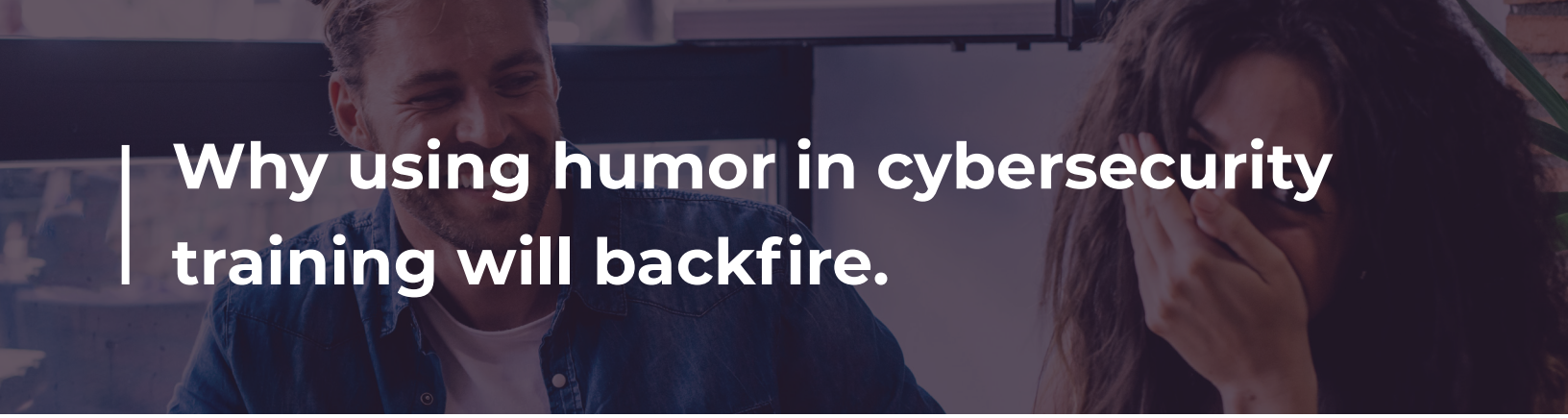

NINJIO
2021
COMEDY
REPORT
WHY CYBERSECURITY TRAINING
IS NO LAUGHING MATTER
ZACK SCHULER
FOUNDER AND CEO OF NINJIO

ABSTRACT

As social engineering attacks continue to inflict millions of dollars in damage every year, cybersecurity training will remain the most essential resource companies have to protect themselves from cybercriminals. But the type of training companies deploy matters – they should always emphasize the fact that cybersecurity is one of the most serious issues they face, which means providing educational content that informs employees of how destructive cyberattacks can be. The last thing companies should do is trivialize cybersecurity with attempts to be funny.



Why using humor in cybersecurity training will backfire.

Think about the last time you heard a joke that didn't land – it's difficult to imagine anything more awkward for the person who told it and the audience alike. In professional settings, however, awkwardness alone can be a trivial concern when humor goes awry. Jokes can make light of serious issues, offend and alienate colleagues, and make workplaces less inclusive for people with different backgrounds and experiences.

Employees already underestimate the severity of cyberthreats.

The tension between humor and healthy, productive, and safe workplace cultures isn't just limited to interactions between employees – it's even more pronounced in the development and distribution of training content. If employees are encouraged to joke around about grave issues – from harassment to discrimination to security threats – they won't appreciate just how consequential those issues can be. Nor will they be fully engaged with the training materials, which will limit their ability to recall what they learn and put it into practice.

These problems are especially prevalent when it comes to cybersecurity awareness training, as many employees already underestimate the severity of cyberthreats and need compelling and consistent reminders of just how devastating a major data breach or other cyberattack can be. Instead of making cybersecurity out to be a laughing matter as many training platforms have done, your company should approach it with the seriousness it deserves.

USING HUMOR WHERE IT DOESN'T BELONG

It's possible to think of training that could deploy humor without compromising the core message a company is trying to convey – with trivial issues like parking or how to use the time clock, for instance. But there are many issues that should never be trivialized, and considering the destructive consequences wrought by cyberattacks day after day, cybersecurity is one of them.

According to a 2020 IBM study, the average cost of a data breach in the United States is $8.64 million and it typically takes companies 280 days to identify and contain a breach. Meanwhile, the FBI reports that cyberattacks of all types are on the rise, both in terms of the overall number of complaints and the financial losses to victims. But as disturbing as these statistics are, they don't capture the true cost of cybercrime: businesses ruined, identities stolen, fraudulent information about healthcare sent to vulnerable populations like seniors (a problem that has been especially pervasive amid COVID-19), and millions of lives disrupted.

Any effective cybersecurity awareness platform has to emphasize these real-world consequences, which demonstrate to employees the gravity of what they're learning. That's why emotionally affecting stories of lives torn asunder and businesses irreparably damaged will always have a more profound impact on employee behavior than goofy skits or other attempts at humor where it does more harm than good.

HUMOR CAN BE AN IMPEDIMENT TO DIVERSITY AND INCLUSION

As the American workforce becomes increasingly diverse and an ever-growing share of employees (especially from younger generations) say they value inclusive workplaces, it's vital for companies to recognize that people with different backgrounds and experiences have perspectives that don't align with their colleagues. This recognition is particularly important when companies are teaching employees about a serious issue like cybersecurity, as it should inform the techniques they use to do so.

There's no telling who will get the joke and who won't.

When humor works on a broad scale, it's because the audience shares certain assumptions, social and cultural experiences, and other characteristics that can make a joke universally intelligible and funny. Different cultures interpret humor in divergent ways – what's funny to members of one community might be incomprehensible or offensive to members of another. A study published in the North American Journal of Psychology even found differences between British, Australian, and American respondents in how they use and perceive humor – cultures that have far more in common than many others around the world.

Effective cybersecurity awareness platforms need to bring employees together around the common goal of protecting themselves and the company, which means security awareness content should always appeal to all employees – not just the ones who happen to come from a certain culture. This is why companies should always be wary of humor in cybersecurity training – there's no telling who will get the joke and who won't.

A BETTER WAY TO HELP EMPLOYEES BECOME CYBER AWARE

Education has always been at the center of any successful cybersecurity awareness platform because cybercriminals rely on the deception, manipulation, and exploitation of employees to infiltrate companies. Since the beginning of the COVID-19 pandemic, almost two-thirds of companies have seen a spike in social engineering attacks – a trend that's only going to continue as remote work remains the norm and cybersecurity protocols struggle to keep up.

Two-thirds of companies have seen a spike in social engineering attacks

Companies are consistently increasing their cybersecurity budgets, but investments alone aren't enough – companies need to implement cybersecurity policies that actually work, and training is at the top of that list. However, the type of training matters – companies shouldn't be flippant about cybersecurity, as it's an issue that can cost them millions of dollars, sever relationships with customers, and put employees and their families at risk. What's worse, humor can undermine the solidarity needed to galvanize employees around the importance of preventing cyberattacks and keeping the company safe.

SO HOW DO COMPANIES MOVE FORWARD?

Instead of attempting to make employees laugh about cybersecurity, companies should provide engaging and informative content with stories about real cyberattacks (and their victims) pulled straight from the headlines. This won't just demonstrate the immense human cost of cyberattacks to employees – it will also show them exactly how they can avoid becoming victims themselves. Any effort to impart these tough realities in a frivolous way is bound to give employees a warped idea of what they're up against, which will ensure that they aren't equipped to fight back.

NINJIO

805.864.1999 | info@ninjio.com | www.ninjio.com