Security, Oct 2017. Accessed Mar 2021. www.sciencedirect.com/science/article/abs/pii/S1361372317300921.

13. Gazet, Alexandre. 'Comparative analysis of various ransomware virii'. Journal of Computer Virology 6(1), 77-90, 2010.
14. Moussaileb, Routa; Cuppens, Nora ; Lanet, Jean-Louis ; Le Bouder, Hélène. 'Ransomware network traffic analysis for pre-encryption alert'. International Symposium on Foundations and Practice of Security, 2019.
15. 'What is SIEM? Security Information and Event Management Explained'. IBM. Accessed Mar 2021. www.ibm.com/topics/siem.
16. Anumol, ET. 'Use of machine learning algorithms with SIEM for attack prediction'. Intelligent Computing, Communication and Devices, pp.231-235, 2015.
17. Menon, Rakesh. 'Log analysis based intrusion prediction system'. Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI), 2015.
18. Oliner, Adam; Ganapathi, Archana; Xu, Wei. 'Advances and challenges in log analysis'. Communications of the ACM, 55(2), pp.55-61, 2015.
19. Krizak, Paul. 'Log analysis and event correlation using variable temporal event correlator (VTEC)'. LISA '10: 24th Large Installation System Administration Conference, 2010.
20. Rajan, Sheena; Khanna, Ashish. 'Real-time data aggregation and analysis: a new era machine learning'. International Conference on Innovative Computing & Communications, 2020.
21. Mallissery, Sanoop; Praveen, K; Sathar, Shahana. 'Correlation of alerts using prerequisites and consequences for intrusion detection'. International Conference on Computational Intelligence and Information Technology, pp.662-666, 2011.
22. NiranjanRaja, M Siva; Vasudevan, AR. 'Rule generation for TCP SYN flood attack in SIEM environment'. Procedia Computer Science, 115, p.580-587, 2017.
23. Bilge, Leyla; Balzarotti, Davide; Robertson, William; Kirda, Engin; Kruegel, Christopher. 'DISCLOSURE: detecting botnet command and control servers through large-scale Netflow analysis'. 28th Annual Computer Security Applications Conference, 2012.
24. Karnikis, Karolos; Thompson, Erick; Ivanov, Ivaylo; Graham, John; Hickey, Jason. 'Systems and methods for cyberthreat detection'. US Patent Publication No.US 2013/0232576A1, 2013.
25. Murphey, Rich. 'Automated windows event log forensics'. Digital Investigation 4, pp.92-100, 2010.
26. Kim, Ikkyun; Kim, Daewon; Kim, Byunggoo; Choi, Yangseo; Yoon, Seongyong; Oh, Jintae; Jang, Jongsoo. 'A case study of unknown attack detection against zero-day worm in the honeynet environment'. International Conference on Advanced Communication Technology, IEEE, 2009.
27. Patel, Reshma; Thaker, Chirag. 'Zero-day attack signatures detection using honeypot'. International Conference on Computer Communication and Networks, pp.79-85, 2011.
28. Todd, Michael; Koster, Scott; Choy, Patrick; Wong Ming. 'System and method for securing a network from zero-day vulnerability exploits'. US Patent No.US9264441B2, 2012.

Gamification – can it be applied to security awareness training?

David Emm

David Emm, Kaspersky

Typically, and traditionally, people don't enjoy corporate learning. Many workers associate its various forms – from health & safety, compliance and cyber security training – as a mundane but necessary tick box that disrupts their normal workload.

Research supports this: 42% of respondents working in companies with more than 1,000 employees said that the majority of training programmes they attended were 'useless' and 'uninteresting'.[1,2] Unfortunately, the well-documented risks surrounding cyber attacks and data leaks have not been enough to make cyber security training an exception to this rule.

Within this lies an immense risk for businesses. The research also found that careless and uninformed staff are the second most likely cause of a serious security breach, second only to malware. In addition, in 46% of the cyber security incidents that took place in the past year, uninformed staff contributed to the attack. With phishing and social engineering scams on the rise, and coupled with the increased responsibility of remote working, it has never been more vital that employees engage with cyber security training.

Looking for engagement

With apathy towards cyber security training presenting a huge risk for businesses, many organisations have increasingly been looking at ways of revolutionising their training methods, with engagement being the highest priority. With this in mind, game-based courses, in which cyber security training is delivered in the format of video games, are increasingly becoming a go to-method for businesses in a variety of different sectors. The idea is that by blending entertainment, competition and learning, businesses can ensure that cyber security measures become more engaging and are taken up more enthusiastically.

Of course, there are an equal number of business leaders that remain sceptical. Some customers don't feel comfortable about implementing gaming techniques in corporate education, primarily because they still believe that 'games' are merely recreational outlets for teenagers and children. Naturally, people that believe this are less inclined to believe that adults – and especially business executives – should even play games, let alone use them in education.

From the experience of organisations that have tried it, however, this is simply not the case. The process of gamification (when only some game elements are added) offers a fantastic way to learn and explore ideas within a controlled environment. However, in order to advance with this, it is paramount we understand the potential limitations and barriers with security awareness games, so that they are implemented effectively.

Core barriers

Perhaps the largest barrier to even the most basic cyber security game is the size and scope of the experience. The extent of even the most basic cyber security rules can be very large, and as such, a great many factors need to be accounted for when security training is 'gamified'.

Strong cyber security simulations need to contain all possible situations, and a successful cyber security game would need to challenge employees to 'check' every potential option until they consistently came to the most secure decisions. This could be seen as a daunting task for many cyber security vendors, who may run the risk of producing an experience that is either overly long and unengaging, or conversely, not extensive enough to provide genuine training. Creating an effective cyber security game will require expertise from across game development and cyber security, and the final experience needs to strike a balance between education and engagement.

This is not the only factor to consider. Engagement can prove to be an issue in and of itself. As a person is immersed in an artificial environment, gaming techniques require concentration and involvement. Research shows that the human body reacts to stress in a game the same way as during problematic situations in real life.[3] This is why people may even feel tired after playing video games. In a game based on cyber security basics, the player will constantly face dilemmas – after all, the decisions could affect their virtual money or career, for example.

After several hours of such training, we both expect and advise employees to not simply return to their duties, but to instead find time to rest, recover and reflect.

Enhancing cybersafe behaviour

Before exploring the benefits of gamification, it is important to understand the ultimate aim of any security awareness course.

Cyber security training is introduced to not only encourage staff to study cyber security rules, but to ensure that employees gain the appropriate skills and understanding, as well as apply that learning. Commonly, guidelines are not always the most convenient for employees, and within fast-paced or high-pressure environments, they can even be considered cumbersome. For example, it is easier to share a confidential document through the same cloud storage that an employee uses to store personal photos of their family and friends, instead of using a secure, corporate-specific service. As such, in the interest of changing such behavioural patterns, it is necessary to not only provide instructions, but also train and develop practical skills.

In this regard, a game turns out to be a very effective option to encourage employees to not only learn, but also apply cyber security protocols. Like anything else, the best way to understand why (or why not) one should act in a certain way is often trial and error. Of course, in the case of cyber security, a company cannot let every employee do something wrong – such as wait until a document is leaked to malefactors – just to see how severe the consequences of a cyber attack could be.

What businesses can do instead is explore the consequences in a controlled environment. The immersive and involved nature of games provides a great opportunity for this, and when coupled with elements of competition and team play, in-game mistakes can feel just as painful as real-life slip ups. Hopefully, by the time the employee came across the real thing, cyber security protocols would be practically muscle memory after ample experience with its in-game counterpart.

Erasing the barriers

As a culmination of all of this, gamification also becomes a positive way of overcoming initial resistance to learning. The context of a game situation ensures a base level of engagement in the material – even if it is simply just to win against the opposing team.

This competition element is key. In addition to the employees with little interest to learn, there will always be some employees who are sure that they have already mastered cyber security skills, and that any course is a waste of time. Businesses can look to overcome this attitude by adding another level of engagement to the training – competition. With a short, competitive test, where a person makes bets, sets records and challenges their friends, proving your mastery over the material becomes increasingly more appetising.

Moreover, experience also shows that, despite the doubts of managers responsible for training, business executives are often excited to get involved in game formats – for example, a gaming experience where C-level managers try to walk in the shoes of CISOs. As a result, they get first-hand experience of how cyber security may affect the business, including critical areas such as profit losses and employee wellbeing.

Getting employees of all levels to engage in e-learning is the first step in making it more productive. Cyber security is a collective responsibility and workplace culture is a key part of ensuring that cyber security protocols are adhered to across the board. In this regard, the team-based nature of cyber security games offers a way to build the positive and effective communication that is crucial to building a secure workplace.

Gaming in the future

Successful education on cyber security basics should consist of different formats. Gaming techniques are not a silver bullet and alone they will not solve all issues related to corporate education or cyber security. However, as employee engagement, communication and behaviour become paramount to the safety and continuity of businesses, gamification is a great place to start.

As with all aspects of cyber security, however, there are no half measures. For gamification to produce the best results, businesses and vendors should believe in, and commit to, the concept. Naturally, for cyber security games to work, they must be enjoyable. Just because the subject material may be serious and somewhat inflexible does not mean that vendors cannot get creative about how they engage their audience. Where possible, vendors should even look to hire developers with previous game experience, to deliver a product that meets the high standards of non-educational video games.

On the flip side, and perhaps more importantly, businesses should look to embrace cyber security games with enthusiasm and an open mind. Workplace culture is an unshakable part of a business's ability to deal with cyberthreats, and cyber security games present an exciting way to enhance not only employee behaviour, but also morale, while reducing risks to the business.

About the author

David Emm is principal security researcher at Kaspersky, having joined the company in 2004. He is a member of the company's Global Research & Analysis Team (GReAT) and has worked in the anti-malware industry since 1990 in a variety of roles, including that of senior technology consultant at Dr Solomon's Software, and systems engineer and product manager at McAfee.

References

1. 'Disconnected'. Kaspersky. Accessed Apr 2021. https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_%5bdis%5dconnected_datasheet_0121EN_Gl.pdf.
2. 'The Digital Talent Gap'. Capgemini/LinkedIn. Accessed Apr 2021. www.capgemini.com/wp-content/uploads/2017/10/report_the-digital-talent-gap_final.pdf.
3. Aliyari, Hamed et al. 'The beneficial or harmful effects of computer game stress on cognitive functions of players'. Basic and Clinical Neuroscience, May-Jun 2018, 9(3): 177–186, doi: 10.29252/nirp.bcn.9.3.177. Accessed Apr 2021. www.ncbi.nlm.nih.gov/pmc/articles/PMC6037427/.

Securing connectivity for remote workforces

Matias Katz, Byos

Matias Katz

In the ongoing work-from-home (WFH) evolution, the need to better secure employee endpoints has emerged as a key issue. Many organisations have discovered what network and security professionals have long known – once the endpoint is outside the perimeter, the level of security is degraded.

This has become every organisation's reality as employees' home networks have become prime targets. The stats show there are typically 10 or more unmanaged devices connecting to the average home wifi network, such as personal laptops, cellphones, gaming consoles and home IoT devices.

A recent Dark Reading survey asked infosec practitioners: "Which cyber security aspects of the Covid-19 crisis are most likely to increase risk?". Almost 40% of respondents ranked vulnerabilities in the remote access systems and processes that support remote workers as a top threat, another 38% cited vulnerabilities in devices used by quarantined home workers to access enterprise data, and 24% cited vulnerabilities in service provider connections used by remote workers.

Their concern is justified, given both WFH imperatives and increasing regulatory and privacy pressures. Legacy services and methods have not effectively addressed network security and governance beyond the organisation's network perimeter, nor have they provided meaningful visibility and control over remote users and their connections.

The gap in today's cyber security posture is a layer of isolation from the threats of remote and 'dirty' home networks. Threat actors know all of this and increasingly exploit it for targeted attacks. After gaining access through any device on a home wifi network, they seek to move laterally to and through their main target – the corporate devices and data.

Struggle to secure

Lacking an effective, scalable way to monitor or enforce secure behaviour, IT teams struggle with securing remote users. The Centre for Internet Security (CIS) advises: