TECHNOLOGY BYTES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER , EASIER & BE MORE PROFITABLY

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! A true professional IT support team you can count on, available 24/7."

Bhavin Mehta, Fusion Factor Corporation
Contact us:- 760(940)4200

Exclusive For CEOs

3 Ways You Are Unknowingly Rolling Out The Red Carpet For Identity Thieves

What's Inside

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, cybersecurity 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 cybersecurity 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 cybersecurity trainings, your business could be at risk, regardless of size.

Every single one of your employees should be familiar with your cybersecurity 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 cybersecurity. At the very least, you should host at least one security training annually. If you've never put together a cybersecurity 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 cybersecurity 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 cybersecurity threat.

Internet Usage
Does your company have restrictions on what websites your employees can use while at work? If not, that's something

---

Effective IT for Business
FUSIONFactor

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 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.

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

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 cybersecurity 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.

Ensuring that your team is aware of your cybersecurity practices and actively taking steps to strengthen your cybersecurity is the best way to stay compliant and prevent cyber-attacks. If your team is not regularly going through cybersecurity 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.

3 Ways You Are Unknowingly Rolling Out The Red Carpet For Identity Thieves

Warning! Even if you have anti-virus, spyware protection, and a firewall, you could still be an easy target for identity thieves, hackers and cyber criminals. Read on to find out how YOU are giving online criminals free access to your personal and financial information…

You've done all the right things. You've installed a good firewall, you keep your antivirus up to date, and you're making sure you keep up with the latest security patches…so your computer network should be safe from identity thieves, right?

Wrong !

According to a recent study, 37% of electronic identity theft cases had one thing in common: they were caused by an action taken by the user. That's right, more than a third of identity thefts were not thefts, but giveaways!

So How Do You Avoid This Happening To You And Your Company?

No one is 100% safe, but the following 3 tips will stop you from accidentally giving online criminals access to your computer network and confidential information:

1. Never visit or download free music files, videos or programs from file-sharing sites such as Kazaa. Not only are you downloading stolen materials, but these sites are surefire ways to introduce worms and viruses to your computer. If you are a business owner, set up web filtering software to prevent employees from downloading any unauthorized programs or files.

2. Never respond to any e-mail from a bank, credit card company, PayPal or online store where items are purchased (such as eBay) asking you to verify your account information, no matter how credible or legitimate it looks. These are phishing scams set up to access your account information.

3. Ask for identification from anyone asking for physical access to electronic equipment and instruct staff do so as well. Just to test a theory, I asked a friend to walk into an office, say they are from "the phone company" responding to a problem, and ask to see the network. Access was granted to a complete stranger 100% of the time.

Get A FREE Security Audit (For September 2022) To Make Sure Your Company Is Protected!
Call Us Right Now : 760 (940) 4200

Shiny New Gadget Of The Month:

Logitech Litra Glow

Zoom 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 Zoom calls, shooting marketing videos or doing anything else webcam-related, the Litra Glow provides you with perfect light for any situation.

3 Questions No Leader Should Ever Ask

Over the years, I have advised many board members and CEOs of large companies on their most important leadership issues. In life, people like to think that there aren't inherently right and wrong questions to ask, but I think that's a misconception – especially in the world of business. "Right" questions are the ones that matter. They cut to the heart of the issue and produce an answer that a leader can act on. The "right" questions help leaders get results.
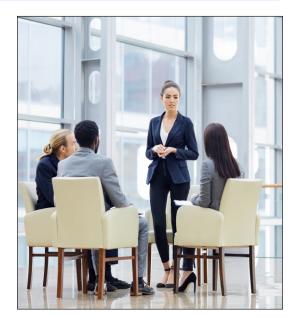
On the other hand, you have "wrong" questions. The mere act of asking these questions can lead you down the wrong path and prevent you from achieving your full potential in your career. Over the years, I've heard the "wrong" questions asked a multitude of times, and they can usually be grouped into three distinct categories.

Ethical Questions
The wisest, most successful leaders I have worked alongside all seem to lead according to this rule regarding ethical questions: "If you have to ask, then don't." In other words, if there is something that makes you feel that it is in the gray area or that taking an action might even be misinterpreted as unethical, then just don't do it. I've never seen a leader regret having held back from taking an action when they had an ethical question. "How unethical would it be if…" is a question no leader should ever ask.

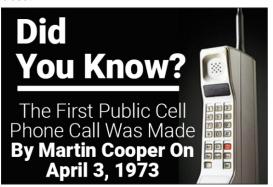**Questions Regarding Underperformance**
There is a cycle of "facing reality" that my clients sometimes go through. They have a bold vision: a goal to achieve something great. And when they realize that they don't have the team to make it happen, they start to fantasize and think, "I wonder if Fred or Amy will rise to the occasion and suddenly

display strengths or show a burst of energy we have not seen to achieve these results." Subordinates typically follow a very predictable pattern of performance. Great leaders know who they can count on to do what. So you rarely see great leaders asking themselves, "I wonder if my subordinate will suddenly perform well in a role that does not appear to fit their talents and interests."

Questions About Trusting Your Boss
There is a saying that people don't quit companies, they quit bad bosses. So if you find yourself wondering whether you can trust your boss or not, you likely can't. Go find a boss you can trust, one who will hold your interests in high regard. Rarely do you see great leaders staying in roles where they ask themselves, "I wonder if I can trust my boss."

Did You Know?
The First Public Cell Phone Call Was Made By Martin Cooper On April 3, 1973

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

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 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.

> "It Has Become Appallingly Obvious That Our Technology Has Exceeded Our Humanity."
>
> **Albert Einstein**

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.