feature

Security in an Age of Distraction

In addition to the challenges that security awareness programs have always faced in obtaining the attention of participants and communicating information to promote secure behaviors, practitioners must deal with a new obstacle—individuals distracted by a multitude of electronic devices. Members of all generations have adopted mobile technologies, including smartphones, tablets, MP3 players, laptops, game players and hybrid combinations of these devices. Today, people are regularly connected by a myriad of devices and technologies. While mobile devices have enhanced productivity, these devices compete for limited attention span and may make it more difficult to gain sufficient attention for security awareness.

To be effective, secure awareness professionals will need to acknowledge this challenge and create strategies to manage electronically distracted participants.

Technology's Impact on Learning and Retention

While current technology makes it possible to make former lulls potentially productive time, it may be at the cost of acquiring and retaining new information. Scientists at the University of California (USA) have discovered that the brains of rats show new patterns of activity when engaged in new experiences.

However, it is only when there is a break from the new experience that those patterns are processed to create a persistent memory of the new learning. It is believed this same learning phenomenon applies to humans. Loren Frank, assistant professor at the university who specializes in learning and memory, states, "Almost certainly, downtime lets the brain go over experiences it's had, solidify them and turn them into permanent, long-term memories." Frank goes on to state that constant brain stimulation may prevent or inhibit this learning process.[1] This could have an impact on the effectiveness of security awareness efforts. In addition to managing participants who may already be distracted by mobile devices, the constant barrage of stimulation may make it more difficult for those involved to retain the information presented.

Splitting attention between electronic devices and other activities is referred to as multitasking. Multitasking is a misnomer for task switching because the brain has a finite amount of attention and productivity. According to Guy Winch, Ph.D., "It's like a pie chart, and whatever we're working on is going to take up the majority of that pie. There's not a lot leftover for other things, with the exception of automatic behaviors."[2] Task switching creates a scenario in which neither activity gets the brain's full resources and tends to miss important details of one or both tasks.

> **"Multitasking is a misnomer for task switching because the brain has a finite amount of attention and productivity."**

In addition to the possible impact on learning and retention created by electronic device usage, there has been an overall decline in the frequency and proficiency associated with a skill used in the majority of learning—reading. The percentage of Americans who read the paper has declined over the last decade from 41 percent to 23 percent. Forty-three percent of American adults read at or below the basic level.[3]

The combination of these factors makes developing an effective security awareness program even

Kerry A. Anderson, CISA, CISM, CGEIT, CRISC, CCSK, CFE, CISSP, CSSLP, ISSAP, ISSMP
Is an information security professional with more than 17 years of experience in information security and compliance. She is an adjunct professor of cybersecurity and has been a speaker, panelist, moderator and chairperson at many professional conferences. Anderson is the author of numerous articles in professional journals and the book *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture* (CRC Press).

more difficult than in the previous decade. Security awareness may need to add some new tricks to its training tactics. Strategies for promoting security awareness in the current climate include:

1. Give them what they want (securely). The method of approaching a topic matters with respect to the amount of communication that audiences will receive and the potential for its continuing impact. People may act in ways that they should not, even when they know how they ought to act.

Often, individuals engage in unsafe behaviors because they prioritize achieving work tasks or personal desires over security requirements. Individuals will utilize their creativity and technology prowess to accomplish their objectives. The net result may be the creation of security risk. For example, a security policy may explicitly forbid the use of Universal Serial Bus (USB) drives or third-party email accounts to access organizational files from remote locations, but individuals may use personal drop boxes as a way of gaining access to these files. The information security challenge is to unite the desire to accomplish a task with the appropriate security. By offering secure alternative ways to accomplish a task, achieving compliance becomes easily possible. For instance, in the example of providing remote-access to files, the organization could make employees aware of an enterprise remote-access solution or establish a private cloud drop box for storing its files. This requires a shift in mind-set for information security; rather than prohibiting actions, the department can try to find ways to facilitate employee needs while prioritizing security.

2. Have adult conversations. Some information security practitioners may, on occasion, view end users as risk factors that need to be controlled. This mind-set may bleed into awareness training through the language used, body language or humorous anecdotes that make end users look silly. To encourage end users to behave like responsible Netizens[4] or corporate citizens, it is important to view security awareness as having adult conversations that embody two-way dialogue. According to Steve Durbin of the Information Security Forum, "You need to have adult conversations. You can't do it at all levels of the organization, but you should really try to be trusting, empowering and motivating across as much of the enterprise as possible."[5]

> This also involves creating accountability for security-related behaviors. Durbin says, "You have to try to do away with ignorance around all of this. It is about getting across what good information security behavior looks like. If someone makes an honest mistake, you want them to come forward. Create a positive environment where people understand that it happens."[6]

3. Consider the timing of awareness events. Some times of day are characterized by an increase in the amount of distraction. Early morning or late afternoon, when individuals may feel compelled to catch up on email or check in with social networking sites, tend to be especially prone to distraction. Some trainers used to try to avoid the after-lunch hour because of potential attention issues created by fluctuations in circadian rhythms. However, this might be an ideal time as participants may have used the lunch hour to check their devices.

4. Use social media and applications. The old adage goes, "If you can't beat them, join them."[7] Electronic devices have created an expectation that a blend of technology and entertainment can be used to get and maintain attention. Social awareness professionals may find it effective to add social media, YouTube-style videos, microblogging (e.g., Twitter), photo sharing (e.g., Instagram), games (mobile and multiplayer) and mobile applications to spread information about security practices.

5. Use micromoments. When designing awareness content, shorter is better in terms of retaining attention of distracted users. On average, the duration of a mobile game session is under six and a half minutes, and some popular games have a duration under three minutes. Mobile game makers have an objective to utilize small amounts of free time. According to Sebastien de Halleux, a cofounder of a mobile gaming company, "Instead of having long relaxing breaks, like taking two hours for lunch, we have a lot of these micro-moments" and "have reinvented the game experience to fit into micro-moments."[8] Content

should fit into smaller time slots for consumption. People learn better when they can focus on small bits of information that the mind can easily assimilate. Short training bursts are more effective and adaptable to social media formats.

6. Use guerrilla marketing. Guerrilla marketing is an advertising strategy that utilizes low-cost and quirky marketing techniques to achieve great outcomes. It originated from guerrilla warfare, a tactic that used unconventional civilian warfare tactics that depended largely upon the element of surprise. Guerrilla marketing brings this same tactical approach to marketing.[9] The hallmarks of guerrilla marketing are innovation and energy to take the intended audience by surprise and leave a lasting impression. Popular Internet terms for the objective is creating social buzz or "going viral."[10] The primary benefits of guerrilla marketing are its low cost and valuable impression with consumers at a more personal and memorable level. Some possible ideas using guerrilla marketing to raise security awareness include:

- Hiding secret clues and surprises in printed collateral, web sites and physical locations to earn rewards on security web sites and clues in monthly newsletters
- Having flash mob events, e.g., assembling in a given location to perform a security-related activity with a unique twist that is filmed and sent to all organizational locations
- Using contests that require multiple interactions that present different security-related messages, such as scanning a quick response (QR) code on a security poster and visiting a link in an article in the security newsletter or blog
- Having live events (disc jockey, coffee bar, scavenger hunt) with a security-related theme, such as "do not become the 'phish of the day'"
- Gamification[11] of security content to earn points to win rewards by creating a security game that presents multiple scenarios in which a "hacker" tries to trick the individual into performing insecure behaviorsThe key to successful use of guerrilla marketing tactics with a distracted audience is to gain full engagement by minimizing the opportunity to use mobile devices, for example, by incorporating activities that require use of the hands.

7. Recruiting brand advocates. Security awareness professionals may wish to consider the information security program as a brand and develop brand advocates. It is important to build a strong brand around the information security program. Brands grow by word of mouth. While only 12 percent of people believe ads, 96 percent of individuals will act on a friend's recommendation.[12] Security awareness professionals need to reach out to the organizational community to build a network of advocates for the program. Friends promote brands to other friends, and messages from friends may cut through the distractions.

8. Use fear of missing out (FOMO) creatively. A new psychological term, FOMO, seems to apply especially to younger generations. FOMO captures the phenomenon of people experiencing anxiety if they believe they are missing what is trending or the next big event. To allay that anxiety, they remain constantly connected. A way of exploiting FOMO is to promote live and online awareness campaigns or sponsor contests. Some ways to create FOMO for security awareness sites might include:

- Contests to create awareness using social media channels
- Security-themed games (mobile and multiplayer) with prizes for high scores
- Live awareness events, such as expos or parties, with social media reporting

Successfully Competing in a Distracted Universe

Messages competing for a slice of people's attention bombard all generations daily. Until recently, most distractions originated from external sources. The average individual living in an urban locale views up to 5,000 advertisements per day.[13] To cope with this constant onslaught of information, individuals become adept at blocking out most messages; the messages

become white noise. In addition to these external distractions that are not so welcome are the diversions people invite into their lives in the form of a multitude of electronic devices. These numerous sources of distraction make it more difficult to engage individuals fully in awareness efforts, especially in ways that will enable them to retain the information communicated to effect behavioral changes.

To be effective, security awareness professionals will need to acknowledge this challenge and create strategies to manage distracted participants. This requires transforming security awareness programs to meet these challenges by adapting many of the same techniques that distract individuals such as microblogging, viral videos, applications and games. To remain relevant, security awareness must evolve with the times and not become stuck in the past.

Endnotes

1 Richtel, M.; "Digital Devices Deprive Brain of Needed Downtime," *The New York Times*, 24 August 2010, *www.nytimes.com/2010/08/25/technology/25brain.html?_r=0*

2 Etailinsights, "Why Multitasking Doesn't Actually Increase Productivity," 24 November 2014, *www.etailinsights.com/blog/multitasking-productivity*

3 Leach, J.; "Can We Get the 'Distracted Generation' Reading Again?" *Daily Genius*, 14 August 2014, *www.dailygenius.com/can-get-distracted-generation-reading/*

4 This is a combination of the terms "Internet" and "citizen" that is defined as an entity or person actively involved in online communities and a user of the Internet, also referred to as cybercitizens, *www.columbia.edu/~rh120/ch106.x01.*

5 Olavsrud, T.; "10 Tips to Embed Positive Information Security Behaviors in Employees," *CIO*, 21 May 2014, *www.cio.com/slideshow/detail/153570/10-Tips-to-Embed-Positive-Information-Security-Behaviors-in-Employees*

6 *Ibid.*

7 "If you are unable to outdo rivals in some endeavor, you might as well cooperate with them and thereby possibly gain an advantage." See Oxford Dictionary, "If you can't beat them, join them," *www.oxforddictionaries.com/us/definition/english/if-you-can't-beat-them-join-them.*

8 *Op cit,* Richtel

9 Levinson, J.; *Guerrilla Advertising*, Houghton Mifflin Company, USA, 1984

10 Going viral refers to digital content that has spiked in popularity and reached a large number of users quickly. While there is no exact number of views that makes something go viral, most viral media is viewed by more than a million people in less than a week. See TechTerms, "viral," *http://techterms.com/definition/viral.*

11 "The application of typical elements of game playing (e.g., point scoring, competition with others, rules of play) to other areas of activity, typically as an online marketing technique to encourage engagement with a product or service," Oxford Dictionary, "gamification," *www.oxforddictionaries.com/us/definition/american_english/gamification.*

12 SocialAgenda Media,"Selling Despite Distractions: Customer Retention and Repeat Sales," 14 December 2013, *http://socialagendamedia.com/digital-pr-blog/selling-despite-distractions-customer-retention-and-repeat-sales/*

13 Story, L.; "Anywhere the Eye Can See, It's Likely to See an Ad," *The New York Times*, 15 January 2007, *www.nytimes.com/2007/01/15/business/media/15everywhere.html?pagewanted=all&_r=1*