IMMERSIVE
TRAINING AHEAD

7 CYBERSECURITY AWARENESS TRENDS FOR 2020

livingsecurity

2019 TRENDING THREATS

01

2019 was marked by a number of emerging threats, including vendor email compromise, synthetic identity theft and war-shipping. All are important to recognize as part of a new wave of attacks that are variations of traditional ones.

VEC is the New BEC

Vendor email compromise (VEC) emerged as a variant of business email compromise (BEC) in which attackers hijack a legitimate vendor business account, lay low, gather information and then send a fraudulent invoice to a client.

What makes it so hard to spot is that it is virtually the same as the real invoice, except for different payment information.

Agari, a security firm, tracked one threat actor's infiltration of over **700 vendor employee email accounts**, spanning more than **500 companies** in the US and a dozen other countries. They claim that VEC is the most dangerous cyber threat faced by businesses and their supply chains in the next 12 months.

Synthetic Identity Theft

The identity theft of yesterday captured all necessary details about a person in order to impersonate them and compromise their accounts. The identity theft of today and tomorrow captures some of the necessary details about a person and fabricates the rest. This is known as synthetic identity theft and lowers the barrier of entry for cyber criminals to successfully steal an identity.

War-shipping

According to the New Jersey Cybersecurity & Communications Integrations Cell (NJCCIC) war-shipping is "unlike wardialing and wardriving techniques [in that it] utilizes disposable, low-cost, and low-power devices to remotely infiltrate corporate or personal home networks and further exploit existing vulnerabilities, steal sensitive information, and exfiltrate data or credentials."

Imagine receiving a package at your work address, setting it aside because you're not exactly sure who it belongs to and going about your business. In the meantime, the box proceeds to identify and exploit your local wireless networks remotely because it is loaded with listening devices and WiFi-enabled gear.

The Takeaway:

New variants of old threats are equally as destructive. If you have implemented defenses against BEC, identity theft and war-dialing, you may want to consider VEC, synthetic identity theft and war-shipping as part of your 2020 security strategic plan.

INTEL-DRIVEN CONTENT

Reducing human risk is likely a founding principle of your security awareness program. But if you neglect to update training content on a regular basis, all the training in the world won't reduce risk. This sounds obvious, but the point is that end-users have to actually be aware of current and emerging threats to combat them. This is where security awareness program owners are increasingly turning to threat intelligence analysts.

01 Threat Intelligence Defined

Threat intelligence is - simply put - knowledge of the adversary. Threat intelligence analysts ask questions like: What are the biggest cyber threats to our organization and our industry? What are cyber criminals doing, today, that could impact our bottom line? How can we get the best ROI with our current toolset to combat these threats? Which employees are our highest-value targets (HVTs)? What new techniques are we seeing against people our industry? How can we equip them with knowledge and awareness to report fast and defend the network?

Threat intelligence analysts know it makes a difference whether you believe 'malware targets organizations' or 'people target people.' A 'malware' view of the world is in bits and bytes, ones and zeroes. Even if that malware is driven by computer machine-learning, it cannot adapt and think like a human being.

02 Why Human Threats Need a Human Firewall

So when 'people target people,' something else happens. Phishing emails look and feel like they come from your coworker down the hall. Vishing calls sound like they're really from Microsoft tech support. And ransomware provides better customer service than your bank.

Threat intelligence analysts see this everyday. So when the output of their work is knowledge and situational awareness, it only makes sense that security awareness teams will want to use it for training. Then, when end-users become aware of the latest threats (and understand how to combat them), your security awareness program will see progress in reducing risk, eliminating blind-spots, creating a human firewall and influencing culture change.

★★★ ★★ **In other words, intelligence-driven content is a growing trend which helps security teams train end-users for the next threat, not the last one.**

Train users for the next threat, not the last one!

The Takeaway:

Use threat intelligence to create powerful, relevant training content for people to combat the unique threats to your industry, business and mission.

EXPERIENTIAL LEARNING IN TRAINING

The effectiveness of experiential learning as a cybersecurity training method is clear: People exhibit 16-times greater retention through experiential learning than through traditional, didactic lessons.

In 2020, fun, engaging, hands-on, immersive learning is poised to become an even more vital tool to reduce human error as a cybersecurity risk factor.

01 Fighting the 'Forgetting Curve'

Following the invention of the "forgetting curve" by German researcher Hermann Ebbinghaus, educator David Kolb developed the modern theory of experiential learning in the 1970s. Kolb concluded that an experiential approach to learning – coupled with thoughtful reflection on the topic – is more effective for memory retention than rote learning.

Yet, experiential learning alone will not provide a maximum return on training team members to act as a human firewall against potential data breaches. The experience must be enjoyable, as well as educational.

This is where a cyber escape room comes in.

02 Why Human Threats Need a Human Firewall

Living Security client Splunk found success using our cyber escape room for experiential training, and much of that success was due to a 99% user satisfaction rate.

One Splunk user's evaluation summed it up: "This was very entertaining. Much better than just watching a video and answering questions."

A cyber escape room meets the two main functions of experiential learning: It is immersive AND engaging engaging. The Living Security escape room couples the fundamentals of behavioral science and gamification to deliver relevant, custom curriculum that does more than help an organization become compliant.

Interactive game play with puzzles and challenges to educative team members about internal threats, corporate espionage, email and web vulnerabilities, cybercrime, password hygiene and more.

99%

★★★
★★

99% of participants in Living Security experiential training who say they'd enjoy doing it again.

The Takeaway:

Cybersecurity training with an emphasis on immersion plus engagement will set the bar in 2020 and beyond by getting team members engaged with security, helping increase retention of material, and reinforcing positive security behavior.

GAMIFIED LEARNING

Gamified learning is not merely about having fun and achieving instant gratification. After all, the goal of cybersecurity training is to help employees recognize and guard against threats that could jeopardize a company. This is serious business.

What does fun have to do with it?

It turns out that fun, interesting, engaging activities might just be the key to success when it comes to helping team members retain what they learn during cybersecurity training. And that fact will help shape the industry in 2020.

01 Stimulate the Brain to Make Lessons Stick

Employees are the first line of defense against breaches, but they can only defend against what they are prepared to recognize and act on. Memories begin to fade with time, but retention is strengthened by an emotional connection to a lesson.

The neuroscience of learning is informed by four systems of the brain: cognitive (information), experiential (immersive), behavioral (motor skills) and emotional (situational awareness). All four of these systems work together to help people learn through sight, sound and touch. Science tells us that the brain is 68 percent more engaged when a person is having fun.

How does gamification help create that crucial emotional connection during the learning process?

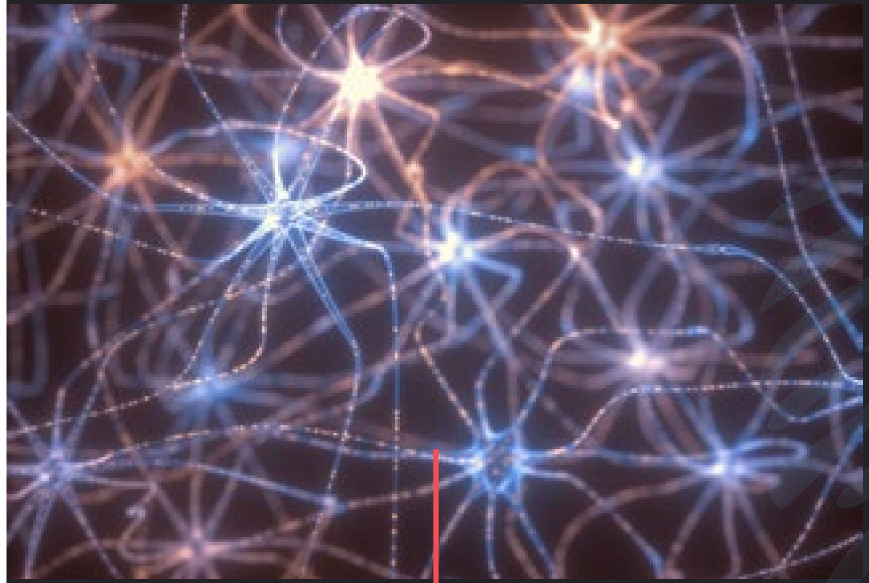
02 Achievement, Gratification, Retention

Author and educator Jonathan Cassie examined the effects of gamified learning in his 2017 book, Level Up Your Classroom. Cassie wrote that students who learn through gamification have a better capacity for persistence, develop self-direction habits, embrace risk-taking and are empowered to own their learning.

In cybersecurity training, team members can achieve that level of immersion through:

- Live-action and online puzzles
- **Immersive storylines**
- **Role-based micro-models**
- **Collaborative activities, such as an escape room**
- **Competitive activities, such as a game show format**

The lesson is connected with an emotional response, which helps reinforce the knowledge and inspire action where it matters – on the front line of an organization's cyber presence.



The systems of the brain (cognitive, experiential, behavioral, emotional) help people learn through sight, sound and touch

The Takeaway:

Gamification training will be an even more vital tool in 2020 as organizations seek to empower their employees to help guard against cyber breaches.

05 MICROLEARNING

Microlearning is the dissemination of lessons in small, digestible snippets or "chunks." The anticipated increase in its use in cybersecurity training in 2020 and beyond is a nod to the way so many consumers get their information in the 21st century – from social media-driven videos, infographics, quick reads and memes.

In the context of cybersecurity training, microlearning provides an excellent platform to effectively reinforce specific information in a short amount of time. Microlearning modules can be created for targeted training sessions, allowing an organization to customize its security training as needed.

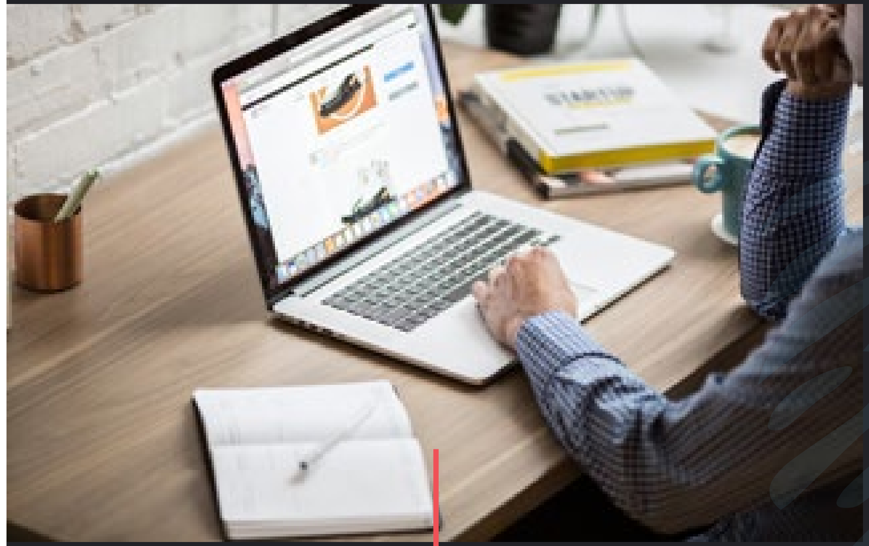
01 Customizable Experience

In addition to creating immersive experiences that address concept specific training, microlearning modules provide the opportunity to create relatable content that connects with team members.

The bite-sized lessons allow security managers to create lessons that cover specific threats, with messaging that is crafted to speak directly to members of a specific department or team.

02 Respond Quickly to Evolving Threats

As cyber threats become more sophisticated, defense mechanisms must evolve. Sometimes, even evolution is too slow, and what is required is a fast response. Microlearning modules can quickly be developed and implemented to respond to new threats.



Select the modules you want and specify participants for targeted training, and analyze user metrics for greater understanding of risk areas.

★★★★★ In 2020, Living Security will launch one new micro-module every month in order to address current and emerging threats and equip users with the awareness they need to fight back.

The Takeaway:

The use of microlearning modules for cybersecurity training in 2020 will help security awareness program managers remain agile in the face of new and more insidious cyber threats. Microlearning also will help managers boost engagement among employees with more-relevant content.

LEVERAGING VIDEO IN TRAINING

Video as a tool for cybersecurity training will become even more of a factor in 2020 as security awareness program managers, CTOs and CISOs recognize its ability to provide an immersive, effective platform for lessons that will resonate with participants.

In addition, the scalability of video presentations will enable organizations of any size to present a consistent, impactful cybersecurity message across all departments.

01 Train Smarter with Video

Video learning allows trainees to participate on their own schedules, solving the potential problem of getting all team members in one place at the same time for training sessions. In addition, it's a big potential cost-saver. Microsoft estimates that since implementing its internal video portal to facilitate training, it has reduced the per person cost of training from $320 per hour to $17 per hour. IBM says it saved $579 million across two years in training costs after shifting to an emphasis on video.

02 Education Through Storytelling

Living Security is at the forefront of using vivid, engaging storytelling to teach important cybersecurity lessons. Video enables trainers to use the "show, don't tell" method of teaching, rather than relying on rote memorization. The right story reinforces lessons by creating an emotional connection through the eyes of a well-developed, on-screen character who must respond to real-world examples of potential breaches.

03 Enterprise-Level Scalability

Video training allows for easy scalability for organizations of all sizes. A high-production episode that pits a sympathetic protagonist against potential cybersecurity threats can be shared quickly across teams, and the messaging can be quickly customized to address emerging threats. It's a faster, most-effective way to reinforce a culture of security throughout the organization.

75%

75% of employees are more likely to watch video than to read a document (Forrester Research)

The Takeaway:

Video learning is effective, cost-efficient and scalable. The emotional connections video storytelling creates will resonate with trainees. These facts will spur the growth of video as a cybersecurity training tool in 2020 and beyond.

METRICS IN ACTION

The adept security manager knows that all the enthusiasm in the world can't manage what it doesn't measure, and can't measure what it doesn't understand.

01 The Metrics Machine

Cue the metrics machine. Metrics in security awareness are science-based measurements of human risk (with predictive utility) which are followed by non-punitive, rehabilitative action steps for security awareness program owners to manage risky behavior and wage culture change.

This level of insight is possible across every data point you gather, it just takes intentionality. The truth is, "we perceive what we expect to perceive" unless we see it up close and personal across a trend line.

02 Metrics Examples

Some things are easier to measure than others. For example, phishing assessments are now the norm for companies of all sizes, in regards to "testing" their end users and analyzing their ability to not only spot a "phishy" email, but also how to properly report it based on company policy and previous training.

Let's say you send an email to 10,000 of your employees, your reports are showing a click rate of 15 percent within the HR department, 5 percent of whom reported it, and the rest ignored. You have interesting quantitative results, but not much context. Drilling in even further with the Living Security platform, you find that members of the HR department indicate a higher number of suspicious emails received and a higher than average ability to identify suspicious email successfully, but a lower than average performance score on the phishing skills training modules.

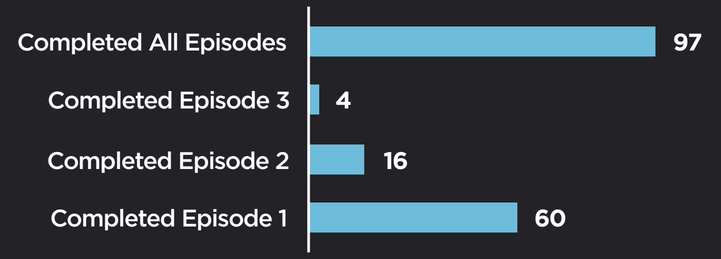
You can deduce that, qualitatively, HR has an inappropriate level of confidence for identifying a large number of suspicious emails and may benefit from additional, targeted training with an emphasis on being realistic than over-confident.

Use metrics to measure human risk, connect with people and implement cultural change.

Simon Says - General User Role Results

Unique Users	250
# of Users Completed	97
Completion Rate	39%
Overall Risk Score	90%
Phishing Score	84%
Personality Profile Participation Rate	10%

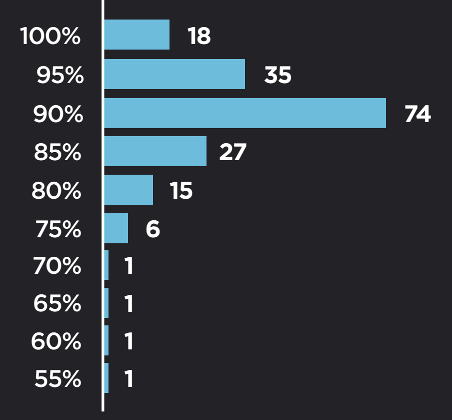
User Episode Status



Question Category Performance

Behavior	87%
Education	92%
Policy	69%
Risk Score	90%

Simon Says - General User Role Grades



The Takeaway:

As the security maturity of your organization increases year-over-year, actionable metrics become an essential element of your security awareness program.

BUILD A POSITIVE SECURITY CULTURE IN 2020

Living Security delivers engaging, scalable, effective cybersecurity awareness training that is brought to life by tech-enabled experiences. Our immersive training engages team members using science-backed techniques to strengthen an organization's cybersecurity culture through knowledge and behavior change. The content is continually refreshed to respond to evolving threats as they arise.

Ready to schedule a consultation? Contact us.

livingsecurity

livingsecurity.com

(512) 920-0422 | info@livingsecurity.com

3595 RR 620 South Suite 150
Austin, TX 78738