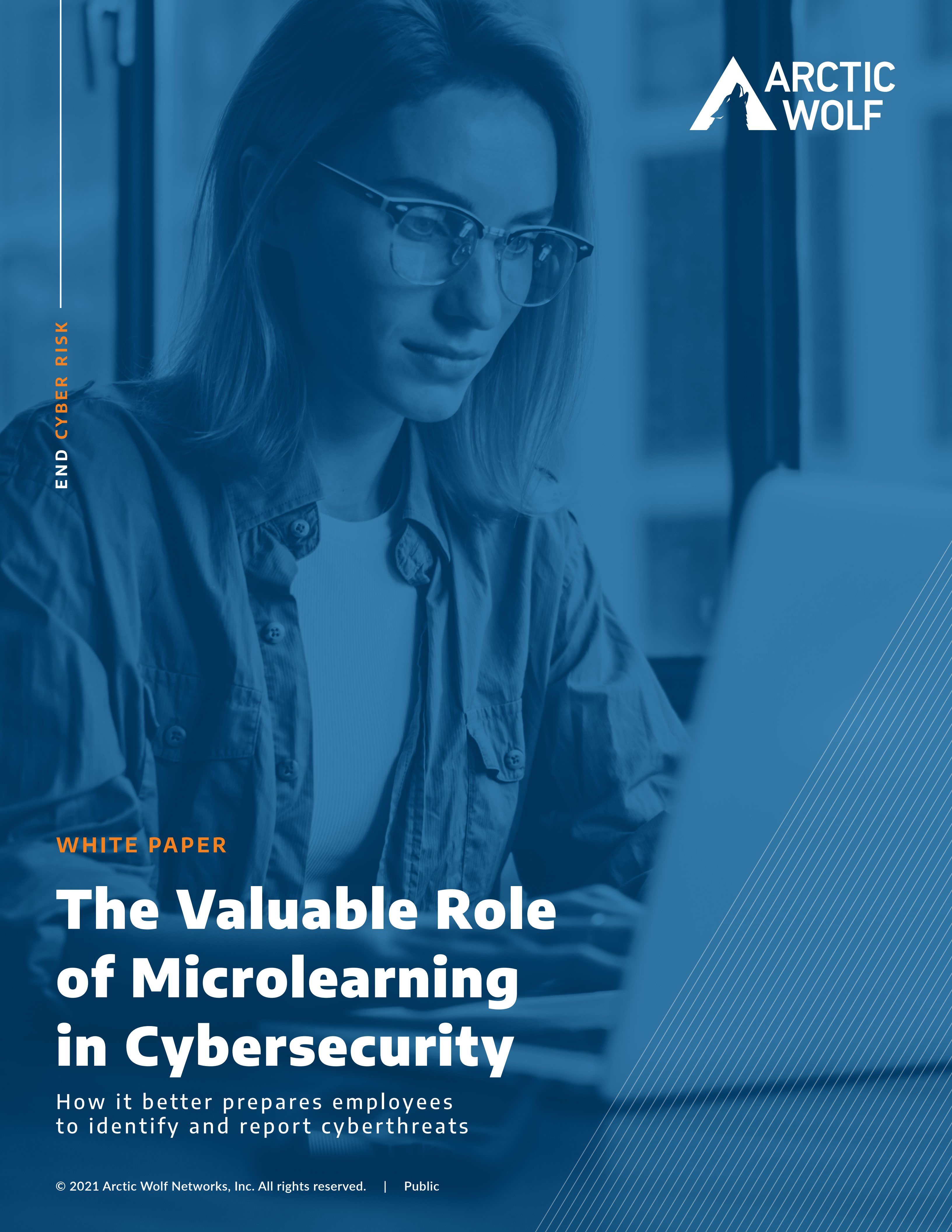


END CYBER RISK

WHITE PAPER

The Valuable Role of Microlearning in Cybersecurity

How it better prepares employees to identify and report cyberthreats

Table of Contents

Executive Summary

Data breaches and cyberattacks continue to be a serious threat to organizations, and the risk is only on the rise. Attacks are growing at 20 percent a year, and can affect businesses, their supply chains, customers, and partners.

Technology tools used to prevent, detect, and react to security threats are a key weapon in the battle against ransomware and other attacks. But there's another critical step organizations must take to protect themselves: Educating employees on how to recognize potential attacks—such as phishing and social engineering—and what they need to do in response to avoid providing an entryway for attackers.

All too often employees are considered the problem, or the weakest link, and get blamed for being unprepared and falling for a clever attack. Rarely do businesses look at the bigger picture, and evaluate whether their training tools are effectively educating and preparing people for the threats they may encounter. Security awareness training tools are not all the same. The methodology, strategies, and development behind them can have a significant impact on the results they produce.

A holistic, skills-based approach that incorporates short-session learning techniques as an educational strategy is microlearning. This white paper explores why microlearning is the most effective way for modern adults to learn and successfully retain useful information about security awareness, and why it essential in a time when bad actors use increasingly sophisticated social engineering attacks to plague businesses of every size.

01

Microlearning Techniques in Security Awareness Training

Microlearning Techniques in Security Awareness Training

The microlearning technique teaches cybersecurity information in small chunks over short periods that are easy to learn and absorb and recall. Instead of taking employees away from their jobs for hours or days at a time with a fire hose full of information they soon forget, microlearning sessions are easy to digest, and can become a convenient part of an employee's normal routine.

Microlearning follows six basic principles:

01 Learning is presented in short sessions.

02 Each session is narrowly focused.

03 Accessing the session is convenient and frictionless.

04 Each session has a clear and practical application.

05 A performance-based measuring system gauges improvement.

06 It must drive a culture of ongoing learning.

Microlearning is optimized for retention, and specifically how the brain learns about things that may need to be recalled later on, unexpectedly, and under stressful conditions. That makes microlearning ideal for security awareness education. Microlearning ensures employees will recognize and be prepared to respond to the signs of an attempted attack, months or years after their training, even when they're fully engaged in their day-to-day work.

How Microlearning Takes Advantage of Brain Processes That Help Us Remember

To understand why microlearning is so effective at preparing employees to recognize and respond to threats, it helps to look at how the brain processes, stores, and recalls information.

We're constantly bombarded by far more information than our brains can possibly pay attention to and retain. A continuous current of sights, sounds, messages, and interactions hits us, but the brain can only think about four things at once, according to experts. Everything else gets sifted out and ignored. To make the best use of this limited capacity to focus, the brain enlists strategies to determine what gets noticed and what doesn't to ensure the right information gets stored, so that we can recall it when needed.

The three primary strategies the brain uses to filter and store information are spotlighting, chunking, and assimilation/accommodation.

SPOTLIGHTING

This filtering technique is what the brain uses to ignore certain information that may not be pertinent, while concentrating instead on what matters. The brain primarily does this by quickly detecting anomalies—that is, what seems different from everything else, what changes, or what's most unexpected. At the office, for instance, the appearance of a stranger is more likely to grab your attention than seeing one of your usual office mates.

According to predictive mind theory, even without obvious anomalies the brain naturally predicts which information matters most. So, only that information surfaces into our conscious awareness, and we remain unconscious of the rest. Staring out a window at the street, you might not be aware of the individual cars in the stream of traffic—but you'd snap to attention if your car drove by when it was supposed to be parked in your garage.

We can also consciously choose to spotlight information, in what is commonly referred to as "the cocktail party effect." For example, there could be a lot of background noise—plates and silverware clanking, many conversations happening at once—but, because you choose to focus on the conversation in which you are engaged, your mind will subconsciously tune out the background noise so it's not a distraction.

Microlearning aligns with this function of the brain by staying within a brief amount of time. That way, the learner doesn't have to continuously exert energy to ignore the inevitable distractions they experience in their work environment. It is much easier for someone to tune out distractions and remain focused on one task for three minutes or less than it is to get undivided attention for an hour or more.

CHUNKING

This technique addresses the brain's ability to easily store and recall a set of four or fewer pieces of information, but struggles with larger sets. The idea is simply to break down the larger set of information into smaller sets that are more easily memorized.

A familiar example: North American seven-digit phone numbers are grouped as a chunk of three numbers and a chunk of four numbers—a single unbroken chain of seven numbers is more difficult to memorize. That's why 867-5309 is easier to remember than 8675309.

Visual information can be chunked simply by creating spaces around small groups of visual data, and audio information can be chunked by setting it to rhythms, which is in part why the words to a song (like 867-5309/Jenny) or poem may be easier to remember than a string of unbroken prose.

The brain's natural behavior of chunking aligns with microlearning because the short and singular focus of a microlearning session restricts the instructor to strategize their message with only necessary details on a singular topic, typically in short lists that can be easily understood and retained by the learner.

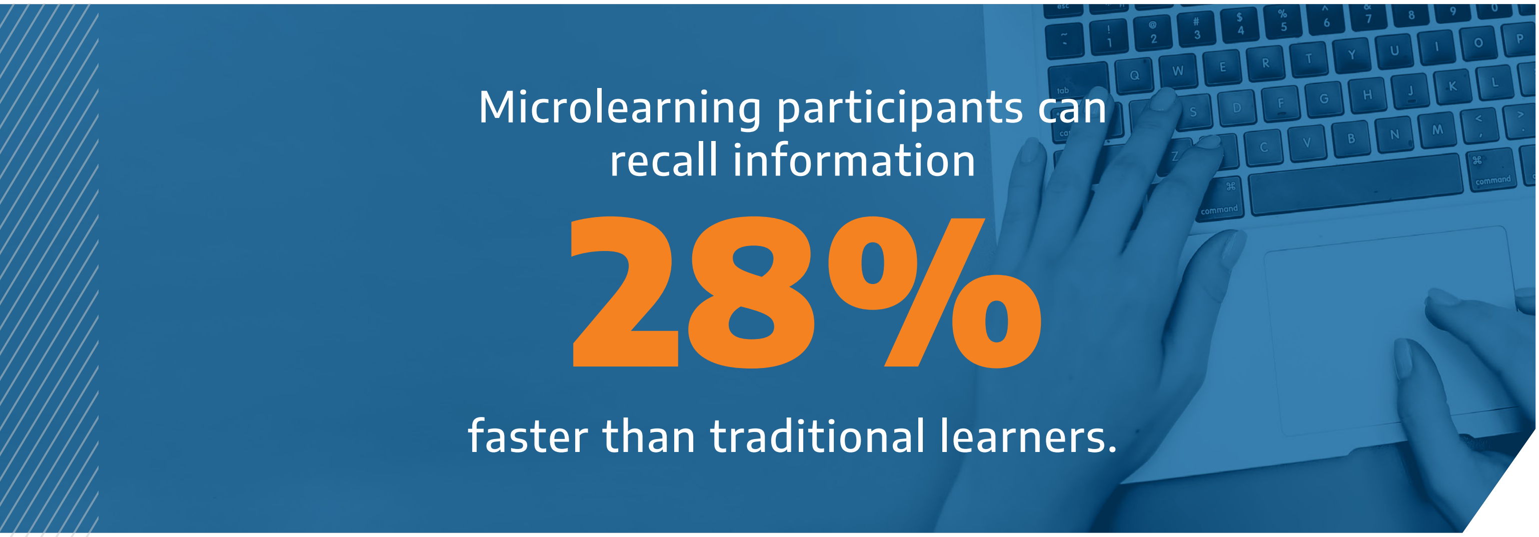
ASSIMILATION AND ACCOMMODATION

These are the brain's approaches to efficiently associate and store information for better recall and application when needed.

The brain develops "schemas," which are useful ways of structuring information. When it takes in something new, it quickly determines how the information might neatly be assimilated into an existing schema, so it can be stored there alongside other, similar information.

However, when a new piece of information doesn't mesh with an existing schema, the brain accommodates it by adjusting the existing schema or creating a new one. Your brain's ability to rapidly assimilate and accommodate information is extremely important for memory recall. It's like filing papers into certain drawers and files so you can easily remember where they are and access them quickly when needed.

While learning, the mind rapidly assesses the information it receives to determine if it's something familiar so it can quickly store it. But if, for instance, you hear about something for the first time, the brain must create a new way to understand and remember it. As a result, traditional security awareness training sessions from 30 minutes to days on end typically lose the attention of learners. They overtax the brain, forcing it to continually make these assessments and creative decisions, which leaves employees mentally exhausted.



Microlearning participants can recall information

28%

faster than traditional learners.

Applying Brain Functionality Traits to Microlearning

Microlearning strategically limits the amount of new information, and only presents as much information as can be fully understood in a given session.

That way, your mind doesn't need to work extra hard to recall information that you first heard days, months, or even years previously. It gives your mind more working power to pay attention during a current session, rather than becoming distracted with having to recollect what happened in prior sessions.

As discussed earlier, spotlighting, chunking, and assimilation/accommodation work together to help the brain take in and remember needed information. People do not simply take in all the information around them and store it in the brain as is. Rather, the mind actively spotlights the information predicted to be most important, chunks the information into small sets in order to better remember it, and assimilates or accommodates it into schema so as to organize the information for efficient recall.

Microlearning is designed to present information in the format of how the brain already functions, ensuring people remember what they're taught and can recall the information they most need exactly when they need it. Allowing the brain to function most efficiently greatly increases the rate of retention and recall speed of learners.

02

Incorporating Powerful Learning Strategies

The basic principles of microlearning go back decades, but the technique has become increasingly popular in recent years in parallel with the growing impact of digital technology and the resulting impact of information overload.

90%

Ninety percent of all data ever gathered by humans was generated in the past two years and the rate of data growth increases every second. As a result, it's more important than ever to use learning strategies that help narrow down what we need to know and why we need to know it.

MICROLEARNING VS. MACROLEARNING

Microlearning provides an alternative to the teaching methods typically encountered in schools, courses, seminars, and workshops—not to mention those of many security awareness training tools. "Macrolearning", a deep dive and lengthy study of a given subject, usually asks learners to absorb a lot of information about a narrow subject over an extended chunk of time. It can work well in certain situations. For instance:

- If the goal is to instill narrow and in-depth learning on a topic, and push a learner toward mastery of the subject.
- When learners are in a good position to allocate several hours at a time to a given class.
- When a learner is already engaged with or passionate about the subject matter, and is self-motivated to pay attention and apply effort and discipline in order to absorb the material.

In contrast, microlearning occurs in short chunks, each designed to provide a much more digestible and convenient lesson, so information is easier to grasp and recall. It assumes learners may not be especially motivated to pay close attention, and aims to impart key points rather than an overwhelming level of detail.

Microlearning is ideal for addressing different topics one session at a time, helping students achieve a narrow, well-defined objective. For example, instruction that helps them recognize a specific set of critical situations and recall the appropriate responses to them. In other words, microlearning is highly effective when someone needs to keep many different pieces of information top of mind. In terms of security awareness training where employees must learn about the indicators of cybersecurity threats and dangers, and how they need to respond, microlearning has clear retention and recall benefits.

The following are six key characteristics that make microlearning so effective for employee cybersecurity training.

01 Learning is presented in short sessions.

Microlearning sessions are short. According to a study by MIT, the highest engagement comes in sessions of three minutes or less. This offers the advantage of being convenient for employees who often need to fit training into an already busy schedule.

Keeping material under three minutes requires content producers to focus on only the most critical information. This creates a more valuable viewing experience and respects a learner's valuable time. Ongoing microlearning programs build trust with their audience by delivering lessons of consistent length, unlike other programs where the lesson time varies widely. Viewers understand that a true microlearning program won't waste their time, bore them, or overly tax them. For that reason, the three-minutes-or-less rule is essential.

02 Each session is narrowly focused.

The brain works hard to take in information and store it efficiently for on-demand recall. If a presenter shares too many pieces of separate information or jumps between different topics, the brain works that much harder. Since a variety of topics entails less association between different pieces of information, it becomes more difficult for the brain to efficiently store that information.

What's more, in order to make it into the brain's long-term memory, new information must first reside in "working memory," where the information is accessible but soon fades away. According to cognitive load theory, the information won't be promoted from working memory to long-term memory for more permanent storage unless it's rehearsed—that is, the brain has to access it at least a few times while it's still in working memory. In an ongoing microlearning program, it's easy to revisit topics, principles, and conduct practical assessments since they take up little time and focus on just one learning objective at a time. The opposite is true when training is relegated to long sessions only a few times a year. If material spans different topics and is spaced months or years apart, there is little opportunity to rehearse all of it before the knowledge fades away.

03 Accessing the session is convenient and frictionless.

Anyone who has jumped through multiple hoops in order to access an online presentation knows how annoying and time-wasting the process often is. That's why part of the microlearning approach is to push content out to learners without barriers to access the material.

Making things easy for learners increases the chance they will engage with the material. According to bioscience eLearning expert, Dr. Nick Morris, if they have to work to get at it, they won't just feel annoyed; they may drop the lesson altogether.

Even Walt Disney observed that the vast majority of people will only go so far out of their way to complete a task. In his theme parks, he observed how many steps people would be willing to take to deposit litter in a trash can. When the nearest can was more than 30 feet away, participation plummeted. This led to a park rule that trash cans be placed no more than 30 feet from each other.

In terms of learning and its constraints, people also have their limits. They are typically busy enough without the demands of additional training. Adding barriers to the task—such as having to locate assignments on an eLearning portal, or needing to reset a forgotten username or password—is simply a recipe for discouraging and disengaging learners.

04 Each session has a clear and practical application.

We're more likely to remember something if we have a clear understanding of why it is important or essential to our job functions or responsibilities. Will there be opportunities or situations to put the lessons we learn into practical use? If so, we're more apt to remember the information.

Microlearning equips people with an understanding of why they need to learn something when they need to know it, allowing for immediate and practical application. Using the information to make a decision or take an action makes the brain far more likely to take in and process that information, while also committing it to long-term memory.

05 A performance-based measuring system gauges improvement.

An essential part of microlearning is its ongoing tracking, measuring, and performance reporting of the overall program. Unlike macrolearning, such as a university course where a learner could spend a semester diving deep into subject matter before being assessed with a grade for a final exam or term paper, microlearning tracks each piece of the program in order to give a clearer understanding of each learner's ongoing engagement.

Tracking and understanding how each learner performs on assessments, what their participation level is, and evaluating their performance in the practical application of their lessons is essential. To be most effective, assessments should mimic real-world circumstances while also providing instructional feedback to guide learners toward mastery.

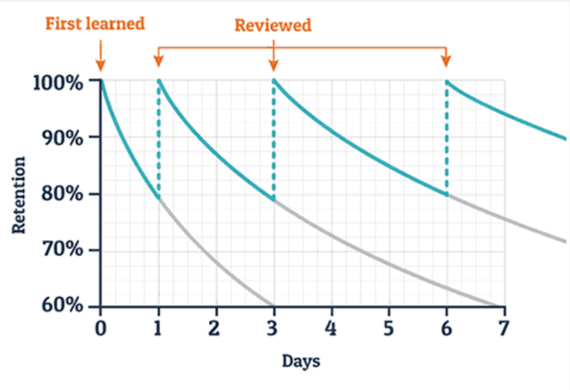
06 It must drive a culture of ongoing learning.

Without reengagement, people quickly forget everything they learn. Hermann Ebbinghaus, a German psychologist, conducted studies on human memory. He discovered that we forget more than 50 percent of what we're taught after just one hour and more than 80 percent after a month if we are never re-engaged on the topic. Ebbinghaus's studies showed that, conversely, if a learner is re-engaged with the topic on a regular and ongoing cadence, not only will the learner retain more information but they also retain that information for longer periods of time.

Basically if you hear something once, you start to forget it almost immediately—and in less than a month you'll almost completely forget it. Not so, however, with microlearning. As the accompanying chart shows, if you revisit the topic on a regular basis, you achieve full retention. Additionally, the more you are re-engaged, the longer you'll retain concepts.

Imagine you took a single piano lesson a year ago. How much of it would you still remember? Now imagine you had a piano lesson every week, ongoing for years. That's the power of microlearning. Its ongoing nature keeps knowledge and information top of mind, so that recalling it becomes second nature when you need to put it to use. This drives a culture of learning.

The Forgetting the Curve of Newly Learned Information



03

Why Microlearning is Ideal for Observing Signs of Danger

If we suspect we are in danger, we become hyper-alert to our surroundings, processing and evaluating each observation to determine if it confirms or relieves us of the danger we perceive.

The process of acting according to the observations we make when we perceive danger is a learned construct. We aren't born knowing a glowing red stove burner is hot and will injure us if touched. We learn this either through the passing of information or from direct experience. This learned construct requires us to recognize warning signs, use them and other contextual observations to decide whether to act, and then rapidly recall what we've previously learned so that we react properly in those circumstances.

We are often able to react quickly as a result of a special part of our memory that makes the information available for easy and immediate recall. We rarely have the luxury to stand around and wonder if something poses an active danger. Rather, our recollection of how certain observations map to danger can become automatic once we observe them. Yet, we also must react selectively: Hearing a snapping twig in the middle of the night when you're camping alone in the deep forest puts us on alert, but the same reaction doesn't apply when you're doing yardwork.

Because microlearning is short, narrowly focused, and has clear practical applications by nature, it is especially effective when instructing learners to be more observant for signs of danger, evaluating additional context to determine if danger exists, and recalling how to react in a dangerous situation. Microlearning equips people to:

- Be more observant of the environment
- Evaluate observations and determine if they are indicators of impending danger
- Quickly make a decision of how to react to indications of danger
- Know which action to take to avoid danger
- Alert those who are in a position to neutralize the danger

Each of these abilities needs to be learned for fast, consistent recall when needed, including how to respond. When danger is involved, people can't dig back through their notes from a training months before—they need clear and concise chunks of knowledge stored top of mind. That's why microlearning, by instructing in small bites for quick recall and a fast response, helps us quickly assess danger.

When considering the types of dangers people are exposed to on a regular basis, we must acknowledge the pervasive threat that cybercriminals impose on employees every day.

How potential impact affects likelihood of behavior change:

↑ Understanding how the acquired information allows self to have impact on others

Understanding impact of the acquired information on self

Understanding impact of the acquired information on others

Acquiring the information

Increasing level of impact

04

Why Microlearning is a Perfect Fit for Security Awareness

/// With 85% of data breaches resulting from social engineering attacks and human error, employees are continuously targeted by cybercriminals. Potential threats and bad actors increasingly show up in your email, call on the phone, and find other methods to get in direct contact.

According to one report, in 2020 phishing was the second-most-common tactic used in attempted breaches, accounting for one-third of all attacks. The success social engineers enjoy in our email inboxes has a lot to do with counting on us to pay little time and attention to their email. While they can't control this directly, our current work environments play directly into their hands. This is because, the more things we observe, the less observant we become. We are simply not equipped to give individual attention to the high levels of activity in today's offices. With employees getting an average of 121 emails a day, your brain isn't exactly on high alert about each specific one as it comes in.

We can become oblivious to what happens in the background—even when it deserves special notice. That phenomenon was perfectly illustrated by a famous experiment in which subjects were told to keep track of people playing basketball in a video. They became so focused on that task that half of the subjects didn't even notice that a person in a gorilla suit was walking by the players. This "inattentional blindness" can lead people to completely miss the unexpected when they're distracted by a task.

Not only do people's working environments often lower their ability to perceive danger or take caution, but the bad guys are talented about hiding their intentions. Phishing lures don't come into your inbox labeled as threats, and hackers don't call you up and identify themselves as cybercriminals. They also don't remind you to check your security training notes from last year, or to think about how you fell hook, line, and sinker for the phishing-simulation email your IT manager sent several months ago. Instead, they do everything they can to make themselves blend into the ordinary, and avoid drawing suspicion.

Threat actors seek to take advantage of lapses in vigilance. They employ social engineering techniques to communicate with employees via false identities in order to gain their trust and trick them into giving up passwords and other credentials needed to access unauthorized information. Phishing attacks, where employees are directed via deceptive emails to access a bogus website designed to look like a trusted, familiar site so unaware visitors give up their passwords, are an even bigger problem. The FBI's Internet Crime Complaint Center received nearly a quarter million complaints about phishing schemes in 2020. And, as it turns out, four out of ten employees with little or no phishing awareness training fail simulated phishing campaign and assessment tests.

These cybercriminals have different ways of observing clues about your work environment in hopes of gaining physical access to your workplace. They may:

- Check your social media accounts like Facebook and Instagram.
- Pay close attention to the background in a video meeting.
- Shoulder-surf at a coffee shop—looking over your shoulders to observe what you're working on.
- Drop thumb drives in your office's parking lot.
- Pose as a visitor and slip into the office to see if there are passwords or other sensitive information lying around for them to collect.

The use of the above and other techniques resulted in

3,932

breaches in 2020, compromising

37

billion records

With employees overwhelmingly targeted, the damage of these exploits continues to grow. It's essential for today's organizations to implement education and training solutions that successfully equip people to more observant for the warning signs of an attack, while also preparing them to know how to react. Building and managing an effective security awareness program isn't easy, especially if your security awareness tools don't utilize the strengths of microlearning to prepare your employees and begin to build a culture of security.

Security awareness tools that engage users too infrequently—or don't provide clear application but instead overload people with too much information all at once and no ongoing reinforcement—will never effectively drive change because learners will be left wondering where to even begin or where they are going wrong.

Instead, a security awareness solution that incorporates a true microlearning strategy as its foundation leverages the brain's own learning techniques and will help build a culture of security where employees recognize threats, know what to do about them, and take action to protect one another and keep their organization safe.

In Aesop's fable of three bulls and a lion, when the three bulls stood tails together, each one looking out in different directions, they effectively guarded and protected each other from attacks from the lion. Likewise, a workforce that builds an inclusive culture of security by effectively educating and enabling its people to remain alert and stand together makes for a powerful defense against attackers.

Managed Security Awareness®

Learn more about Arctic Wolf's Managed Security Awareness® program, which employs state-of-the-art microlearning as part of a unique concierge service that prepares and empowers employees to recognize and neutralize social engineering and phishing attacks.

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Arctic Wolf solutions include Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, Managed Cloud Monitoring and Managed Security Awareness®—each delivered by the industry's original Concierge Security® Team. Highly trained Concierge Security® experts work as an extension of internal teams to provide 24x7 monitoring, detection and response, as well as ongoing risk management to proactively protect organizations while continually strengthening their security posture.

For more information about Arctic Wolf, visit arcticwolf.com

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com