental reward of solving gaming-like problems with a real-world challenge using everyday objects as an analogy for cyber threats.

By discovering, you're already engaged, and retaining knowledge without even knowing it. And it's important these challenges aren't a series of separate puzzles, but linked together as a story, where one puzzle leads to the next, with a goal at the end.

Think of your favorite TV drama: You're glued to the story from start to finish. This is what Xcapism Learning aims for with its cybersecurity training programs.

Cybersecurity awareness campaigns have generally become associated with the faceless hacker, hunched over a computer, in hiding from the law. But in reality, a hacker could be someone on the bus, someone who sits next to you at work, someone not living in their parents' basement.

Do whatever possible to help your organization rethink who cyber-attackers are. Depending on your organization's culture, the tone may need to be widened, to make it as simple and relatable as possible to appeal to your diverse workforce. Why not replace the guy in the hoodie with a cartoon crook?

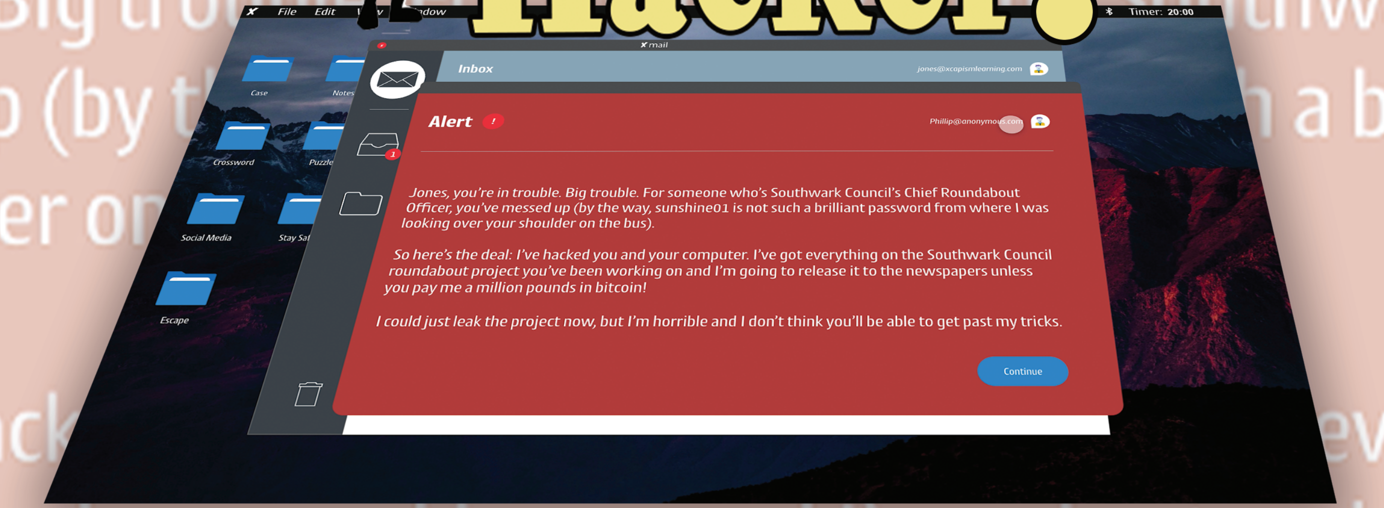
Additionally, what we've found at Xcapism Learning is that cybersecurity training is enhanced when internal teams at companies compete. Playing in teams, adding a league to find the fastest time out of a cyber escape room, prizes for the best team name, all combine to heighten the enjoyment, and consequently, engagement.

Gamification principles will lead your colleagues to remembering more, because you're more likely to remember a time when you had fun. And if you've had fun, you're building a more cyber-risk averse culture across your company. ⊞

Meera Mehta is CEO of Xcapism Learning. With a background in financial services and media, and more than 15 years' experience in the areas change improvement, risk, cybersecurity and privacy, her work has inspired Xcapism Learning's ethos of influencing real behavioral change. *meera@xcapismlearning.com*

Has your team got what it takes to

Beat the Hacker?



Jones, you're in trouble. Big trouble. For someone who's Southwark Council's Chief Roundabout Officer, you've messed up (by the way, sunshine01 is not such a brilliant password from where I was looking over your shoulder on the bus).

So here's the deal: I've hacked you and your computer. I've got everything on the Southwark Council roundabout project you've been working on and I'm going to release it to the newspapers unless you pay me a million pounds in bitcoin!

I could just leak the project now, but I'm horrible and I don't think you'll be able to get past my tricks.

Save your stolen project by solving cyber security tasks on:

Password security

Encryption

Preventing data loss

Data privacy

...and more

Book a demo now:

info@xcapismlearning.com

XCAPISM LEARNING.COM

COMING SOON...