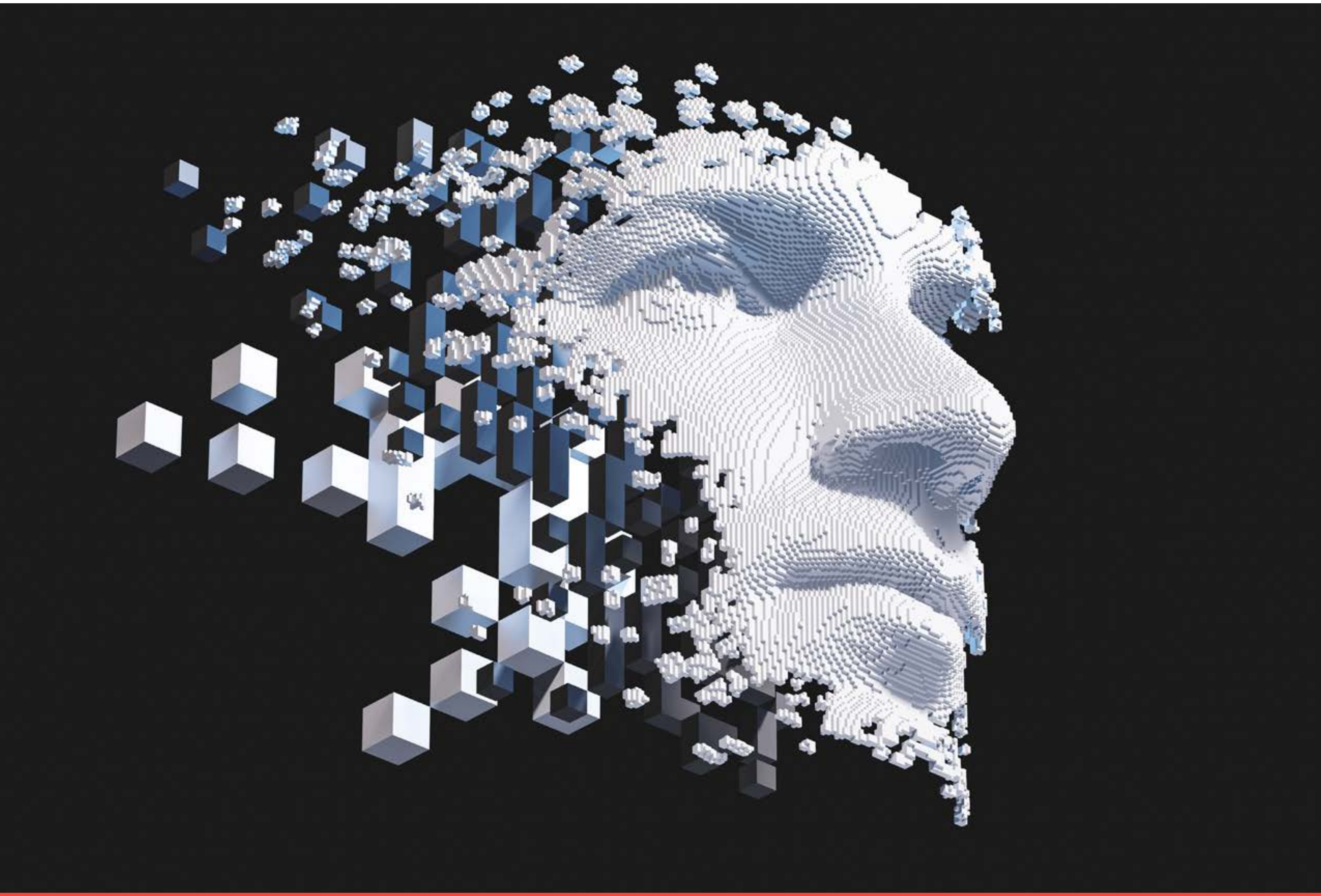
NINJIO

WHITEPAPER



Cybersecurity & Neuroscience

Why memory, habits, and identity play the most important roles in cybercriminal defense.

How many times have you settled an argument by Googling it? How many trips have you taken with that little rectangle on the dash as your guide instead of the tabletop-size piece of paper folded up in the glovebox? Dare we even ask if you know your spouse's or best friend's phone number by heart? At a time when smartphones are in almost every pocket, memory doesn't seem to be as important as it once was.

While it may be true that more information is available and accessible than ever before, **memory has by no means become obsolete.** In fact, the digital tools we use to access information have given us a whole new set of things to remember: passcodes, usernames, and security pins, not to mention what a phishing email looks like or making sure to use a virtual private network (VPN) when we're using public WiFi. As cybercriminals devise increasingly sophisticated ways to exploit our reliance on those tools, it's up to each of us individually to take the necessary steps to ensure we aren't giving hackers an entry point.

From an organizational standpoint, the goal of any effective cybersecurity awareness platform is to help employees get to a point where they no longer have to actively remember what it takes to keep the company safe – instead, they **develop healthy cybersecurity habits.** When you walk out the front door in the morning, do you really have to remember to lock the door? When you leave a restaurant or a coffee shop, do you have to remember to grab your wallet or purse? You don't do these things because you recall that criminals sometimes break into homes and steal unattended personal items – you do them habitually. Cybersecurity awareness should be no different.

As American author Annie Dillard famously said: “How we spend our days is, of course, how we spend our lives.” In other words, habits aren’t just the things we do. Eventually, they become who we are. Consider what you’ve learned about someone if you know they have a habit of holding doors open for people and donating to charity: This is a person who cares about the well-being of others. While it may be less intuitively obvious, our cybersecurity behavior is also inextricably linked to **important elements of our identity.** If you’re someone who clicks on malicious links or readily provides company information to dubious people, it reveals carelessness and gullibility. On the other hand, if you’re scrupulous about your online activity and refuse to give hackers a foothold, you demonstrate that you’re responsible, well-informed, and trustworthy.

These three elements – **memory, habits, and identity** – are the keys to developing a culture of security. Let’s take a closer look at each one.

Teaching and learning cybersecurity

The biggest cybersecurity vulnerability companies face is their employees. This is because hackers often use social engineering techniques that capitalize on employee negligence and ignorance to infiltrate organizations. As the FBI’s 2018 Internet Crime Report demonstrates, the most destructive forms of hacking (such as business email compromise, or BEC) rely on the manipulation of human beings to gain access to sensitive information, wire funds to fraudulent accounts, and defraud companies in various other ways.

Despite the fact that hacks of large companies dominate the headlines, small and medium-sized businesses are also constantly targeted by hackers. According to Verizon's 2019 Data Breach Investigations Report, a substantial proportion of data breaches affect small businesses. And just like large companies, small and medium-sized businesses are struggling to train employees to guard against cyberattacks. A 2018 report from the Ponemon Institute points out that 60 percent of respondents in "companies that had a data breach say the root cause of the data breach was a negligent employee or contractor" – a number that spiked from 54 percent in 2017.

It's clear that negligent employees expose companies to huge amounts of risk, but this should come as no surprise. The Ponemon report found that almost half of organizations say they have "no understanding (of) how to protect against cyberattacks." Considering the fact that so many cyberattacks are caused by employees, effective cybersecurity platforms must be focused around **educating employees and changing their behavior.** But even when companies recognize this fact, it doesn't mean they'll be able to teach employees how to spot and repel cyberattacks. If anything, the frequency and persistence of cyberattacks demonstrates that companies are failing to adequately prepare their employees.

One of the main reasons for this failure is the fact that cybersecurity training is an afterthought for many companies: a check-the-box exercise that most employees immediately forget. For example, if your cybersecurity platform consists of an occasional information dump via email or a tedious PowerPoint presentation every few months, you're ignoring the huge research literature on learning and memory that has seen rapid growth in recent years.

One of the most common methods for learning new material is rereading blocks of text, but the evidence suggests that this doesn't improve information retention. A study published in Frontiers in Psychology points out that "Recent research has found that when individuals view a lecture, mind wandering increases as a function of time." Neither of these facts will come as a shock to anyone who has crammed for a test or sat through an interminable lecture.

We know there are better ways to learn. For example, according to a study in Behavioral and Brain Sciences, "Hundreds of studies in cognitive and educational psychology have demonstrated that spacing out repeated encounters with the material over time produces superior long-term learning." This is a reminder that cybersecurity awareness isn't a box you can check before moving on. Rather, it requires a comprehensive strategy and consistent reinforcement over time. Cyber threats are always evolving, and cybersecurity will never become a core part of your company's culture if you don't continually remind employees that it's a priority.

However, even if you adopt spaced learning techniques and consistently follow up with employees, it won't make a difference if they aren't engaged by the content itself. As a literature review in Current Opinion in Neurobiology explains: "Memory has a limited capacity, and thus attention determines what will be encoded" ("encoding" refers to the creation of memories). This is why long-winded lectures, PowerPoint presentations, and mass emails won't cut it – you have to give employees a reason to keep paying attention.

Finally, it's vital to use all the tools at your disposal to help employees retain what they learn. For example, according to a literature review in Dialogues in Clinical Neuroscience, one of the most effective forms of information retention is "practice testing, where students are intermittently given brief quizzes about what they have learned prior to taking a formal test." Similarly, the aforementioned study in Behavioral and Brain Sciences pointed out that "incorporating tests into spaced practice amplifies the benefits."

If you keep all these components of cybersecurity training in mind – consistency, engagement, and reinforcement – you'll ensure that your employees will actually remember how to keep themselves and the company safe.

Making cybersecurity a habit

Take a moment to consider a few of your daily habits. When you brush your teeth after waking up or look both ways as you back out of the driveway, you're not consciously thinking about why you're making these decisions. They're more like reflexes – ingrained parts of your routine that don't require any unnecessary cognitive energy.

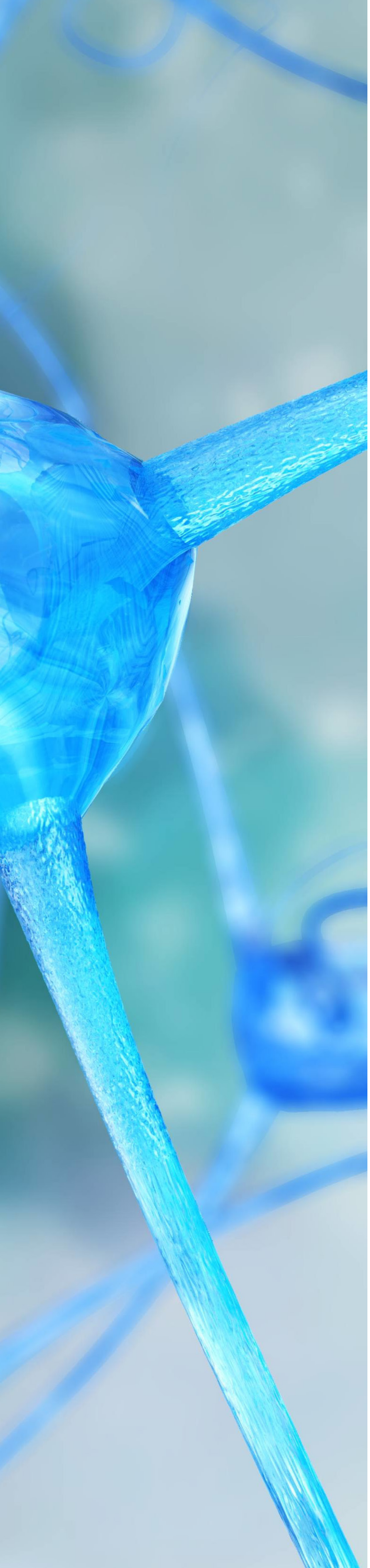
The ability to develop healthy habits is one of our most powerful tools for personal development. This is because habitual behaviors don't require the same amount of cognitive strain as behaviors that are undertaken infrequently or for the first time. As a study in Psychology, Health & Medicine puts it: "Habit formation is an important goal for behavior change interventions because habitual behaviors are elicited automatically and are therefore likely to be maintained." The ultimate goal of a cybersecurity training platform is sustainable behavior change, and habit formation is a crucial part of that process.

As a leader, it's your job to create an environment that will make it as easy as possible for employees to cultivate and maintain the right habits. This means you have to understand why employees behave as they do and develop a set of incentives that will keep them moving in the desired direction. For example, a study in the Journal of Behavioral Medicine found that new gym members were more likely to continue working out if trainers gave them simple and consistent exercises. Similarly, cybersecurity training should never overwhelm employees with dry and technical language – it should be **clear, consistent, and engaging.**

Habit formation requires us to reduce certain forms of friction in our lives. A study in the British Journal of Social Psychology found that "Intentions guided future behavior when habits were weak (low frequency or unstable context), while this was not the case when habits were strong (high frequency and stable context)." In other words, strong habits reduce the need to constantly decide to engage in healthy behaviors – they make those behaviors automatic.

However, habits aren't just about incentivizing good cybersecurity behavior. Companies need to focus on two strategies simultaneously: habit formation and habit disruption. Just as there are many healthy cybersecurity habits that companies want to encourage, there are also plenty of unhealthy habits they want to break. For example, employees often use a single password across multiple accounts, click on suspicious links, fail to update their smartphones and other devices with the latest security software, and put themselves and their companies at risk in countless other ways. These bad habits have to be addressed directly.

A study in the Journal of Public Policy and Marketing explains that "Policy interventions can be oriented not only to the change of established habits but also to the acquisition and maintenance of new behaviors through the formation of new habits." The same study points out that "Successful habit change interventions involve disrupting the environmental factors that automatically cue habit performance." These environmental factors include everything from boring or nonexistent cybersecurity training practices to a company culture that rewards risk-taking instead of prudence.



While some environmental factors have to be disrupted, others should be vigorously promoted. A study published in the European Journal of Social Psychology reports that habits are formed with the "repetition of a behavior in a consistent context." This is why cybersecurity training (when done properly) is indispensable: It weaves security awareness into your employees' everyday lives. When you consistently reinforce the importance of cybersecurity, reward employees for changing their behavior, and help them develop healthy lifelong habits, you'll **create a culture of security at your company.**

Building a security identity

We often think of habits as practical mechanisms to get things done, but they're far more significant than that. In many ways, our very identities are bound up with our habits. Everything from working hard in the gym every day to being punctual is an expression of who you are: diligent, considerate, and so on. This fact is clear to most people, which is why we instantly understand the meaning of expressions like "Actions speak louder than words."

Habits are actions you perform repeatedly, which makes them speak even louder. According to a 2019 study in Frontiers in Psychology, people recognize the inextricable relationship between habits and identity: "Habits may serve to define who we are, in particular when these are considered in the context of self-related goals or central values." And when we consciously recognize the link between positive habits and identity, this can have powerful emotional and psychological benefits: "When habits relate to feelings of identity this comes with stronger cognitive self-integration, higher self-esteem, and a striving toward an ideal self."

None of this is to say that people with unhealthy cybersecurity habits deserve condemnation – far from it. Many people simply haven't had a chance to develop their cybersecurity awareness. The whole world is in the middle of a never-ending digital transformation, and the learning curve isn't just steep – it's always shifting. As we spend more and more time on our devices, hackers are constantly developing new ways to infiltrate them. Even IT and cybersecurity professionals struggle to keep up with the ever-shifting threat landscape, so it would be unreasonable to expect non-technical employees to have excellent cybersecurity habits right out of the gate.

But this doesn't change the fact that, due to the surging number of attack vectors – from a secretary's email account to a product designer's cloud-based productivity tools – every employee is becoming increasingly responsible for cybersecurity. The key isn't to criticize employees for irresponsible behavior, it's to show them how healthy cybersecurity habits reflect the positive aspects of their identities.

The relationship between identity and habit formation has been demonstrated in many different contexts, such as the process of learning to play a musical instrument. According to a study published in the Bulletin of the Council for Research in Music Education, "Children's commitment to learning their instrument and the amount of practice they undertook was useful in predicting their achievement after nine months of learning." Consider the first predictive element mentioned there: children's commitment to learning their instrument. The author of the study, Gary E. McPherson, points out that factors such as the "importance to them (the children) of being good at music" and "whether they thought their learning would be useful to their short and long-term goals" were directly related to how much they improved.

In Daniel Coyle's book The Talent Code, McPherson explains that the ideas students "brought to that first lesson were probably far more important than anything a teacher could've done, or any amount of practice. At some point very early on they had a crystallizing experience that brought the idea to the fore that said, 'I am a musician.' That idea was like a snowball rolling downhill." When being a musician was a core part of a student's identity, the student was more likely to develop habits that reflected that identity.

The implications for companies looking to instill habits in their employees are clear. As the Frontiers in Psychology article explains: “Linking habits to identity may sustain newly formed behaviors and may thus lead to more effective behavior change interventions.” When it comes to cybersecurity, this means making explicit connections between habits – avoiding malicious links, using a VPN, updating security software, downloading safe applications, keeping confidential information away from public channels, etc. – and positive aspects of identity, such as responsibility, accountability, prudence, awareness, and so on.

Most people don’t think twice about physical security: They would never leave their home for an extended period of time without locking the door or exit the office late at night without locking the doors and arming the alarm. If they failed to do these things, they would immediately recognize that it reflects poorly on their values and priorities – fundamental aspects of their identities. While it’s understandable that attitudes toward cybersecurity haven’t kept pace with the rate of digital transformation, this doesn’t mean it isn’t an integral part of your overall security identity.

Our identities aren’t static. While different people have different cognitive and emotional equipment, the formation of new habits can actually change who we are. This is a process that requires education, diligence, and time, but it’s an empowering fact about the way we’re wired. In the world of cybersecurity, there’s no piece of hardware more important than the human brain, which is why the ability to change it is so powerful.