Responsive Technology Partners

Issue 43 | August 2022

Plans for Greater Vidalia Center for Rural Entrepreneuership

CEO STEVEN MCCOMAS HONORED IN VIDALIA, GA

Steven McComas, Chief Executive Officer of Responsive Technology Partners, was recognized by the City of Vidalia, Georgia, the Greater Vidalia Chamber of Commerce, and Toombs County Development Authority at a recent City Council meeting for his leadership and efforts toward creating the new Greater Vidalia Center for Rural Entrepreneurship.

Steven is the Immediate Past President of the Greater Vidalia Chamber of Commerce and was honored as the July Sweet Onion Citizen of the month at the City Council meeting.

"We recognize your hard work and dedication," Mayor Doug Roper said of Steven. "We know that you did a lot of work on your own volition, and it didn't go unnoticed."

Steven accepted the award with these words, while also thanking others for their contribution to the success of the project.

"This project shows that rural communities matter. My hopes and dreams are that this center will be used by the community and that it will make a difference in lives for years to come." Steven said.

Responsive Technology Partners strives to be an ongoing active tenant in the new Greater Vidalia Center for Rural Entrepreneurship and are committed to investing in the local community. The center will act as a small business incubator, allowing for small businesses to grow, and cultivating the rural community.

Left to Right: CEO Steven McComas, Vidalia Mayor Doug Roper

Coming Soon to a venue near you...

CYBER SUMMIT 2022 SERIES

Fri 9/16 — **Raleigh, NC**

Register now! 👉

Fri 10/7 — **Marietta, GA**

Register now! 👉

Discover Critical Cyber Security Protections EVERY Business Must Have in Place NOW to Avoid Cyber-Attacks, Ransomware, and Data-Breach Penalties.

GA Bonus Round: HIPAA DINE & LEARN

Tues 8/30 — **Statesboro, GA**

Wens 8/31 — **Vidalia, GA**

Learn how our dedicated IT team will ensure your company's sensitive information is protected and keep your business compliant with any third-party regulating bodies in the process.

*Seating limited to 25 per event, register now: (912) 325-3120

4 WAYS TO BETTER PROTECT YOUR PERSONAL INFORMATION

Most people keep their personal information as secure as possible. They don't post their passwords on social media or share Social Security numbers with untrustworthy sources. These practices seem obvious, but there are smaller things we can do to provide better protection. You'll find four of those tactics here.

- **Dangers Of Unsecured WiFi**

Hackers can use this connection to download malware on your devices.

- **Password Manager**

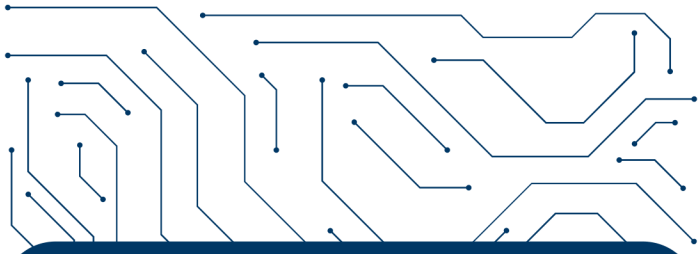
You shouldn't use the same password between multiple accounts. Utilizing a password manager will help you keep track of different passwords.

- **Breached Companies**

When a company's security is compromised, all of its customers' personal information can be exposed. Avoid working with these companies until they've offered improved security.

- **Think Before Posting**

Be careful about what you share on social media. Revealing too much personal information can leave you vulnerable to a cyber-attack.



TECH TRENDS TO IMPROVE CUSTOMER LOYALTY

If you want your business to succeed, you must build a solid customer base. Over the past few years, advancements in technology have made it easier for companies to improve their relationships with their customers. One such way is through the use of AI chatbots. If someone has a question about your service or product, you don't want to leave them waiting for an answer. Chatbots can be programmed to answer common questions until a live representative is available, if they're even needed.

Additionally, you should make an effort to monitor content created by people outside your company. If someone is spreading false information about your business, you need to combat it. If disinformation is allowed to fester, it can quickly sink a small business. Simply replying to misinformed reviews or reporting inappropriate content about your business can go a long way toward becoming a more trustworthy source in your industry.

August 2022

CYBER SECURITY AND HIPAA

Cyber security and HIPPA compliance are pretty closely linked. The stronger your cyber security, the less likely a technical security HIPPA breach will occur. Here is some more information on HIPPA compliance in relation to maintaining tight cyber security.

1. Business Associates vs Covered Entities

Cyber security and HIPPA compliance are pretty closely linked. The stronger your cyber security, the less likely a technical security HIPPA breach will occur. Here is some more information on HIPPA compliance in relation to maintaining tight cyber security.

2. PHI

PHI stands for Protected Health Information. There are many identifiers of PHI, and all covered entities and business associates must keep PHI private in order to abide by HIPPA laws, electronic PHI included. Cyber security is especially important in the protection of online PHI records.

3. Do All Audits and Assessments

To ensure the protection of stored PHI, make sure to complete all required audits and assessments when it comes to HIPPA compliance. These include, Security Risk Assessments, Privacy Standard Audits, Security Standards Audits, Asset and Device Audits, HITECH Subtitle D Privacy Audits, and Physical Site Audits.

4. HIPPA Security Rule Risk Assessment

SRAs, or Security Risk Assessments include collecting data, determining potential threats and vulnerabilities, ePHI and document vulnerabilities, assessing current security measures, assessing the likelihood of threat occurrence, the potential impact, and determining the level of risk. A lack of an SRA can result in HIPPA fines. SRAs increase cyber security

5. Annual HIPPA training

Having an annual HIPPA training course for all employees will greatly improve competence and safety with important documents. Also, having a designated HIPPA compliance, security, and privacy officer will help this run more smoothly each year. Make sure to document each employee's participation.

6. Have a process for breaches

In addition to training employees, there must be a plan in place if a breach were to occur. You should have the ability to track and record the investigation following the incident. Having staff be able to report incidents anonymously will likely increase the number of incidents that are handled and resolved.

7. HIPPA covered entity employee tips

For employees of both Covered Entities and Business Associates, it is important for them to be aware of HIPPA compliance in their everyday work lives. Never share login credentials and don't access your own PHI records through your own login credentials. Go through HR or access them as a client or patient would. Don't share PHI on social media and don't leave PHI containing devices unattended.

8.Cost of HIPPA compliance

HIPPA compliance can get costly. There are many consultants and groups you can hire and utilize to realize the full potential of HIPPA and security compliance. One of these groups is the Compliancy Group. The Compliancy Group can help you meet all HIPPA requirements for an affordable price.

HIPAA SEAL OF COMPLIANCE
COMPLIANCY GROUP

HIPAA VERIFIED

855-55-HIPAA
info@compliancygroup.com