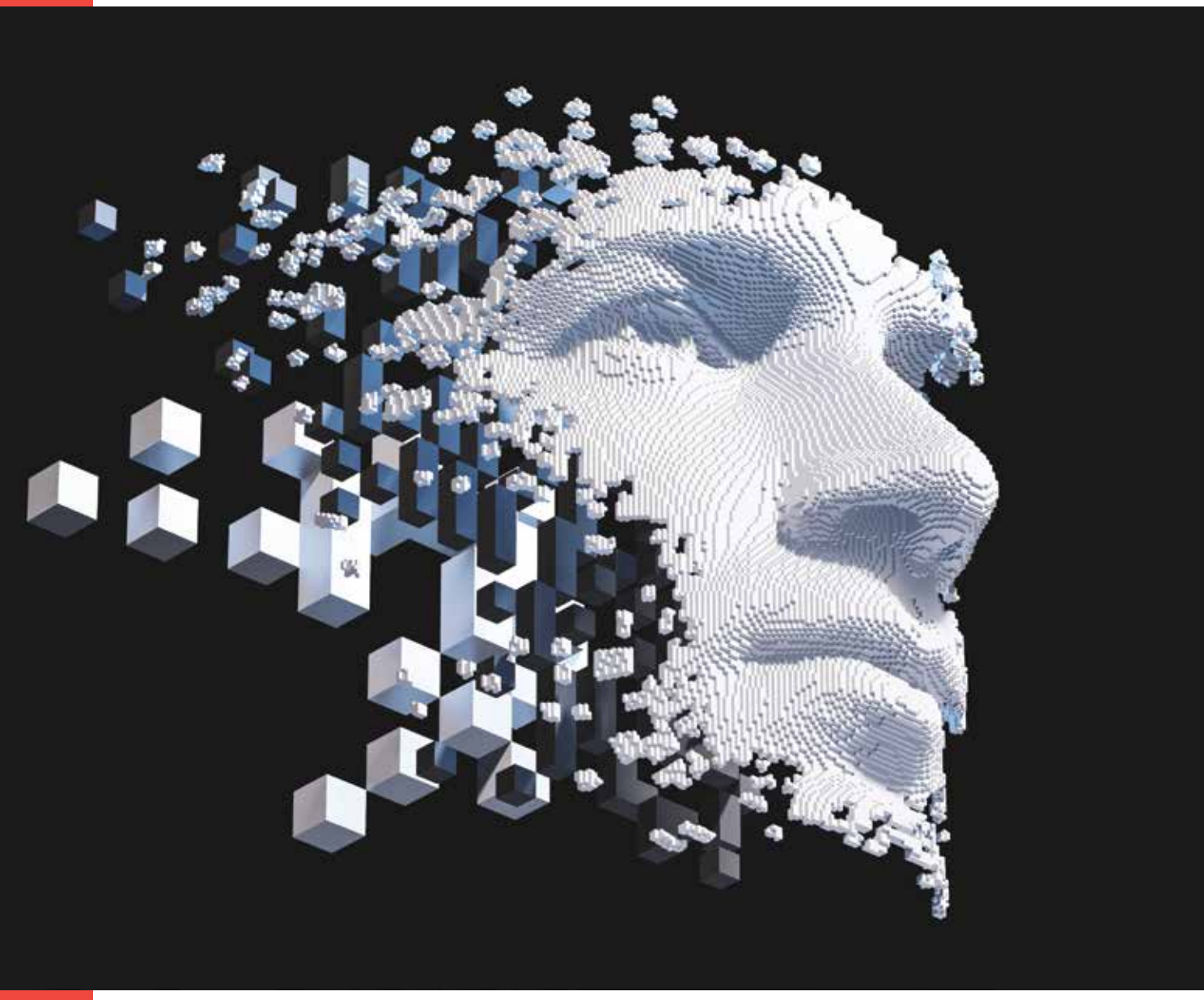
AWARE magazine



CYBERSECURITY & NEUROSCIENCE

Aligning security practices with human nature

Protecting your company in the age of cyberwarfare

Exclusive interview with actor Jon Lovitz

ISSUE 01
February 2020

“Awareness is a key ingredient in success. If you have it, teach it. If you lack it, seek it.”

–Michael Kitson

presented by

NINJIO

AWARE Magazine is published by NINJIO, a leading security awareness education company specializing in Hollywood-style micro-learning videos. NINJIO partners with Fortune 500 companies and small businesses alike to build security aware cultures, helping to make employees and their families less vulnerable to hackers and online cyberthreats.

Letter from the editor

Prior to NINJIO, Zack Schuler started his first company as a solo-preneur based from the trunk of his car. Over the next 15 years, he turned Cal Net Technology Group into a multimillion-dollar business that was acquired by Olympic Valley Capital in 2013.

From the billions upon billions of connected devices that are in use every day to the increasingly sophisticated methods of digital infiltration developed by cybercriminals, hostile foreign governments, and hackers of all kinds, there are many reasons companies are more vulnerable than ever before. We need innovative and effective solutions to counter these threats, which is why we’ve launched AWARE Magazine – the definitive guide to emerging cyber trends and cutting-edge strategies for keeping your company, its employees, and your families safe and aware.

How is the human brain wired to be both an asset and a liability when it comes to cybersecurity? Why should you expect to see an influx of cyberattacks on critical infrastructure in the coming years (or even months), and what can be done to stop them? How can you develop healthy security habits among your employees that will give them a personal stake in protecting your company? You’ll find answers to all these questions and much more—from smartphone security tips to a discussion of possible nation state cyberattacks—within these pages.

With hackers constantly figuring out new ways to cause more damage than ever, companies have to understand the ever-shifting cyberthreat landscape if they want to avoid being victims of one of the countless data breaches that hit companies every day. That’s why the first issue of AWARE Magazine gives you the latest security insights from analysts who are on the front lines of the battle against cybercriminals.

Thank you for reading, and we hope you find the contents useful!

Zack Schuler
Founder and CEO of NINJIO

ISSUE 01
February 2020

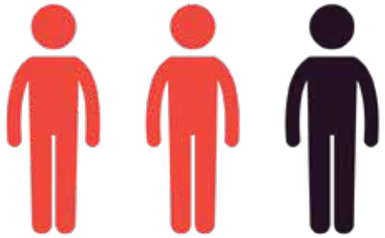
CONTENTS

SECTIONS

QUICK FACTS

DID YOU KNOW?

55% of organizations say that privileged users are their biggest insider threat risk.



Employee or contractor negligence is responsible for two out of three insider threat incidents.

01 BEING HUMAN

How HR plays an important role in creating cultures of security awareness

WHY IT'S TIME TO REVAMP YOUR **EMPLOYEE INCENTIVES**

From exhausting and tedious mandatory training programs to boilerplate benefits packages that make employees feel like numbers instead of human beings, companies are often terrible at providing meaningful and effective incentives. This can lead to less productivity, plummeting morale, and a workplace culture that makes employees dread showing up at the office. Here are a few ways companies can avoid these problems and give their employees compelling reasons to do their best work every day:

01. FOCUS ON EMPLOYEE ENGAGEMENT

According to Gallup, just one-third of American employees say they're engaged at work – a problem that leads to decreased customer loyalty, productivity, and profitability. This is why companies should give employees opportunities to exercise their strengths and develop their skills, provide flexibility and autonomy, maintain open lines of communication, and offer training materials that don't put people to sleep.

02. RETHINK THE BENEFITS STATUS QUO

A 2018 Deloitte survey found that just 21 percent of employers would recommend their benefits program to others. Companies should rethink the incentives they offer, which could include bonuses based on specific targets and projects, opportunities to do more remote work, and programs that allow them to use company resources to work on social issues and charitable causes that matter to them.

03. GIVE YOUR EMPLOYEES A SENSE OF PURPOSE

The day-to-day stresses of work often make it difficult for employees to focus on the big picture: how your company is improving customers' lives. This is why you have to consistently reinforce the idea that your company doesn't just exist to make money – it exists to make the world a better place. Meanwhile, take corporate social responsibility seriously and ask employees how they would like to contribute. Employees shouldn't just feel like they have a job – they should feel like they have a purpose.

The original long-form version of this article appeared in HR Dive, authored by NINJIO CEO & founder, Zack Schuler.

HOW TO ALIGN YOUR **CYBERSECURITY PLATFORM** WITH HUMAN NATURE

by Zack Schuler, founder/CEO @NINJIO

What comes to mind when you think of cybersecurity? Encryption? Firewalls? Antivirus software? While these are all important components of a cybersecurity platform, there's one piece of hardware that doesn't receive the attention it deserves: the human brain.

The companies best equipped to handle the evolving threats from hackers and other cybercriminals are the ones that have established a culture of security. According to a recent Ipsos survey, almost half of C-suite executives at large companies say "human error or accidental loss by an employee/insider caused a breach at their organization." This is a stark reminder that all

the security technology in the world won't protect your company from the vicissitudes of human behavior.

There are many aspects of human behavior that are particularly salient to cybersecurity professionals – from our propensity to take risks to the incentives that motivate us to how we absorb and retain information. The better you understand why your employees think and act the way they do, the more effective your cybersecurity platform will be.

Understanding and differentiating risk

While this may sound surprising coming from the CEO of a security awareness company, not all risk-taking is bad. A tolerance for risk is a powerful engine of innovation – we never would have invented airplanes or walked on the moon if our species was totally risk-averse. But our willingness to assume risk can also be dangerous and unnecessary. If you dump all your savings into a dicey investment, ride a motorcycle without a helmet, or spend all day outside without sunscreen, you're taking inordinate risks for no apparent reason.

The psychology of risk-taking is nuanced and complex – many of the tendencies that are implicated in reckless behavior can also serve a useful purpose if they're channeled properly. For example, a study recently published in the Academy of Management Journal found that rivalry can lead to increased risk-taking. This makes sense, as many other studies have pointed to the link between competition and elevated testosterone, which is a hormone associated with risky behavior. Rivalries are particularly intense forms of competition, so it's no surprise that they make participants feel extra inclined to take risks.

But this doesn't mean companies should always be wary of rivalries with competitors and among employees. As the authors of the Academy of Management study note, "Risk-taking is not inherently good or bad; it depends on the context." A rivalry with another company could inspire employees to take the controlled risk of embarking on an ambitious and demanding project. But the same rivalry could push employees to do something irresponsible in search of an advantage, such as using an unsecured cloud productivity tool.

It's vital to distinguish between the risks that are worth taking and those that aren't, which is what security awareness helps employees do.

Learn how to change behavior

It's impossible to change the culture of a company without the right set of incentives and a thorough understanding of employees' needs, priorities, and attitudes.

To build on the example we looked at in the previous section: competition can be a catalyst for behavioral change. Gamification techniques such as leaderboards and team-based challenges encourage healthy competition between employees – a tactic that has proven successful across many different businesses and contexts. An Accenture report notes that "one company experienced a 230 percent increase in new product sales within 30 days" when it implemented gamification platforms to motivate employees.

No matter what strategies you use to change employee behavior, it's crucial to establish norms of open communication and mutual respect if you want employees to be engaged and responsive. For example, an international survey of almost 20,000 employees conducted by Harvard Business Review found that respect was what employees valued more than anything else from their leaders.

Cybersecurity requires long-term solutions

The most fundamental goal of any security awareness program is to create lasting cultural change. This is why I've always opposed check the box security exercises like cursory emails from the IT department and monotonous security meetings that take place a few times a year.

Two of the most important characteristics of a security-oriented culture are consistency and frequency. The landscape of cybersecurity is constantly changing, so employees always need to be informed about emerging threats and strategies for combating them. Repetition also helps with memory retention – at a time when there are more demands on employees' attention than ever before, they won't make cybersecurity a priority unless the importance of doing so is consistently reinforced.

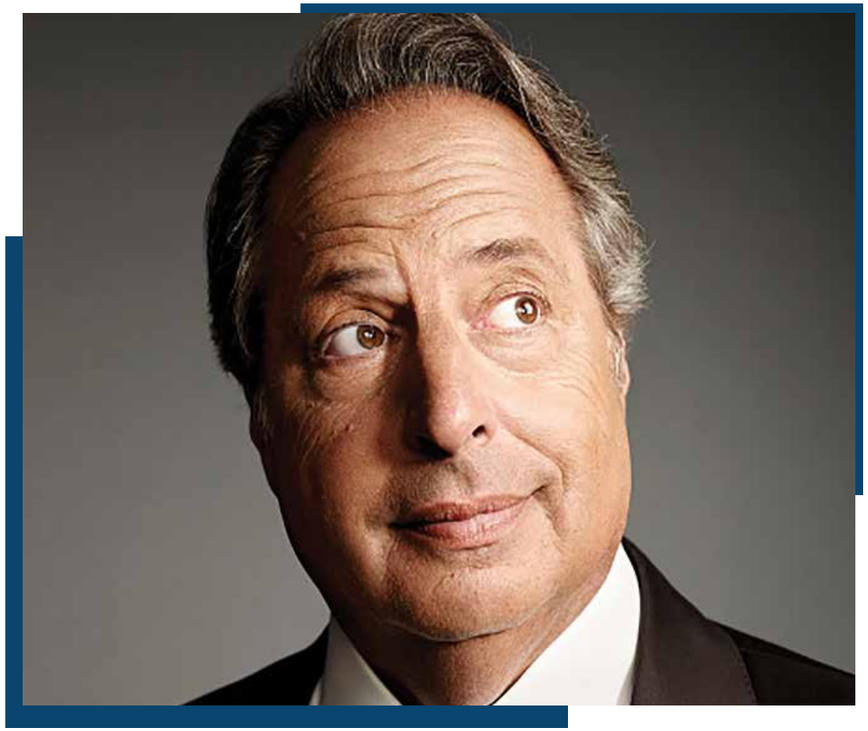
One way to ensure that employees retain the information they learn about cybersecurity is to present it in narrative form (i.e., case studies about major data breaches and what could have been done to prevent them). People have an easier time processing and remembering stories than random, discrete pieces of information because they have emotional value and a cohesive structure. A literature review published in the Proceedings of the National Academy of Sciences observes that "Empirical studies support … a categorical difference between paradigmatic and narrative processing, and suggest that narrative processing is generally more efficient."

Finally, we return to the issue of respect. Your employees should always feel like stakeholders who have an active interest in protecting the company over the long term. If your employees don't feel like valued members of the team, none of your risk management strategies or engagement initiatives will make a bit of difference.

From employee programs that leverage our natural urge to compete to the recognition that each employee craves and deserves respect, your attempts to develop a culture of security should be built around an in-depth understanding of human behavior.

FUNNY YOU SHOULD ASK

WITH THE LEGENDARY JON LOVITZ



Jon Lovitz is a storied American actor, comedian, and singer whose tenure on Saturday Night Live from 1985 to 1990 threw him into the spotlight. What followed over the next three decades ranged from appearing in legendary films like A League of Their Own and Three Amigos to starring as the voice of Jay Sherman in The Critic and acting in countless television series including Seinfeld. Jon has figured out that magic formula for choosing his endeavors wisely and remaining relevant, while not letting fame throw him off his game.

I sat down with Jon, who will regularly appear in NINJIO's Hollywood-style micro-learning content beginning in spring 2020, to ask some questions that have probably been on everyone's mind.

Rebekah Iliff: Dogs or cats?

Jon Lovtiz: I have both, but I'm currently on the road for my comedy tour so I take the dog—Jerry Bruckheimer III—with me.

RI: Which is more detrimental to humankind: Twitter, Instagram, or Snapchat?

JL: I don't think any of them are detrimental necessarily, but I think Insta is a little weird and narcissistic with all the selfies. Taking pictures of yourself just seems silly…and taking pictures of yourself in a mirror: it's like double narcissism.

RI: If you could live your actual life as any character you've ever played, which one would you choose?

JL: That's an interesting question, I've never heard that one before. Well, I did this movie in the late 80s called *My Stepmother Is An Alien*. At the end of the movie I'm given an ambassadorship to join the spaceship as an act of goodwill, and I'm basically surrounded by a bunch of beautiful women that all look like Princess Stephanie. So that could be a good way to live.

RI: What was your favorite animated character to voice?

JL: Definitely Jay Sherman in *The Critic* because they wrote the character for me. The writing was really good, and it was a fun experience. I still do *The Simpsons* too, and always enjoy that.

RI: IYHO, who is actually funnier: Steve Martin or Martin Short?

JL: I know them both pretty well, and I'd say that onstage they are equally funny. But offstage Martin Short is always trying to make everyone laugh, he's kind of always "on." Steve Martin is much more reserved when he's not working.

RI: How do you stay relevant, and how do you decide what projects to take on?

JL: The hardest part of my career is to keep it going. If a project comes my way, and I think it's a good part for me, I'll generally do it. It's not like I just pick and choose whatever I want, it's competitive out there and there's a lot of good talent. To that point, in my mid-forties things really slowed down for me—so I decided to start doing stand-up comedy. I had to somewhat start over, learn a new craft. Stand-up isn't like being a comedic actor.

These days I do a variety of things. I was just on *Saturday Night Live*, which was a blast. Voiceovers are fun. Most of the stuff I've done, I basically never thought I'd do. For example, I'm on this game show called *Funny You Should Ask*. At first I was skeptical, but it turned out to be great once I got in a groove...and the writers figured out which jokes would work for me.

RI: How would you describe your humor?

JL: The funniest thing to me is people who are arrogant idiots, and they think they're smart. But the kicker is: they think they're smart and getting away with all this stuff. These characters are what I'd call "likable idiots"—like my character on *SNL*, "Master Thespian." That's the perfect example of my favorite type of humor.

RI: Have you ever Googled yourself?

JL: Honestly, I Google myself every day. When I first did it, I was really excited. I didn't totally understand how the Internet worked, so it was fascinating. Seeing what's out there kind of keeps you aware of the perception of you. One thing I find interesting [when I Google myself] is that every time a politician lies, they bring up my "Pathological Liar" character from *SNL*. Trump has brought it up three times. It's crazy.

RI: What's the best part of your day?

JL: When I'm not working I like to play tennis.

RI: Ok, now we're going to play a round of "Would you rather." Ready?

JL: I'm ready.

RI: Would you rather be POTUS, FLOTUS, or FDOTUS (First Dog)?

JL: Definitely POTUS. I like making speeches, so I'd be good at that part. The rest of it, maybe not so much. It's actually just more of a figurehead. Good story: I've met George Bush senior a couple of times. One time we were at this charity event that [tennis great] Chris Evert hosts annually in Florida. So I asked him if being president was the hardest job he'd ever had. And he was like: "Not really. All you do is wake up, and at around 9:30 you get handed a sheet of paper, then you just do whatever is on that sheet of paper."

RI: Would you rather have a computer or a smartphone?

JL: Smartphone. Because you can basically do everything on a smartphone that you can do on a computer.

RI: Would you rather lose all your data in a house fire or get hacked?

JL: I'd rather be hacked. If there was a fire I'd lose my house AND my data. This seems like a trick question?

This interview was conducted by business and humor writer, Rebekah Iliff. Her words have appeared in Inc. Magazine, Entrepreneur, Mashable, Forbes, HuffPost Comedy, Weekly Humorist, Slackjaw, Points in Case, Syndrome Mag, and Erma Bombeck blog. Rebekah spearheads NINJIO's content, and she is currently the lead writer for NINJIO HR, which will feature Jon Lovitz.

02 SPECIAL REPORT

News and insights on some of today's most pressing security-related topics

GET READY FOR **MORE CYBERATTACKS** ON CRITICAL INFRASTRUCTURE

by Matt Lindley, chief info security officer @NINJIO

In December 2015, the control systems of three Ukrainian energy companies were infiltrated by Russian hackers – a cyberattack that caused a power outage for more than 225,000 people. According to a 2016 report by the Electricity Sharing and Analysis Center, this hack was the "first publicly acknowledged" cyberattack to result in a power outage, and it was immediately clear that something similar could happen in the United States.

Cyberattacks on critical infrastructure are going to become more and more common. Not only are countries increasingly capable of launching sophisticated cyberattacks, but the surging number of IoT devices is also opening up a vast range of potential attack vectors. What's more, cybercriminals have powerful incentives to attack critical infrastructure and the sector is often ill-equipped to repel these attacks. These factors come together to create a cybersecurity environment that's more threatening than ever for companies and government agencies responsible for protecting critical infrastructure in the United States.

As cyberattacks on critical infrastructure have become more likely, their potential effects have become more devastating. And this isn't just because so many companies and public services would cease to function without reliable electricity, roads, Internet connections, etc. It's because the infrastructure sector itself is so interconnected – from the widespread reliance on a single power grid to the vulnerabilities of global supply chains. It's no surprise that a recent Russian cyberattack on Ukraine quickly spread around the world and caused billions of dollars in damage and lost economic activity.

These are all reasons why infrastructure companies have to develop a comprehensive and integrated cybersecurity platform that covers as many attack vectors as possible and cultivates a security-oriented mindset among all their employees. With so many more methods of infiltration available to hackers – particularly in the infrastructure sector – it's vital for employees across departments and teams to be equipped to identify and prevent cyberattacks. Employee errors constitute one of the biggest threats to companies in the infrastructure sector, but this is a problem that can be solved.

Security awareness training should be provided to all infrastructure employees – not just personnel who have direct access to control systems and networks. As the number of attack vectors continues to increase and systems become more and more interconnected, a single mistake (such as using the wrong software on a company computer) can lead to a massive breach.

Integration is the key to an effective cybersecurity platform – especially for companies that maintain and protect the arteries of the global economy, from roads, bridges, and powerlines to cargo ships and lines of fiber optic cable. As cyberattacks on critical infrastructure become more common and destructive, companies have to use all the resources at their disposal to thwart them if possible and contain them if necessary.

DEFENDING YOUR COMPANY IN THE AGE OF CYBERWARFARE

After President Trump ordered the killing of Qasem Soleimani, the head of Iran's Quds Force (think: a hybrid of the CIA and the special forces), it's no surprise that the situation rapidly escalated. Soleimani was instrumental in Iran's military power projection throughout the region and around the world, and he was one of the most powerful men in the country. Days after Ayatollah Ali Khamenei announced that there would be "severe retaliation" for the strike, Iran launched a barrage of ballistic missiles at U.S. positions in Iraq.

This attack didn't take any American lives, which meant the United States was under less pressure to escalate the situation even more. However, many security analysts are still concerned about the possibility of a different sort of Iranian provocation in the near future: a series of cyberattacks against the U.S. and our allies. Iran might bet that President Trump will pursue a more measured response to an attack of this kind, such as retaliatory cyberattacks. Crippling as cyberwarfare can be, if the conflict can be moved to a realm that avoids more bloodshed, neither side will be as motivated to launch additional physical attacks.

A U.S. Department of Homeland Security bulletin released on January 4 reports that "Iran maintains a robust cyber program and can execute cyberattacks against the United States." Iran has repeatedly demonstrated its ability to launch cyberattacks against targets in the United States and around the world – from major financial institutions to critical infrastructure.

For example, the U.S. Department of Justice indicted seven Iranians in 2016 for a series of coordinated cyberattacks on 46 major American financial institutions, including JPMorgan Chase, Wells Fargo, and American Express. As part of the same string of cyberattacks, an Iranian hacker gained access to a dam in New York. Although the dam was offline when its systems were infiltrated, the attack was a reminder that U.S. infrastructure could be targeted.

Other Iranian cyberattacks have been conducted on a much larger scale. An attack on Saudi Aramco ripped through 30,000 computers, destroying hard drives and replacing their contents with images of burning American flags. The hackers used a form of "wiper" malware that obliterates the memory and files of computers within a target network. While it's likely that the Aramco attack involved someone with privileged access to the company's networks, attacks can also be carried out remotely – by tricking employees into opening a malicious link or attachment, for instance.

According to the Center for Strategic and International Studies, in the past year alone, there have been Iranian attacks on manufacturers and industrial control systems, government officials, universities, and many other targets. Meanwhile, Texas recently reported thousands of attempted Iranian cyberattacks on state agency networks. It's virtually certain that more attacks are on the way – and not just from Iran, as more and more countries, organizations, and criminals are developing increasingly sophisticated forms of cyberwarfare.

So what can companies do to keep themselves safe?

First, make sure all your endpoint protection software, operating systems, and internal applications are up to date. This should be a matter of basic cybersecurity hygiene, but it's often overlooked.

Second, if you're in a sector that's a particularly tempting target for hackers (such as supply chain or infrastructure), stay up to date on the most likely attack vectors and know the exact officials in federal law enforcement you should contact in the event of a breach.

Third, most firewalls have the capability to prevent inbound digital traffic from specific countries in regions such as the Middle East and North Africa. Blocking that traffic could be worth considering in times of crisis, assuming it won't have an inordinate negative impact on business. If you solely do business in the U.S., it would make sense to only allow domestic traffic when there are potential threats from abroad. Many bad actors will use systems based in other countries for their attacks, but identifying countries that could possibly launch an attack and filtering them out is a good step.

But most importantly, ensure that your employees know how to protect themselves and the company by identifying and preventing cyberattacks. The most effective infiltration tactic for state-sponsored hackers (or hackers of any kind) is social engineering, which is particularly effective against an untrained workforce.

When you make cybersecurity training a core focus of your company, you don't just give employees the tools they need to counter cyberattacks – you make sure the all-too-real possibility of those attacks is top of mind. At a time when cyberthreats are all over the headlines, companies have a unique opportunity to open up a discussion about how they can defend themselves – and the country – from those who wish to do us harm.

A special note of thanks to political writer Matthew Johnson, who provided research and insights for this article and worked closely with NINJIO executives to cover this critical topic.

DID YOU KNOW?

80%

80% of hacking-related breaches still involve compromised and weak credentials

29%

29% of all breaches, regardless of attack type, involved the use of stolen credentials

4.1B

Data breaches exposed 4.1 billion records in the first six months of 2019

What can be done?

Make your passwords strong. Emphasize unique passphrases for every account and enable this behavior by providing password managers and training people on them. Even better, have people use multi-factor authentication (MFA) whenever possible.

Reference: 2019 Verizon Data Breach Investigation Report

03 DEEP DIVE

Spotlighting cybersecurity topics that impact today's leading organizations and their employees

CASE STUDY:

LEADING CONSUMER FOOD COMPANY & DEPARTMENT OF HOMELAND SECURITY

BUSINESS TYPE: Consumer Packaged Goods
REGION: Southwest U.S.
ENTITY SIZE: 25,000
ANNUAL REVENUE: $4.5B

Cybersecurity awareness challenge:

According to CyberGRX security analyst Brianna Groves, the top 5 security threats for today's businesses are ransomware, phishing, data leakage, hacking, and insider threats. Furthermore, these threats continue to grow in frequency and scalability, as bad actors create new and innovative ways to penetrate even the most secure systems. Why? Because, generally speaking, the problem isn't with the technology, it's with the people. In fact, according to Verizon's 2018 Data Breach Investigations Report, 93% of data breaches are caused by human error.

Faced with the increasing threat of cyberattacks on large organizations, a leading global consumer packaged foods company decided it was time to adopt a formal security awareness solution. After meeting with NINJIO in the summer of 2016, the organization agreed to sign on for a year. If the employees and staff genuinely engaged with NINJIO's content, and simultaneously gained the knowledge and education to make them viable defenders against potential hackers, the partnership would continue.

"NINJIO offered something we hadn't seen before. As a company, they were nimble and their solution was creative. They listened to our specific concerns and vision for creating a security aware culture," said the director of technology & governance.

The NINJIO solution:

Since 2016, the organization has remained a NINJIO customer, and has seen tremendous results with NINJIO's Aware Anime solution. According to the director, "We understand that the most susceptible part of the organization lies with the human element, and we have made so much progress in educating our employees, ultimately becoming a much more mature company in terms of security."

"This security mindset is possible because 1500 of our associates are committed to watching NINJIO's monthly videos, completing the quizzes, and consuming the supporting content that NINJIO provides. They have subsequently adopted a NINJIO mentality of reporting suspicious activity (emails etc.), and anything else that doesn't look right from a cybersecurity perspective."

"I hear people referencing NINJIO episodes constantly," continues the director. "After an episode is released, co-workers will talk about it with each other. Everyone seems to have a heightened level of awareness and acknowledgement of potential threats."

But the real test came when the organization partnered with CISA and the Department of Homeland Security (DHS) to run a simulated phishing attack on 600 of their 1500 associates who use computers for their daily workflow.

Results:

As a global leader in consumer packaged goods, the organization's importance to food supply does not go unnoticed. As such, the organization was classified as a "critical infrastructure" organization making it eligible for free programs provided through DHS with respect to cybersecurity. This includes internal and external penetration testing, network security audits, and other solutions designed to ensure that their network, and their people, are secure.

As part of this program, a simulated phishing attack—purportedly originating from the IT department and designed collaboratively by DHS officials and the organization—was launched to a randomly selected 600 employees as potential targets. It was an extensively thought out and well-crafted phishing attack, and both the organization and the DHS were shocked that only 1 of 600 employees (or .17%) took the bait.

"We were floored by the results, and so was CISA and the Department of Homeland Security. The fact that only 1 in 600 took the bait was extraordinary. After that, I think we all rest easier knowing our employees have a true security mindset—all of this based on actual results. Thanks to NINJIO for reinforcing our security-first culture through current and relevant topics."

ONLY 1 OF 600 EMPLOYEES (OR .17%) TOOK THE BAIT.

KEY TAKEAWAYS:

- In three years, NINJIO shifted the organization to a security aware culture.
- Employees engaged with the NINJIO content, creating a cybersecurity identity.
- When faced with a simulated phishing attack, only .17% of employees took the bait.
- According to the KnowBe4 2018 Phishing By Industry Benchmarking Report, after 12 months of computer-based training, the average 1000+ company click rate was 3.04%. In this case, NINJIO beat that by 17x.

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: from passcodes and usernames to the importance of using a virtual private network (VPN) when we're on public WiFi. As cybercriminals devise increasingly sophisticated ways to exploit our reliance on digital tools, we have to ensure we aren't giving hackers an entry point.

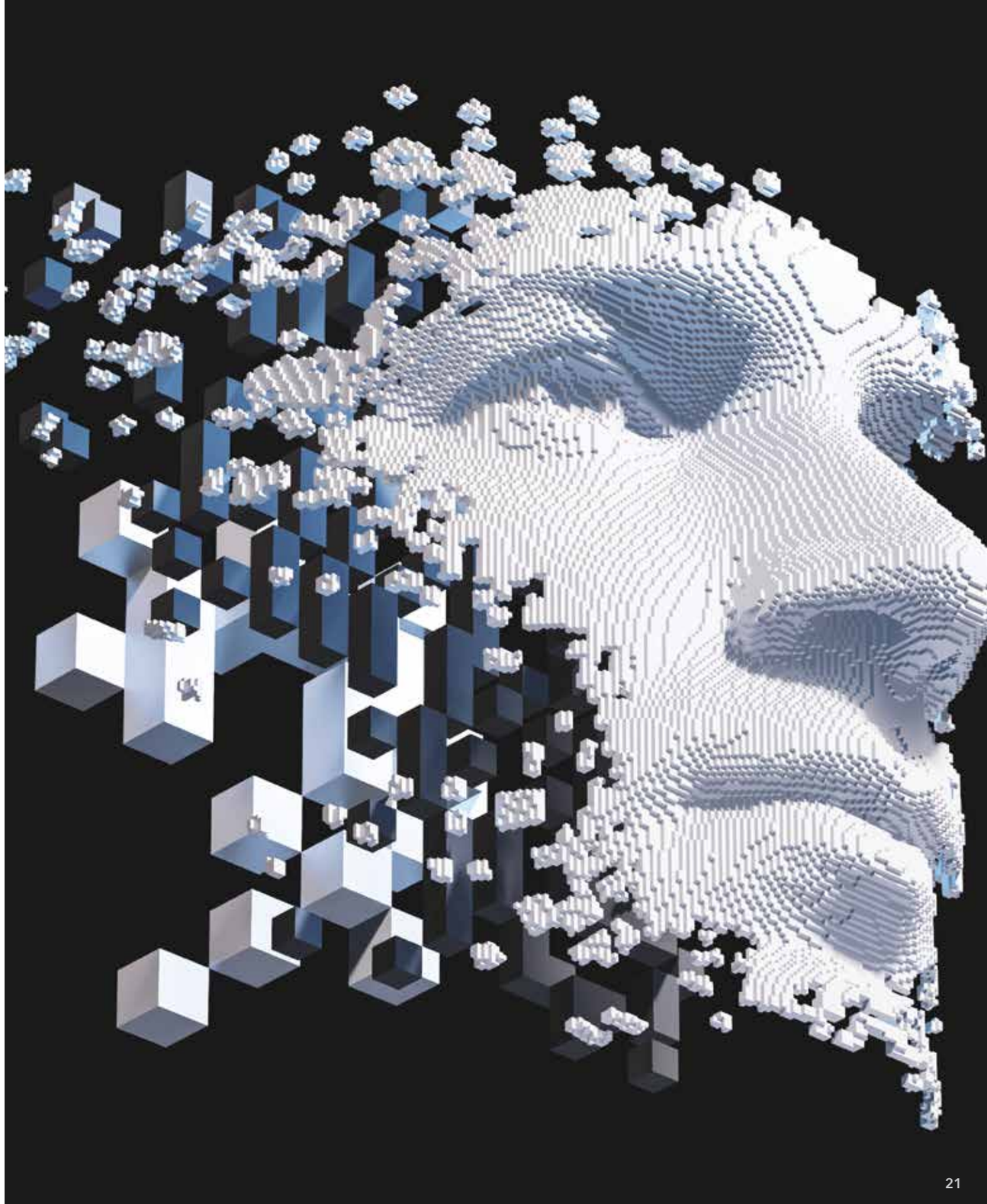
From an organizational standpoint, the goal of any effective cybersecurity awareness platform is to help employees get to a point where they no longer have to actively remember what it takes to keep the company safe—instead, they develop healthy cybersecurity habits. When you walk out the front door in the morning, do you really have to remember to lock the door? You don't do this because you consciously recall that criminals sometimes break into homes—you do it habitually. Cybersecurity awareness should be no different.

Habits aren't just the things we do—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.



It should come as no surprise that negligent employees expose companies to huge amounts of risk. A Ponemon report of cyberattacks on small and medium-sized businesses found that almost half of organizations say they have "no understanding (of) how to protect against cyberattacks." This is why effective cybersecurity platforms must be focused around educating employees and changing their behavior – 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 too often an afterthought: 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 requires a comprehensive strategy and consistent reinforcement over time. Cyberthreats 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. 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.

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.

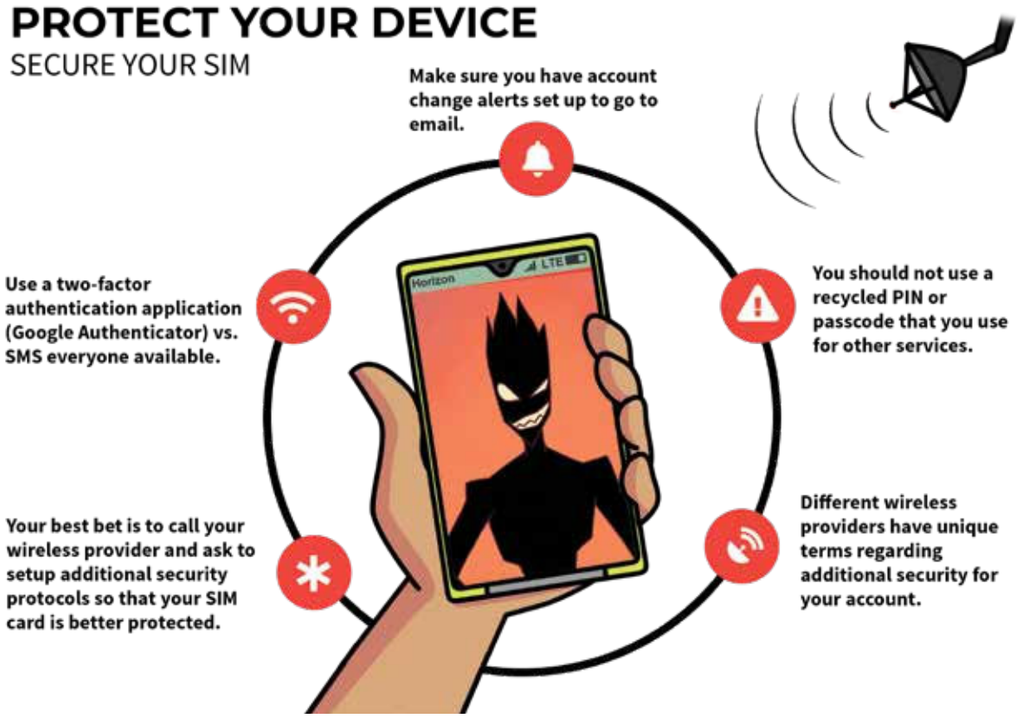
The relationship between identity and habit formation has been demonstrated in many different contexts, such as the process of learning to play a musical instrument. In Daniel Coyle's book The Talent Code, Gary E. McPherson (who has conducted research on music education), explains that students' self-conceptions "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, 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 a child at home 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.

SMART TIPS



04 SECURITY INSIDER

Security tips, tricks, and cautionary tales from the frontlines

KEEP YOUR COMPANY SAFE WITH 3 SMARTPHONE SECURITY TIPS

by Doug Kerzner, director of sales @NINJIO

How many smartphone apps do you actually use? How many do you have? And how many did you download on a whim—because of course you needed that toilet paper racing game and the app that tells you where you parked your car in a pirate voice – only to never use again?

While app hoarding may seem like a relatively innocuous habit, clogging your smartphone with unnecessary apps can actually create serious security risks. There are millions of apps out there, and many of them are no longer maintained – which means they don't receive the security patches that keep your device safe from hackers. Any security gaps that exist on these defunct apps will never be addressed, giving hackers opportunity after opportunity to infiltrate them and exploit their users. This is why it's vital to frequently go through your phone and remove any apps you no longer use.

Stockpiling pointless, outdated apps is just one of the security mistakes smartphone owners routinely make. Here are three more app security measures that every smartphone user should know about:

01

Never download an app from anywhere other than legitimate stores (such as Google Play or the Apple App Store). When users download and install apps that don't come from established sources, it's called "sideloading." While it's true that some users sideload third-party apps without incident, doing so opens them up to a whole lot of risk. For example, the files that install the apps can contain malware capable of stealing data and infiltrating users' smartphones in other ways. It may be tempting to get a free app or one that supposedly has more features, but it isn't worth the risk.

02

Ensure that all of your apps are automatically updated. Software updates don't just offer improved functionality and new features—they provide important security patches. The typical smartphone owner uses dozens of apps (or more), so it just isn't feasible to manually install updates. And with the auto-update feature available, there's no reason to be vulnerable a second longer than you have to be.

03

Use a VPN (virtual private network). A VPN establishes a secure connection to another network (even if it's thousands of miles away), which provides resources that aren't available on your local network and shields your data from cybercriminals. The tunnel from your smartphone to the VPN blocks bad actors from accessing your information, which is why VPNs are so crucial if you're using public WiFi. VPNs can also help you circumvent local restrictions (if you're in a country that censors Internet activity, for instance), provide greater anonymity, and access remote resources such as your company's servers.

According to Pew Research Center, just 39 percent of American adults owned smartphones in 2012—a number that surged to 81 percent by early 2019. Meanwhile, a 2018 report by the Ponemon Institute found that 64 percent of organizations "say they are either very concerned or concerned that they will be hacked through an application." This makes sense: as more and more people use smartphones, hackers are incentivized to develop new ways to attack them. But by following the simple guidelines above, you can drastically reduce the chance that you'll be a victim of one of these attacks.

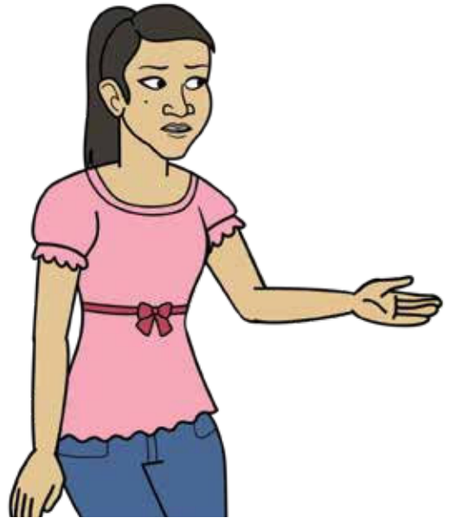
SMART TIPS

3 BEST WAYS
TO STAY SAFE ON SOCIAL MEDIA

1 **Don't accept** friend request from someone you don't know.

2 **Never click** a link from an unverified source.

3 **Double check** the URL to make sure the website is legit.



DID YOU KNOW?

Nearly **two-thirds of U.S. adults** with social media accounts say they have been hacked.

Americans open **a third of phishing emails** they receive.

CAUTIONARY TALE:

HOW ONE SMALL BUSINESS NEARLY WENT UNDER BECAUSE OF A **SPEARPHISHING ATTACK**

When most people think of cyberattacks, major data breaches at huge companies like Equifax and Yahoo typically come to mind. This is perfectly understandable, as these are the attacks that affect the most people at once and always make the headlines. But cybercriminals don't limit their attacks to the largest companies—they also target countless small businesses every year. And in many cases, these attacks destroy businesses and livelihoods.

There's no reason to put it delicately: The state of cybersecurity in the world of small and medium-sized businesses (SMBs) is nothing short of alarming. Not only are SMBs relentlessly targeted by hackers—they're also woefully unprepared to defend themselves and unequipped to handle the aftermath. This is a status quo that has to change immediately because SMBs are the biggest engine of the U.S. economy, and they're at risk like never before.

But don't take our word for it…

We interviewed Carson, a small business owner whose company nearly went under after a spearphishing attack. He agreed to speak with us in hopes that he will prevent others from suffering a similar fate.

NINJIO: Tell us about your company.

Carson: We are essentially a furniture manufacturing partner that supplies custom furniture to five-star hotels around the world via hotel designers and purchasers. We don't own the factories per se, but we use several different factories to fill the orders (like wood, metal, stonetops, glass, etc.) for our customers. We have four employees based in California, five overseas, and ten sales people spread across various regions.

NINJIO: How were you attacked?

Carson: While we work with three or four factories at any given time, one main factory does the bulk of the manufacturing. We are very close with the owner and email him every day because of all the various projects. Cassie is the factory's accountant, and she regularly corresponds with our controller, Julie.

We were in the middle of a big project with a New York hotel and we needed to wire several payments to the factory. Cassie was emailing Julie about the invoices and was being rather pushy about the payments. She had also (unbeknownst to me) given Julie a new bank account number for the wire transfer. Another one of our employees, Hunter, is someone who regularly interacts with our clients, so I asked him to please relay to the client (Cassie) that she needed to back off a little—that we would make the payment soon. Hunter suspected something weird was going on, and emailed me saying "I think there may be a problem and that Cassie may not actually be Cassie."

NINJIO: How did you finally figure out that you'd been hacked?

Carson: After Hunter alerted me about the potential fraud, I told Julie to hold off on wiring any money. But I was about three hours too late. My bank was located on the East Coast, so by the time we'd verified that the real Cassie had NOT asked Julie to wire money to a new bank account, the damage was already done. Nearly a quarter of a million dollars vanished.

NINJIO: How did this ultimately affect your business?

Carson: That money lost wasn't enough to completely put us under, but I still owed the money to my factory partner. I gave them my word I would pay them back—but needed time to do so. Fortunately they agreed, but it had residual effects that bled into other areas of the business. It set us back for months, and I ended up relocating the company to North Carolina.

NINJIO: In retrospect, what would you do differently?

Carson: My controller was vulnerable and she lacked security awareness education. While some of her mistakes were errors in judgment, the major mistake could have been avoided with proper knowledge. Word to the wise: the email address the real Cassie used was long and complicated. (e.g. CTF19319184@bhfactory.com, for example). The fake Cassie's email was the exact same other than ONE character. So these things are easy to miss, which is why it takes education about various aspects of these attacks. Alarm bells should have been going off when Cassie was acting out of character and asking to wire the money to a new bank out of the blue.

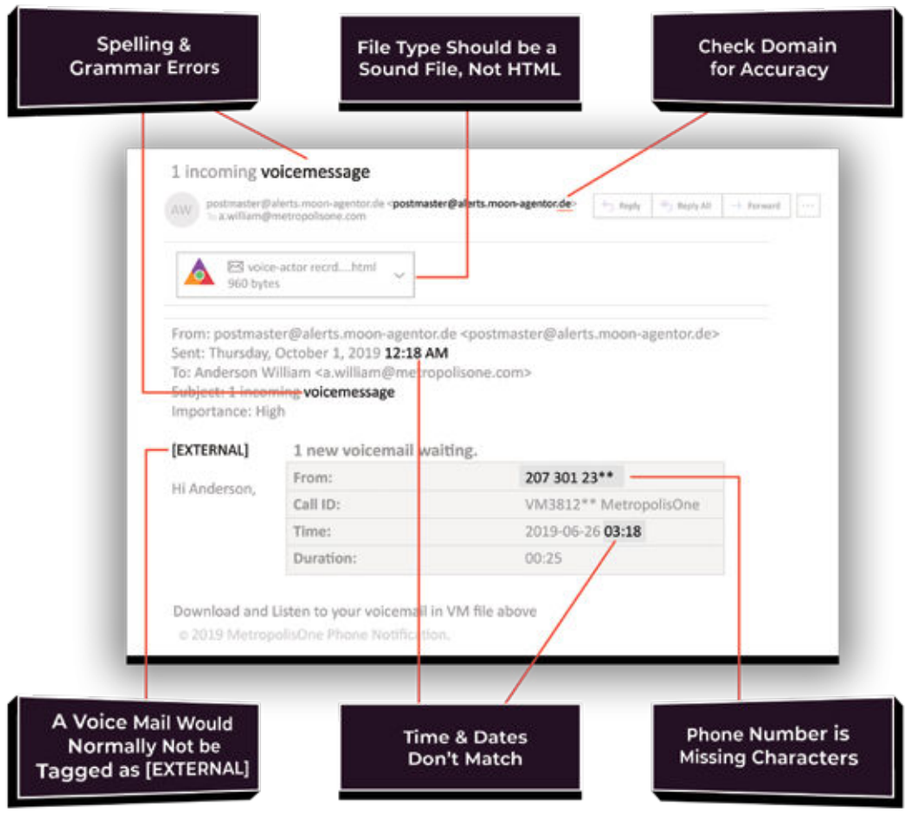
Ultimately, I wish I would have had better checks and balances. I should have trained my controller to ask more questions, especially if bank account information was involved.

Are you a small business? NINJIO SMB has an affordable, subscription-based solution for companies with up to 100 employees. Check out https://ninjio.com/smb/ for details.

DID YOU KNOW?

- Every year, cyberattacks cost small businesses an average of almost $80,000, and losses can range up to $1 million.
- 88 percent of small business owners "felt their business was vulnerable to a cyberattack."
- Almost two-thirds of small businesses "fail to act following a cyber security incident."
- The top three attack vectors cited by SMBs are mobile devices, laptops, and cloud systems.

CHARACTARISTICS OF A **SPEARPHISHING ATTACK**



WE'D LIKE TO THANK

OUR PARTNERS

Our mission is to make the world a more secure place.

To further this mission, we created channel programs for different types of organizations to refer or resell our NINJIO solutions. Whether you are a managed service provider, an end-point protection company, a security awareness firm looking to beef up your content library, or a technology distributor, we would welcome the opportunity to discuss a partnership.

"Repetition is the mother of learning, the father of action, which makes it the architect of accomplishment."

-Zig Ziglar