LASTPASS DATA BREACH

LastPass, a leading password management application, suffered a breach on August 26th and developments have occurred in the following months. The breach allowed hackers to access development servers and LastPass determined in their September investigation that no user data was compromised. However, November and December brought new developments.

Using the stolen data from August, a hacker was able to use a 3rd party cloud service utilized by LastPass to gain access to customer information. Later in December, Last Pass released an update saying that the hacker was able to obtain a copy of customer data backups. The vault data includes details such as usernames, passwords, notes, form data and URLs.

According to LastPass, this data is encrypted, however with access to a master password, hackers can decrypt the data. Additionally, the data that was accessed could be used to launch other cyber-attacks such as phishing schemes. If you are a Last Pass user, Responsive Technology Partners recommends that you take these steps to ensure your cyber safety.

- Revolve passwords and keys in LastPass
- Don't reuse passwords and change any recurring passwords
- Use Multi-factor Authentication
- Be vigilant in checking for suspicious activity

LastPass will never ask you for information through text or email, especially one containing links to verify information. Stay alert and aware of the possibility that phishers may impersonate LastPass support. As always, Responsive Technology Partners is here to guide you with any cybersecurity issue you may have.

Responsive Technology Partners Receives "Outstanding Community Participant" Award

CLEARWATER HOUSING AUTHORITY

Florida Market President, Jose Remon, had the pleasure of accepting the first Clearwater Housing Authority Outstanding Community Participant Award on behalf of Responsive Technology Partners.

"They are always available and quick to respond no matter how simple the matter or complicated. The RTP staff are very personable and always fix our issues with a smile. They provide quick meaningful solutions for our Information technology systems. They make us all feel like we are their only client. They are incredibly patient, timely, and responsive to all our needs. They truly care about CHA and it shows in their work. They continue to go above and beyond each and every day. We appreciate everything they do and we feel that Responsive Technology Partners truly deserve this Outstanding Community Participant Award" - Clearwater Housing Authority

RESPONSIVE TECHNOLOGY PARTNERS ATTENDS GREATER VIDALIA CHAMBER ANNUAL LEGISLATIVE LUNCHEON

(L-R: Alex Muzafarov, CTO; Mike Hagan; State House Representative Leesa Hagan; State Senator Blake Tillery; Steven McComas, CEO)

The Greater Vidalia Chamber of Toombs-Montgomery counties hosted the Legislative Luncheon on Thursday, January 5, 2023 at Lyons First Baptist Church. Held by the Chamber's Public Policy Council, this annual event spotlights Georgia's Economic Development issues and impacts statewide.

Nearly 240 business leaders and community business members gathered before guest speakers State Senator Blake Tillery and State Representative Leesa Hagan to learn what issues will be addressed and what to expect from Atlanta on business focus and economic development before the legislative members go to session. Interest runs high as Georgia was recently named No. 1 state for business for the ninth consecutive year by Area Development magazine.

In attendance at the event was 280 Society co-sponsor Responsive Technology Partners' CEO Steven McComas and Chief Technology Officer Alex Muzafarov. Responsive Technology Partners, an IT Support provider with offices in Vidalia and Metter Georgia, represents one of the leading growth companies in both the state of Georgia and in the southeast. With a total of 10 offices spanning Georgia, Florida, North Carolina, and Virginia, Responsive was recognized by Inc. 5000 for the third consecutive year among the fastest-growing privately owned companies in the country, ranking No. 474.

"From our humble beginnings five years ago in rural Georgia to where we have grown now, we are so proud to be part of such a dynamic community of growth and development, and look forward to investing in our clients' success," says McComas. "Alex was the first addition to the RTP family, and from there, the growth became exponential."

The annual Legislative Luncheon serves as a platform for Legislative members to ensure their actions during the upcoming session prolongs Georgia's ownership of the prized No. 1 economic development position. "What is good for Atlanta isn't always good for rural Georgia, but what is good for rural Georgia is good for all of Georgia," stated Representative Hagan.

Get More Free Tips, Tools, and Services at Our Website: www.responsivetechnologypartners.com
(877) 358-9388

ADD AN EXTRA LAYER OF CYBER SECURITY PROTECTION BY UTILIZING CYBER INSURANCE

Establishing effective and efficient cyber security policies is one of the most important aspects of protecting your business. We often discuss why cyber security is so important and the different cyber security practices your business can implement. We also mention how advanced cyberthreats and cyber-attacks have become as hackers improve their tactics and technology. For this reason, you may wonder if there's anything that will cover your business if it falls victim to a cyber-attack even though you have strong cyber security practices in place. Thankfully, cyber insurance is available to business owners who have proven they take cyber security seriously.

Cyber insurance (sometimes referred to as cyber liability insurance) is the coverage an organization can acquire to protect against losses incurred by a data breach or other malicious security incidents. Cyber insurance policies have grown exponentially in popularity over the past few decades as cybercriminals have become more cunning. Because of this, cyber insurance prices have also risen, so you may be curious whether cyber insurance is something your business absolutely needs.

Cyber insurance policies differ from provider to provider, but most will include the following coverages:

- **Customer And Employee Outreach**

  If your business is the victim of a cyber-attack and precious information is stolen, who are some of the first people you need to contact? Your customers and employees, of course. They need to be aware that a cyber-attack occurred, and their information may have been compromised. Depending on your industry and location, there may be a legal obligation to inform. If you have a large customer base, notifying them of a cyber security breach can be expensive. Cyber insurance will help cover those costs.

- **Recovering Stolen Data**

  It can be costly to hire a data recovery professional to recover stolen customer or business information, but it is necessary after suffering a cyber-attack. Most cyber insurance policies will pay for a professional's help.

- **Software And Hardware Repair/Replacement**

  Cybercriminals can wreak havoc on your software and hardware. If they damage or corrupt your computers, network or programs, your cyber insurance policy will help cover the cost of repair or replacement.

Some insurance policies will also cover any financial loss due to business interruption caused by a cyber-attack and ransomware demands. Cyber insurance will not cover your system upgrades, estimated future financial losses due to a breach or decreased valuation of your business caused by a cyber-attack. It's vital you know exactly what is covered by your policy before beginning coverage.

Starting a new cyber insurance policy is easier said than done. Since cyber insurance has grown in popularity, most providers have become more selective about who they cover, meaning you have to meet some criteria to qualify for a policy. The most essential thing any cyber insurance provider will look at will be the strength of your current network security and cyber security practices. Ensure you utilize multifactor authentication throughout your entire business and hold training sessions annually with your team. Purchase a firewall and do whatever else you can to improve your security. If you don't, the rates for your policy will be astronomical, if you can even get one at all.

Suppose your business is within an industry that requires a certain level of cyber security compliance. In that case, you should be meeting your requirements or else you won't qualify for a cyber insurance policy. This shouldn't be an issue for your business since you must be compliant regardless of your interest in cyber insurance. Just make sure you look into your compliance requirements before applying for a cyber insurance policy to ensure you don't get denied coverage.

If you work with third-party vendors, you must do your due diligence and ensure they meet their cyber security requirements. Doing thorough research on the parties you interact with will help you get more affordable cyber insurance rates. Additionally, it would be best if you had an incident response plan in place. The insurance provider needs to know you're prepared to help your customers and your business if disaster strikes.

Cyber insurance can help further protect your business if you become the victim of a cyber-attack. In today's society, where every business and their customers' information is a target for cybercriminals, make sure you're as secure as possible. Build a strong cyber security plan and apply for cyber insurance to get maximum protection.

DANGERS OF ONLINE DATING

Dating apps such as Tinder and Bumble make way for a new age of digital dating, however, simultaneously opens doors for cyber criminals to target individuals.

"There is a dilemma with dating apps that we need to address. Strong relationships require vulnerability, authenticity and trust, but responsible dating app use demands security and safety. How do you build a trusting relationship from an app that could potentially introduce you to dangerous people?" (Deseret).

There are many different techniques scammers use to attack online daters, such as identity theft and fraud.

"Unfortunately, scammers target online dating services to commit identity theft and financial fraud. In 2021, over 24,000 Americans were hit by romance scams, with scammers stealing over $1 billion." (Aura).

So, in this new age of dating, how does one stay safe?

"Dating app users should be cautious about how much data they give out on a dating app. As reported by The Guardian, linking your social media account can reveal personal information that you may not want a stranger to know. The Guardian suggests using photos for your dating profile that are different from your social media accounts so that a reverse image search won't give out your social media information. Do not give out your contact information, physical address, financial information or sensitive personal information on a dating app." (Deseret).

Always be careful and suspicious of new matches.

"If you feel a connection with someone, do a quick Google search of their photos and name to make sure they're not a scammer. Meeting people offline (in a public place at first) is always the first step toward trust. Be very careful about doing any favors or trusting a match too much at first if you haven't even met them in real life. If they start talking about money, needing help, or having some kind of medical emergency, you should take that as a red flag." (Aura).

Overall, be wary of anyone you meet online, especially on dating sites this Valentine's Day season!

HOW TO KNOW WHEN TO BREAK UP WITH YOUR CURRENT IT SUPPORT GUY

Working with IT is like being in a relationship. Cyber security is becoming more crucial every day and while IT guys can help, sometimes there are issues preventing a stable and happy arrangement. Here are 5 reasons you should break up with your current IT Guy:

1. Do they respond to emergencies in 1 hour or less?

IT teams can get overloaded. Does your IT provider regularly fail at servicing your needs as quickly and as consistently as promised? If your IT guy isn't listening to you, consider going to someone who will.

2. Do they proactively offer new ways to improve your network's performance, or do they wait until you have a problem to make recommendations?

Security is arguably the most important aspect of your relationship with your IT support provider. If they aren't protecting your business and network, what are they there for? Protecting vital information should be the top priority of your cybersecurity efforts.

3. Are they easy to reach and responsive when you need them for non-emergencies?

Communication is the next important signifier of a healthy relationship. If your IT guy isn't checking in regularly, the quality of your service can suffer. Choose an IT Support provider that will communicate efficiently and effectively.

4. Do they provide detailed invoices that clearly explain what you are paying for?

Sometimes IT guys don't provide detailed invoices that sufficiently lay out what services are being paid for. Itemized invoices are crucial for evaluating budget and spending. Consider finding an IT provider that will provide detailed invoices.

5. Do they explain what they are doing and answer your questions in terms that you can understand?

Compatibility suggests answering your questions in terms that you can understand. Does your IT provider ask questions and offer answers in plain English or geeky tech-talk? If you routinely find yourself with more questions than answers, your current IT relationship may be headed for trouble.