Responsive
Technology Partners
Issue 47 | December 2022

CONSULT AN IT COMPANY ON CYBER INSURANCE

The cyber landscape has a steep and rocky terrain and the best bet for a company wanting the most out of their cyber insurance is to consult with an IT service provider.

IT companies have valuable insight in the cyber field and will be able to coach your company to negotiate the most efficient cyber insurance plan possible.

“Each insurance provider won’t offer the same coverage, so it’s important to know what types of coverage are available and what elements you should look for in an insurance policy.” (U.S Chamber of Commerce). “Even small businesses are vulnerable to cyberattacks and data breaches, and they can be extremely costly. Cyber insurance can help businesses prepare for and deal with any attacks that may come, while also helping them recover from any damage that is done.”

Cyber security service providers will have the most comprehensive information about what is needed in a cyber insurance coverage plan. Many cyber claims are ruled in favor of insurance companies due to ambiguous language. This can be avoided with the consultation of an IT company.

“Victories for insurance companies allowed insurers to avoid paying legal fees as many cyber-related class action suits emerged. Courts also sent a firm message to businesses making cyber claims: If they wanted protection for data breach and cybersecurity incidents, they would need to purchase a newly developed cyber insurance policy.” (Law Fare).

A cyber security professional can tell a company what policies they need and which ones they could do without.

“’Cyber insurance typically contains ‘business interruption’ coverage," said Andrew Lipton, Vice President and head of cyber claims at AmTrust Financial Services. ‘Depending on the wording of the policy, a small business could expect to be covered for lost business income during a given time period when that lost business income is directly attributable to an unintentional computer system interruption.’” (U.S Chamber of Commerce).

Courts may not rule in a company’s favor for a cyber insurance claim. IT professionals have the most expertise on the wording that should be used in a cyber insurance plan.

“Different policies offered different definitions of what was considered computer fraud. In turn, courts had different views about how clear that language was and how directly a crime had to be executed by a computer for it to count as computer fraud. For policyholders, these various definitions and interpretations of computer fraud coverage led to considerable uncertainty about which policies applied as insurers continued to experiment with new language in their computer fraud policies.” (Law Fare).

Want help developing a cyber insurance plan for your company? Responsive Technology Partners offers consultation services that can help companies formulate the right cyber insurance coverage for them. With offices in Athens, Metter, Milledgeville, Vidalia, and Atlanta, GA; Tampa, FL; Roanoke, VA, and Raleigh, SC areas, we are the leading cyber security expert in the South. Service offerings include IT support, cyber-security and compliance, telephony, cloud services, cabling, access control, and camera systems. Our company’s mission is to provide world-class customer service through industry leading IT solutions that make every customer feel as if they are our only customer. Please visit our website to learn more: https://www.responsivetechnologypartners.com/services/

I WAS A VICTIM OF PHISHING: THIS IS HOW I FEEL

My bank sent out an email reminder that they will never call me, email me, or text me and ask for my user ID and password.

I can only hope that I wouldn't have complied with a request for my information had my bank not reminded me. I once had my Venmo account hacked due to a similar scheme. Venmo is an online money-transferring app that connects to your bank account to send funds to your friends and family. My information was stolen through the very same cyber-attack that my bank was describing in their email: phishing.

Phishing is a type of cyber-attack where a cyber-criminal poses as a reputable authority and tries to swindle your information out of you. There are a variety of phishing techniques, but the most common ones demand your information because they "need it" to "help you".

In my case, I received a phone call from "Venmo" (it wasn't Venmo) saying that my account had been hacked (it hadn't). They had already attempted to login to my account before making the call to my phone number and had only made the call to receive the two-factor authentication code sent to my device.

Luckily, nothing major occurred and I was able to lock my accounts and get my password reset so they could no longer access my account. However, I knew that my passwords had been compromised and I had to reset all my accounts that had that same password attached. They had at least my phone number and password and potentially more information than that. The email my bank sent to me reminded me of the incident and the impact it had on me and my emotional state.

I felt ashamed. I felt dumb for giving whoever it was I was on the phone with my authentication code. Oftentimes, cyber-criminals will play on your emotions to get what they want. My specific caller had me feeling panicked, as though my account had already been breached and my only hope was to comply.

Now, reading this email from my bank, I feel more prepared in the event of phishing. I now know that my bank has been subject to these kinds of attacks, and I can now look out for suspicious behavior. Now that I know more about these kinds of attacks, I am confident that it won't happen to me again.

If you feel ashamed after being subjected to a cyber-attack, know that you're not alone. According to USA Today, over two-thirds of victims of cyber-attacks report feeling hopeless or powerless after the attack. In the case of depression or anxiety in the fallout of an attack, always seek help from a professional.

Have any questions about cyber-security? Responsive Technology Partners is the leading cyber-security expert in the Athens, Metter, Milledgeville, Vidalia, and Atlanta, GA areas. We also have locations in Tampa, FL, Roanoke, VA, and Raleigh NC.

IT NEWS, TRENDS AND INFORMATION YOU MAY HAVE MISSED IN 2022

The year 2022 will soon be on its way out the door. It became a year full of ups and downs for many small businesses, but it still felt more promising than the past few years in the midst of the pandemic. Many small-business owners used this past year to re-evaluate their IT services. Some needed to strengthen their cyber security defenses while others utilized new advancements to further assist their customer base.

If you're a small-business owner, it's essential that you're aware of the IT news, trends and events that took place in the recent past. In fact, knowing what happened in the previous year can allow you to develop plans for the future so 2023 will be successful for you and your business. You shouldn't continue following old trends because the competition will quickly leave you behind, and that could open you up to cyber-attacks you didn't know existed. Don't worry, though; we're here to help. Here are our picks for the most important IT events and trends of 2022.

Refined Artificial Intelligence

Artificial intelligence (AI) has come a long way over the past few years. Many people associate AI with video games or using GPS for travel, but many companies have started to implement AI in new ways to boost their businesses. It's even being used to automate certain tasks, provide insight through data analysis and assist customers with their needs.

AI has proved incredibly beneficial when used to help customers, and this can be seen when looking at various small-business websites. They use AI to answer common questions their customer base has, which provides quick, efficient results for their customers, who leave satisfied with their interaction. Around 37% of businesses now utilize AI in the workplace, according to a survey conducted by Gartner. Another study by NewVantage Partners found that nine out of 10 leading businesses have investments in AI technologies. So, if you want to get ahead of your competitors, implement AI into your business.

Managed IT Services Providers Continuing To Grow In Popularity

Gone are the days of having an in-office IT person or team. A more cost-effective solution has been gaining traction over the past few years and will continue to do so for the foreseeable future. Managed IT services providers (MSPs) install, support and maintain all the users, devices and PCs connected to your network on a routine basis. MSPs can even prevent common problems such as lost devices, hardware failures, fires, natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. The managed IT services industry is growing immensely. At the end of 2021, the industry was valued at $239.71 billion, and it's estimated to grow by over 13% annually until 2030. Businesses of all sizes have realized the value of MSPs and are using them to their advantage.

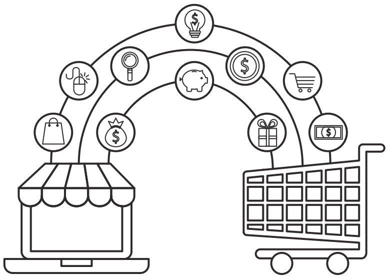
Major Cyber-Attacks Of 2022

Cyber-attacks happen all the time. As new cyberthreats emerge, we'll see more frequent and severe cyber-attacks over the next few years. Uber saw another cyber-attack this past September that caused the company to shut down its internal messaging service and engineering systems in order to get to the bottom of the incident. Cryptocurrency storage and blockchain were also high-value targets for cybercriminals. Ronin and Crypto.com suffered severe cyber-attacks that required both companies to reimburse their users for the cryptocurrency stolen in the attack.Ronin was hacked for $540 million, and Crypto.com was hacked for $33 million worth of cryptocurrencies.

Small businesses weren't safe from cyber-attacks either. While cyber-attacks on big businesses make national news, small businesses are targeted more often since their cyber security defenses aren't as strong. That being said, it's imperative you ensure your business has efficient cyber security practices in place, so you won't have to worry as much about cyber-attacks.

The IT industry is consistently changing to keep up with new developments and advancements. If you're a small-business owner, it's vital to keep up with the latest news and information so you can best protect your business and its data. When you stay ahead of the trends, it's much easier to prevent potential cyber-attacks and threats.

2 CHALLENGES E-COMMERCE BUSINESSES FACE AND HOW TO OVERCOME THEM



With the Internet came a new digital marketplace that allowed people to purchase specific products they couldn't find in their hometowns. These days, most businesses offer a way to buy their products or services online, whether it's through their personal website or an e-commerce marketplace like Amazon. Despite this, selling online brings new challenges you don't often see when selling from within a brick-and-mortar location. Here are some challenges to watch for and solutions to overcome them.

Payments

Oftentimes, e-commerce businesses need to deal with chargebacks. This happens when a customer disputes a charge on their credit card statement, causing you to lose out on the sale and the item.To avoid this, have a clear and concise return policy. You should also keep detailed records of all transactions and shipments to prove the customer received their order.

Shipping

Shipping delays can leave customers feeling frustrated, even if they aren't the company's fault. You can't do anything to control hazardous weather, but you can set a reasonable range of time for your customer to receive their item. You don't have to promise two-day shipping just to compete with Amazon. It can also help to utilize shipping management software to automate your shipping processes.

CPA's and Tax Preparers Ready for December 2022 Compliance Deadline

- In the Gramm-Leach-Bliley Act, the "Safeguards Rule" requires individuals who assist with financial products or tax preparation services to ensure the security and confidentiality of customer information.
- Some provisions take effect in December 2022; compliance for financial institutions is <u>not</u> optional. Companies should prepare to implement safeguards into their programs to follow the guidelines laid down by the FTC.

Protect yourself TODAY with a FREE initial assessment!
Call (877) 358-9388 and book your now!