BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

It's Time For a Refresh!

4 Cybersecurity Trainings To Do With All Employees

Students are returning to the classroom now that back-to-school season is officially underway. During the first few weeks, teachers will be reteaching their students the topics they learned in the previous school year to help them regain knowledge they may have forgotten during summer break. But students aren't the only ones in need of a refresher every year. Your employees also need to be refreshed on company policies, values and, most importantly, cyber security practices.

Did you know that human error accounts for 95% of all successful cyber-attacks? When a cybercriminal is planning an attack, they look for weak points within a company's cyber security plan. The easiest spot for hackers to exploit is a company's employees. New cyberthreats are created on a consistent basis, and it's important that your employees know what to do when they encounter a potential threat. If your employees are not routinely participating in cyber security trainings, your business could be at risk, regardless of size.

Every single one of your employees should be familiar with your cyber security practices. When they're hired on, they should go through an initial training that lays out all of your practices, and they should also participate in refresher trainings throughout the year to ensure that the entire team is on the same page with cyber security. At the very least, you should host at least one security training annually. If you've never put together a cyber security training, you may be wondering what topics you need to cover with your team. Below, you will find four of the most important topics to cover.

Responsibility For Company Data

This is your opportunity to explain to your employees why cyber security is so important. They need to

understand why cybercriminals are interested in your company's data and what they could potentially do with it. Everyone on your team has a legal and regulatory obligation to protect the privacy of your company's information. When discussing this topic with your team, it's imperative that they know the ramifications of falling victim to a cyber security threat.

Internet Usage

Does your company have restrictions on what websites your employees can use while at work? If not, that's something you should look into. Every device that's used by your employees should have safe browsing software downloaded onto it to prevent them from stumbling upon dangerous sites that could put your company's data at risk. Your employees should know what sites are acceptable to use and that they should not be accessing their personal accounts while connected to your company's

Continue on the next page...

Continued from previous page...

network. They should never click on links that are sent from an anonymous source or are found on an unapproved website.

E-mail

If your employees utilize e-mail while at work, it's important that they know which e-mails are safe to open. Employees should not respond to e-mails that are from people they aren't familiar with, as that could be a cybercriminal attempting to gain access to your company's data. Employees should only accept and open e-mails that they are expecting or that come from a familiar e-mail address.

Protecting Their Computers

If your employees have their own personal computers, they should be doing everything in their power to keep them protected. Whenever they walk away from their computer, they should make sure it's locked; they should also never leave their computer in an unsecure location. Also, ensure that your employees are backing up their data routinely and have downloaded necessary antivirus software.

It's of the utmost importance that your team has been fully trained in your cyber security practices. If they haven't, they could open your business up to all sorts of cyber-attacks that will damage your company's reputation from a customer perspective. Your business will also no longer be compliant, and insurance companies may not cover your claims if your team is not participating in regular training.

"Human error accounts for 95% of all successful cyber-attacks."

Ensuring that your team is aware of your cyber security practices and actively taking steps to strengthen your cyber security is the best way to stay compliant and prevent cyber-attacks. If your team is not regularly going through cyber security training, you need to start. It will offer more protection to your business, which will make your customers more comfortable doing business with your company.

Business Tidbit

These Marketing Trends Didn't Go Out of Style

When people think about trends, they often imagine what's in style at that current moment. We like to imagine that trends come and go, but the opposite is sometimes true. In fact, the greatest trends become a part of our culture. At one time, people thought cellphones, texting and computers were just a phase, but decades later, they're still here because they made our lives better! Trends in marketing are the same. Sometimes a fresh marketing strategy will pop up, but if it works, it will become a mainstay.

As you continue to plan your marketing strategy for the next few months and the upcoming year, you can look at previous statistics to ensure your methods are successful. Below, you will find three marketing strategies that have proven successful in the past. If these strategies are properly utilized by your company in today's climate, you will quickly see results.

Using Influencers

People love to use their smartphones and social media. During the pandemic, many businesses started to advertise on Instagram and TikTok *(BSSi2 highly recommends NEVER using TikTok as it is a security risk)* through the use of social media influencers. A TopRank Marketing survey found most B2B marketers believe this strategy changes minds, improves the brand experience and yields better campaign results.

Advertising On Podcasts

There are podcasts available that discuss every topic imaginable, and over 30% of Americans listen to a podcast on a monthly basis. That percentage rises when you look at younger demographics. Advertising on podcasts is a great way to reach a younger audience.

Leveraging AI

The importance of artificial intelligence (AI) for B2B marketing became crystal clear recently, when a Salesforce study reported that 80% of business buyers expect the companies they reach out to will talk to them "in real time," regardless of the hour. This statistic highlights how important chatbots and other AI solutions are for customer conversion.

If you've seen success with certain marketing trends in the past, you don't have to get rid of them when you develop a new marketing strategy.

All it Takes is "Free" Beer to Steal Your Personal Data *From KnowBe4, Inc.*

A recent phishing scam impersonating the Heineken beer brand demonstrates how very little effort is needed by scammers to convince victims to give up all kinds of personal information.

If you're someone that likes beer, seeing a giveaway from a beer vendor seems plausible. Perhaps some hats, a coupon, a beer koozie, etc. all would be reasonable "prizes" in said giveaway. But scammers intent on collecting the personal information of victims went all out impersonating Heineken and promoting the giveaway of 5,000 coolers filled with their beer for Father's Day last month.

As part of the scam, personal details were collected including birthdate, email, address, name and more. This kind of information could be used to attempt takeovers of legitimate email addresses, used as part of a longer-term doxing effort, or simply be used to impersonate the victim in another scam.

In a statement put out by Heineken, the free beer scam was denounced, with Heineken recommending that individuals not engage with such communications. But the scam does make a point: as part of creating the illusion of legitimacy, the scammers used a well-known worldwide brand and placed the scam's hook (the 5,000 coolers) just on the cusp of being implausible.

This is what creates a sense of urgency and causes potential victims to forget the need to remain vigilant when interacting with email and web content that is unsolicited – something taught to employees via security awareness training in organizations that are serious about reducing the organization's threat surface – something that includes the user.

On the Lighter Side

Only using a password to log in

Using two-factor authentication

September 2022

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"I just feel fortunate to live in a world with so much disinformation at my fingertips."

CartoonStock.com

Shiny New Gadget of the Month

Logitech Litra Glow

Video calls have become a part of our daily routine regardless of whether you work remotely, in the office or a combination of the two. If you'll be on camera every day, don't you want to look your best? That's exactly how you'll look with the Logitech Litra Glow light. The Litra Glow uses innovative geometry and is frameless to provide more light to the areas within your camera's view. It uses soft and diffused light that's easy on your eyes in case you have to be on the call for an extended period of time. Whether you're on video calls, shooting marketing videos or doing anything else webcam-related, the Litra Glow provides you with perfect light for any situation.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc