Responsive Technology Partners

Issue 50 | March 2023

KEEP YOUR BUSINESS PROTECTED BY BECOMING AWARE OF THE MOST COMMON TYPES OF CYBER-ATTACKS

The rate of cyber-attacks has significantly increased over the past few years. Businesses of all sizes are at risk of becoming victims of them, which is why it's crucial that every business owner and leader is aware of the most common cyberthreats impacting the business world today. Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals.

These criminals' tactics will improve as technology continues advancing, but cyber security defenses will as well. Knowing exactly what you're up against with cyber-attacks and creating the proper safeguards will protect your business. If you're new to the idea of cyber security or need an update on the common threats that could impact your business, we've got you covered. Below, you will find the most common types of cyber-attacks out there and how to protect your business from them.

Malware

Malware has been around since the dawn of the Internet and has remained a consistent problem. It is any intrusive software developed to steal data and damage or destroy computers and computer systems. Malware is an extensive type of cyber-attack, and many subcategories belong to it, including viruses, spyware, adware and Trojan viruses. One type of malware that has lately been used more frequently is ransomware. Ransomware threatens to publish sensitive information or blocks access to necessary data unless a sum of money is paid to the cybercriminal who developed it.

Unfortunately, malware can be detrimental to nearly every operation of your business, so you should do two essential things to prevent it from affecting your company. First, you should install the latest anti-malware programs. If you hire a services provider, they will take care of this for you. If not, you'll need to find anti-malware that works best for your system. You should also train your team about these risks and ensure they are aware not to click on any suspicious links, websites or files that could be dangerous.

Phishing

Have you ever received an e-mail asking for sensitive information that looked official, but something just wasn't quite right? Chances are it was probably a phishing scam. Phishing occurs when cybercriminals send official-looking messages to individuals, posing as another organization, in an attempt to receive personal information. Falling for a phishing scam can quickly result in you becoming a victim of identity fraud. The results can be substantially worse if a business falls for the scam.

So, how do you best prepare for and protect your team against phishing scams? Utilize employee cyber security trainings so they can spot the warning signs. The actual e-mail will usually line up differently from whom the cybercriminal is trying to represent. Also, most organizations will not request private information over e-mail. Common sense will prevail over phishing scams.

Distributed Denial Of Service

DDoS attacks can bring your business to a standstill. These attacks occur when malicious parties overload servers with user traffic, causing them to lag or shut down since they are unable to handle incoming requests. If your business falls victim to this kind of attack, your employees might not be able to access key functions required to do their jobs, and customers may not be able to use your website or purchase items from you.

DDoS attacks are very difficult to thwart, and a determined cybercriminal can lock up your websites and networks for days on end. You'll have to identify malicious traffic and prevent access before it can cause damage. Hiring an MSP is your best bet to prevent DDoS attacks. If a DDoS attack is successful, you'll probably have to take your servers offline to fix the issue.

Password Attacks

If a cybercriminal gets your password or another employee's password, this is the easiest way for them to access your valuable information. They may attempt to guess the passwords themselves or use a phishing scam to gain access. It is vital that you enable multifactor authentication for your employees and require complex passwords so you can defend your company against password attacks.

Now that you know the most common forms of cyber-attacks currently happening, you can take the necessary precautions to protect your business, employees and customers.

CYBER SPRING CLEANING

With Spring getting ready to be in full swing, it's time for spring cleaning, cyber-security style. Clean out tangible and intangible vices to start the season off fresh.

1. Get rid of old devices and software

Securely dispose of old devices by taking them to a recycling service provider such as Best Buy. It's necessary to wipe your old devices before taking them in to be recycled.

2. Get rid of bad cyber-hygiene

Clean up bad habits with cyber-training. Bad cyber-hygiene causes cyber-attacks and to start your Spring anew, implement lessons in cyber-security.

3. Get rid of old passwords

Compromised passwords must be disposed of. Evaluate each of your passwords, implement multi-factor authentication, and use a password management system.

4. Get rid of unauthorized applications

Application whitelisting can help improve the number of unauthorized applications such as malware and ransomware. Consider implementing whitelisting in your organization this Spring.

5. Get rid of exposed data

Full-disk encryption can help limit the exposure of compromised data. Encryption protects the data, and therefore the organization. Implement full-disk encryption in your organization to protect data.

CYBER SECURITY RISK MANAGEMENT PRESENTATION AT ROTARY CLUB OF VIDALIA

The Rotary Club of Vidalia held a Cyber Security Risk Management program for local business leaders Wednesday, February 15, 2023. During a weekly Rotary luncheon at the Vidalia Presbyterian Church, Responsive Technology Partners presented an executive overview of an organization's risk management profile to the group. "What is an Information Risk Program and Why Does It Matter?" was the security topic aimed at business owners.

Responsive's Chief Security Officer Jay Harmon led a conversation on tailoring Cybersecurity and Information Risk Management to specific organizations. "There is a correlation in today's world where Data and Technology are equivalent to currency and money", said Harmon. "When we think about what we have to protect, we're looking from a perspective of (that) data is money, and money is at risk." He described the various ways organizations are impacted by security breaches, including ransomware and business email compromises, while explaining how other nations' states are after U.S. data because it is easily monetized by selling stolen personal data records on the Dark web.

Harmon shared how to identify potential security threats based on an organization's data use, creating a need for an information risk management program. The half hour Cybersecurity session was followed by a lively Q & A, where the discussion turned to practical applications and use of AI (Artificial Intelligence).

(L-R: Jay Harmon, CISM ISO, BorderHawk; Vidalia Rotarians Angie McDaniel and Brad Owens; Steven McComas, CEO, and Alex Muzafarov, CTO, both of Responsive Technology Partners)

Responsive Technology Partners' CEO Steven McComas offered closing remarks as the meeting ended. "There are two things I'd like to leave with you in this field, because it's growing so fast and it's so complex. If you're concerned about your assets, please have a Disaster enactment to see where the flaws are. Also, Rural communities are not immune; in fact, they're the target. A lot of global organizations have fantastic security systems in place, but in our rural communities, we don't have those types of resources."

Responsive Technology Partners provides superior IT support services throughout Georgia, Florida, North Carolina, and Virginia, as well as across the U.S. Our service offerings include IT support, cybersecurity and compliance, telephony, cloud storage, point of sale implementation and management, cabling, access control, and camera systems. Simply put 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." For more information regarding our services, locations, or employment opportunities, call (877) 358-9388 or email info@responsivetechnologypartners.com

Coming Soon:

Tampa Cyber Summit

Thursday April 4, 2023
Tampa River Center

Julian B Lane Park
402 W Laurel St
Tampa, FL 33607

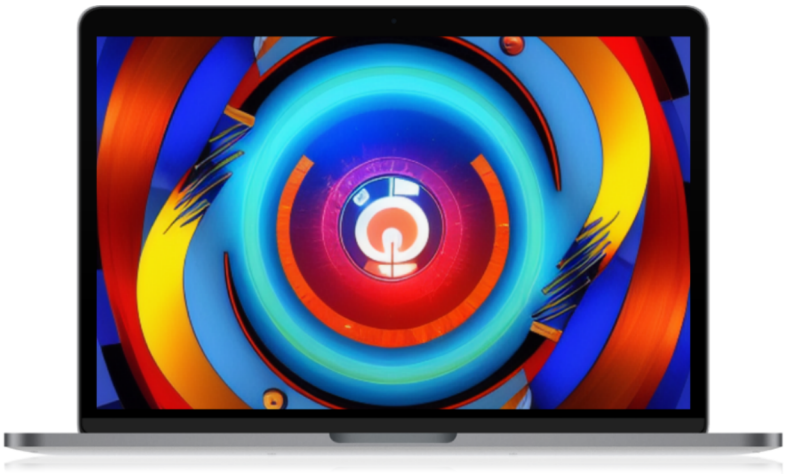
METROPOLITAN MINISTRIES

All proceeds to benefit Metropolitan Ministries

AI Generated Art

A swirling mass of vibrant colors and shapes, with jagged lines in a deep blue and light blue, representing the complex and ever-changing landscape of the digital world. In the center of the image, there's a golden shield, shining brightly, symbolizing the protection that cyber security provides. The shield is surrounded by a swirling vortex of orange and red, representing the dangers and threats that exist online. The overall feeling of the image is one of dynamism, protection, and the ongoing battle against cyber threats.

An AI Poem about Cyber Security:



In a world of ones and zeroes,
Where data flows like endless streams,
Cyber security stands guard,
Defending against malicious schemes.

With firewalls and encryption,
And passwords strong and true,
It keeps our information safe,
From those who would seek to pursue.

Hackers and viruses lurk,
In the shadows of the web,
But cyber security stands tall,
Against their attacks, it won't bend.

So let us all take care,
And protect what we hold dear,
With good practices and secure tech,
Cyber safety will be near.

For our digital world is vast,
And growing every day,
But with cyber security in place,
We'll keep our data safe, always.

This image and poem were created using ChatGPT and StarryAI. The process of creating images and text through AI is a surreal experience. Artificial intelligence will change the scope of how we create.

But how does one generate poetry and images with AI? And what are the implications of this?

“Some may argue that the AI is the true author of the generated content, while others may see the human user as the author for providing the input and structuring the process.” (Medium).

Crafting a poem with AI requires you to give the AI guidance in the kind of result you desire.

“Large language models like ChatGPT are great at generating text, but they often need a little guidance to produce something creative and thought-provoking. That’s where a structured approach comes in.” (Medium).

A structured approach is using follow up questions along with the prompt to help the AI have a better gauge of what kind of product is wanted.

“These questions can help ChatGPT generate a more complex, interesting poem that goes beyond the surface level of the prompt. In addition to improving the quality of the result, such a process is more engaging and interactive. Instead of trying to figure out that perfect prompt, we can actively guide ChatGPT and see how it responds to our questions and feedback.” (Medium).

With an image, it is usually a lot harder to create an image using AI if you are not using a generator such as StarryAI.

“AI Art generation is usually a laborious process that requires technical expertise, we make that process simple and intuitive.” (StarryAI).

StarryAI can make beautiful and complex images based on prompts you can create easily.

You can use a structured approach to generate AI images as well as poetry. Overall, crafting using AI will change the way in which we author and originate content.

“This technique can actually be applied to any creative task, and poetry is just a great example of how it can help generate more complex, interesting responses. I’ve seen how this approach can improve the quality of the generated content, and make the process more engaging and interactive.” (Medium).