Centrend
Volume 7.0
Monthly Newsletter

THE TECH CHRONICLE

October 2023 www.centrend.com Tuesday

WHAT'S INSIDE?

Halloween Special:

The Scariest Cyber Attacks of 2023

In today's increasingly digitized world, one thing has become abundantly clear - cyber security is scarier than Halloween. While the notion of ghouls and goblins may send shivers down our spines, the threats lurking in cyberspace are far more terrifying and have real-life consequences. From data breaches to ransomware attacks, cyber security incidents can cause significant damage to individuals and organizations alike.

With technology constantly evolving and the rise of interconnected devices, the potential for cyber threats has grown exponentially. What was once a concern primarily for tech-savvy individuals has become a mainstream issue affecting everyone, from small businesses to large corporations. It's no longer a question of if an attack will happen but when.

>>> continued on Page 2

Prospect Street Studio: Your E-commerce Photography Expert!

In today's visually-oriented society, imagery plays a crucial role in shaping the perception of your business and brand. It is often said that a picture speaks a thousand words, and this holds true when it comes to communicating the values and personality of your organization.

First impressions are crucial, and professional imagery can make a significant impact on how a business is perceived. High-quality photographs can instantly convey professionalism, credibility, and trustworthiness. Whether it's showcasing products, services, or the overall brand image, visually appealing content has the power to engage customers and leave a lasting impression.

>>> more on page 9

CARRINGTON CROTHERS
owner & founder - Prospect Street Studio

Halloween Special: The Scariest Cyber Attacks of 2023 continued.

The frightening reality is that cybercriminals are becoming increasingly sophisticated in their tactics, employing advanced techniques to breach even the most secure systems. They exploit vulnerabilities in software, use social engineering techniques to trick employees, and utilize malicious software that can lurk undetected until it strikes.

Not only are individuals at risk of having their personal information stolen or misused, but businesses face devastating financial loss, reputational damage, and legal ramifications. The fallout from a cyber-attack can be long-lasting and difficult to recover from.

The United States of America is the country that cybercriminals most frequently target. According to the report's analysis of US cyberattacks in 2023 and a comparison of attacks in 2020 and 2022, 49% targeted US-based enterprises. It's crucial to remember that roughly two-thirds of those attacks were intended to benefit from ransomware attacks. US-based businesses have paid eight of the top ten largest ransoms since 2020.

Cyber-attacks are becoming a greater menace as our environment grows more digital and more advanced technology is deployed widely across our citizen base. According to the US Cyber Attacks 2023 report, criminal actors are continuously looking for weaknesses to exploit, including ransomware and identity theft. While no industry is entirely impervious to these dangers, some are more exposed than others.

Here are some of the scariest cyber-attacks that happened this 2023:

More than 760,000 individuals' personal information on Discord.io was made public.

More than 760,000 users' personal information was made available due to a data breach at Discord.io, a custom invite provider for the Discord instant messaging service.

The breach went undetected until a database containing the personal information of Discord.io members was listed for sale on the dark web on August 14, 2023. Four user records from the database were shared by the hacker who uploaded the data under the identity "Akhirah," demonstrating the reliability of the information. Furthermore, Discord.io attested to the accuracy of the information.

2.6 Million Duolingo members' information was published on the dark web.

On August 22, information that had been scraped from more than 2.6 million Duolingo users was posted to a forum for dark web hackers.

The malicious actor claimed to have obtained access to the data via scraping an exposed application interface (API), and he made a $1,500 offer for it all. Additionally, they provided a sample of the data from 1,000 accounts to attest to its validity.

Regarding the cyber security incident, a Duolingo representative stated: "No data breach or hack has occurred. We take data security and privacy very seriously, and we're still looking into this to see if any additional steps are required to protect our students.

Since March 2023, the accessible API that was used to scrape the data has been known to the public. By entering their username, anyone can access the public details of any Duolingo profile.

On September 1, a Duolingo spokesperson contacted Cyber Security Hub with the following update: "Our investigation confirmed that this was not a breach or a hack; it was a scrape of data from public Duolingo profiles. No Duolingo systems or private user data were compromised."

Hackers target Roblox developers

Roblox, a popular computer game development and playing platform was attacked on August 1, 2023. An unidentified malicious actor seeded Malware known as "LunaGrabber" into many open-source software products. As they are presented as frequently used software packages on the open-source software library npm, malware-filled software packages have deceived developers for the online gaming site Roblox into clicking on them.

On August 22, the malware packages were found by ReversingLabs, a cyber security firm, and were confirmed by software threat researcher Lucija Valenti. She said the malware "imitated the legitimate package noblox.js, a Node.js Roblox application programming interface (API) wrapper used to write scripts interacting with the gaming platform.

Valenti further affirmed that the malware campaign's intended victims were "developers who write scripts to run on the Roblox gaming platform." The majority of the users of Roblox are underage children, and it's scary to imagine how the information gathered will be exploited!

A PurFood data breach exposes 1.2 million customers' personal information.

A data breach at American meal delivery business PurFoods exposed more than 1.2 million customers' financial and medical information, the company disclosed in August.

Even though PurFood's systems were compromised on January 16 of this year, the cyberattack was not identified until July 10. PurFoods realized that some files on its network had been encrypted, which led to the discovery of the breach, which resulted from a malicious actor getting into the company's system, according to a data breach notice filed over the incident.

1,237,681 PurFood customers' names or other personally identifiable information, including their social security number, health insurance account numbers, and credit card numbers, including the special security code, was stolen in the breach. Analysts believe the hostile actor might have accessed the client's medical data.

In conclusion – while October 31 gives us temporary fun frights with its ghosts and witches, the terror of cyber breaches through unpatched, weak information systems is terrifying and enduring. Individuals and organizations alike need to prioritize proactive measures and invest in comprehensive cybersecurity strategies. Only through constant vigilance and collaboration can we hope to tame this digital monster that haunts us throughout the whole year.

10 Tasks You You Didn't Know Your IT Team Could Do For You

When you run your own business, there are never enough hours in the day. Even when you start early and end late, there's always something else, another e-mail or task, nagging for your attention. If you want to be productive and ultimately successful, it's crucial to prioritize what tasks you'll allow to fill your schedule. Not everything needs to be or should be done by you.

Easier said than done. One of the issues we frequently see business owners struggle with is delegating the tasks they don't need to do. "It's faster if I just do it," "I can figure it out myself," and "They won't do it like I do" are statements we often hear. That's true for some tasks, and those should stay on your plate. Still, when it comes to IT and technology, there are always several tasks business owners do themselves that they could and should hand off to someone else.

Some are obvious, like security. Quality cyber security requires 24/7 monitoring, and it's unrealistic for busy business owners to be able to handle that effectively. They have too much to do! Another mistake is when they hand it off to an employee, family member, or friend to do for them. These people are typically not qualified to protect you correctly or implement things clearly and consistently.

However, there are dozens of other to-dos that you might need to realize you can hand off to your IT team. Here are 10 tasks you can delegate to your IT team so you can focus on running your business.

1. Providing Tech Support To Employees – No more troubleshooting questions for you! Your team can submit tech tickets for a quick, efficient response from support.

2. Set Up Dual Monitors – Want to increase productivity and efficiency? IT can set up dual monitors, correctly hooking everything up, so your team can come in and start working instead of trying to DIY it.

3. Procuring and Provisioning Devices – If you need laptops, desktops, tablets, mobile devices, etc., sourced for the best price and configured for use, that's a tech team task.

4. Fix or Optimize Wi-Fi – Whether your Wi-Fi is down, you need to extend coverage area or something else, you don't have to crawl around unplugging and plugging in your router. Your IT team can handle get it working well for you.

5. Manage User Access Permissions and Credentials – Your IT team can handle getting new employees their correct user access, immediately revoking access for fired employees or those who quit, and everything in between.

6. Speed Up Computers To Run Efficiently – If your computer is running slow, don't go to Google looking for tips. Call your IT team. They can help you improve your computer speed.

7. Install E-mail/Spam Protection – No more filtering out dangerous or annoying spam e-mails; IT will do it for you.

8. Procuring and Provisioning Devices – If you need laptops, desktops, tablets, mobile devices, etc., sourced for the best price and configured for use, that's a tech team task.

9. Configure Office Equipment – New printer? No problem. IT can help set it up.

10. Employee Screen Monitoring – Are your employees working when they say they are? We can help you find out by setting up software to track activity.

And the list goes on. IT providers can also aid with HIPAA, CMMC, and PCI compliance, file sharing for external/remote access users, data loss recovery plans, office relocation, cabling, and more. Most business owners we consult with are surprised by the number of responsibilities a tech team can take on beyond cyber security.

The best thing to do is book a **FREE Network Assessment**. During this assessment, our team will look at your entire system for areas of opportunity and improvement. We'll conduct a full audit, provide you with a plan of action to optimize your business for productivity, efficiency and security, and answer any questions you have. Click here to book your assessment now.

The Rise of the Bad Bots

While internet bots can offer numerous benefits and streamline various tasks, it is important to acknowledge the risks and challenges associated with their use. Understanding these potential pitfalls is crucial to make informed decisions about implementing and managing internet bots effectively.

One of the main risks of using internet bots is the potential for malicious activities. Bots can be programmed to engage in harmful behaviors such as spreading misinformation, conducting cyber attacks, or engaging in fraudulent activities. This poses a significant threat to individuals, organizations, and online communities.

Another challenge lies in maintaining ethical standards when using internet bots. Ensuring that these automated systems do not violate privacy rights or engage in unethical practices such as spamming or phishing is essential. Striking a balance between automation and respecting user privacy is vital for building trust and maintaining a positive reputation.

Furthermore, there are technical challenges associated with using internet bots effectively. Bots may encounter difficulties navigating complex websites or interacting with certain types of content. Ensuring that bots are appropriately programmed and regularly updated to adapt to changing online environments is crucial for successful implementation.

What are BAD Bots?

Bad bots are automated computer programs capable of high-speed abuse and attacks and mainly have malicious intent, including criminal activities such as fraud or outright theft. Bad bots are commonly and usually deployed on websites, mobile apps, and APIs.

The increasing sophistication of bot attacks and activities has become a significant risk for businesses. Financial losses, compromised accounts, data theft, spam, and even compromised online services are just a few of the consequences a business might experience during any attack that happens.

Indeed, bad bots can significantly affect business owners and may even have disastrous results. Here are a few ways malicious bots can harm businesses:

Loss of revenue: Bad bots can scrape content, steal confidential data, and engage in fraudulent activities that cost firms money. For instance, bots may purchase many tickets or goods, costing the company money and upsetting the actual consumers.

Negative effects on brand reputation: The business's reputation may suffer if bad bots are used to commit fraud or disseminate malicious content. This results in customer frustration and a decline in customer confidence that causes long-term harm to the brand.

Increased server load: Bad bots can put more strain on a website's servers, resulting in slower page loads, poorer website performance, or even a website crash. Again, adding to customer frustration because they can't get through.

Increased security risks: Malicious bots can seek to find and exploit holes in a website's defenses, making it more straightforward for hackers to access the site and steal personal data.

How firms safeguard themselves from malicious bots

Bad bot defense involves a multi-layered strategy that combines technology and behavioral controls. Here are some measures companies can take to protect against malicious bots:

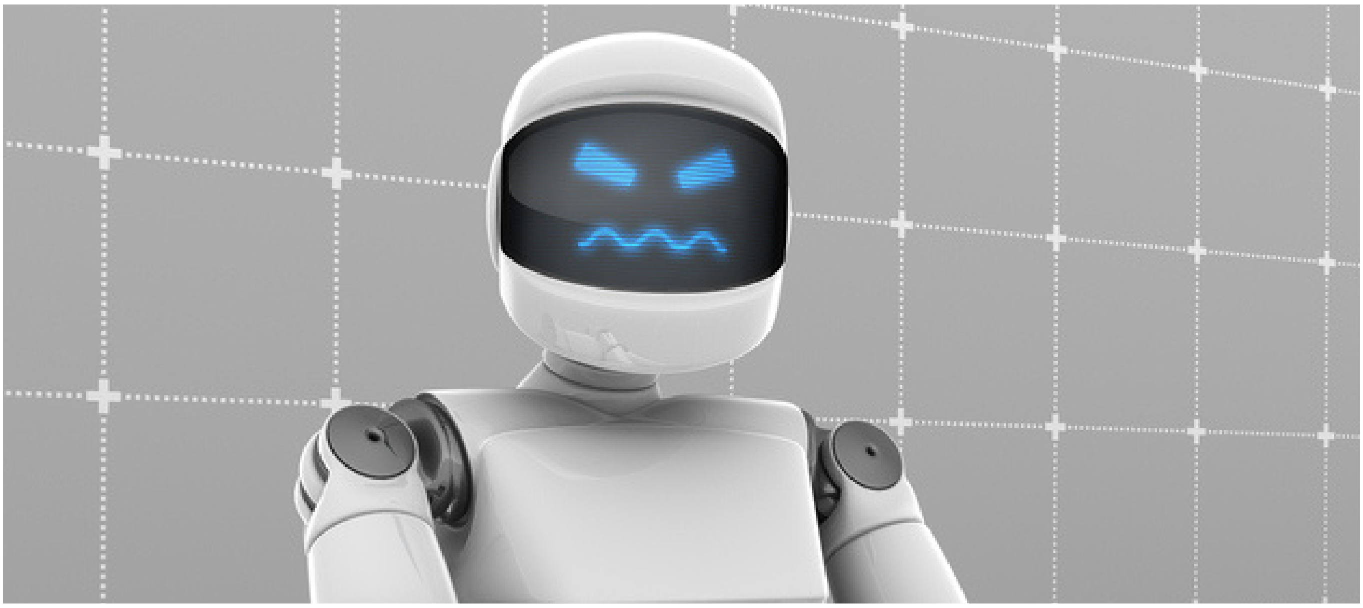
Use bot detection and management software: Bot detection and management tools can detect and block undesirable bots and track website traffic in real time.

Use CAPTCHA: CAPTCHA is a challenge-response system that aids in separating human users from bots. CAPTCHA implementation can assist in lowering the number of malicious bots visiting the website.

Limit the pace of requests: Setting a limit on the number of requests that may be made in a given time frame can assist in stopping bots from taxing the servers of a website.

Update software: Updating software is necessary to avoid vulnerabilities that malicious bots could exploit.

Employee training: Employee training is vital to prevent malicious bots from accessing the website. Teaching employees to spot unusual activity and react appropriately to shut down bot activity early can help considerably.



As AI technology advances, more bots are being developed to assist us in various tasks and interactions. While there are undoubtedly numerous benefits to using these bots, the question of trustworthiness remains a crucial consideration. Can internet bots be trusted to provide a safe, reliable function?

Sure! Like any other tool, internet bots can streamline processes, provide accurate information, and deliver prompt customer service. They can handle repetitive tasks efficiently, freeing human resources for more complex responsibilities. Especially when augmented by AI, bots can quickly analyze vast amounts of data and offer data-driven suggestions that humans might overlook.

However, it is crucial to recognize that even bots have limitations. They lack the human emotions and intuition often required for empathetic interactions or understanding nuanced situations. Trusting them unquestioningly without human oversight could lead to errors or misinterpretations.

Ultimately, the level of trust we place in bots should be based on careful evaluation of their capabilities, reliability, and adherence to ethical standards. While they can enhance our daily experiences and productivity when used appropriately, it is essential to maintain a balance between automation and human involvement to mitigate risks and ensure desired outcomes.

By understanding their limitations and implementing proper oversight mechanisms alongside ethical guidelines during bot development, we can continue leveraging their benefits while maintaining control over crucial aspects of decision-making and ensuring ethical practices are upheld.

Cyber Security October 2023:
It's easy to stay safe online

As technology continues to advance at a rapid pace, so does the importance of cyber security. In an ever-connected world, safeguarding our digital presence has become more vital than ever before. That's why Cyber Security Month 2023 aims to shed light on the topic and assure individuals that staying safe online is in fact easy.

In this day and age, we rely heavily on the internet for various aspects of our lives - from banking and shopping to socializing and entertainment. While these advancements have made our lives more convenient, they have also opened up new opportunities for cybercriminals to exploit vulnerabilities and gain unauthorized access to personal information.

The overarching goal of Cyber Security Month 2023 is to empower individuals with knowledge and resources that will enable them to protect themselves online without feeling overwhelmed or intimidated by complex technology jargon. The theme, "It's easy to stay safe online," emphasizes the notion that implementing essential security measures can be straightforward and manageable for everyone.

Throughout Cyber Security Month 2023, individuals will have access to a wealth of information on best practices, practical tips, and user-friendly tools designed specifically with their online safety in mind. By adopting simple habits such as using strong passwords, regularly updating software, enabling two-factor authentication, and being cautious of suspicious links or emails - anyon0065 can significantly enhance their security posture in the digital realm.

Furthermore, Cyber Security Month 2023 aims not only at individual empowerment but also at fostering a culture of cybersecurity awareness within organizations and communities at large. By encouraging open discussions about potential risks, promoting employee training programs in cybersecurity protocols, and implementing robust security measures across networks - we can collectively create a safer digital environment for all.

Here is a closer look at the four essential processes with simple action items and an added assignment to assist you in safeguarding your identity this year.

1. Use Multi-factor Authenticator

Enable multi-factor authentication on your accounts for one of the quickest and simplest methods to keep safe online. You only need to complete this easy step once, and it only takes a few minutes per account. Once it's set up, hackers will find it twice as difficult to access your accounts.

What exactly is MFA (multi-factor authentication)? This commonly used technique, also referred to as two-factor authentication, secures your accounts by needing two pieces of information to log in.

Entering your password and then entering a one-time code delivered to your email address or smartphone is a typical example of two-factor authentication.

Two-factor authentication, sometimes known as 2FA, may also use additional steps, such as:

- a safety inquiry, such as "Who was the name of your favorite teacher?"
- an identifiable biometric feature, like your face or fingerprint.
- a temporary passcode you receive from an authenticator app.

Multi-factor authentication is normally enabled by going to an account, selecting settings, and selecting security. When necessary, such as your phone number or email address where you want a code sent, you then toggle multi-factor authentication to "on".

2. Improve your password practices

Use a password manager and strong passwords as another top priority for internet safety. If you have a password that is simple to remember, there is a good possibility that a hacker may use a program to guess it and gain access to your online kingdom quickly.

Cyber Security October 2023: It's easy to stay safe online continued.

A secure password ought to be:

- With capital and lowercase characters, numerals, and symbols, complex
- At least 16 characters long to make it far more difficult to crack
- Fake words avoiding personal information like names or birthdays

However, the same qualities that make passwords challenging to guess also make them challenging to remember. Password managers are a very useful tool because of this.

Password managers may let you create strong passwords on demand, keep track of all your passwords in a safe online vault, and even protect other sensitive data like your credit card details. When you log into a website, they can swiftly and conveniently auto-fill your passwords for you.

3. Immediately update your resume

One of the most straightforward and crucial things you can do to stay safe online is to keep your software updated. This is because software updates frequently close security vulnerabilities or bugs that hackers can use to access your data, infect your device with malware or ransomware, or even remotely control your machine.

As soon as you receive an alert that an update is available, update your software. Make it a practice to perform software upgrades straight away rather than delaying them.

Both your device's operating system and its apps should be updated often. Regular updates will not only protect your privacy and keep you safe online, but they'll also repair bugs and make your devices operate more efficiently.

4. Watch Out For Phishing Scams

A phishing scam occurs when a hacker sends you a phony email, direct message, text message, or even pop-up advertisement to coerce you into doing an action like clicking a link, responding with personal information, or sending money. A phishing message may be artfully crafted to appear to be a genuine message from a well-known company, like your bank.

The sophistication of phishing scams used by cybercriminals has led to the creation of numerous phishing tactics with distinctive names. For instance, "whaling" targets a large fish like the CEO of a corporation whereas "spear phishing" targets a specific person or role in an organization instead of a group.

Phishing scams can be avoided to a large extent by becoming familiar with the telltale symptoms of phishing and learning to pause and consider your response before acting on an email or other message. The following are some indicators of a phishing attack:

concerning an account, alarming "news".

- attachments that seem strange.

not addressing you by name.

- spelling or grammar mistakes.
- offers for free electronics, vacations, or other valuable stuff.
- language and grammar usage that seems somewhat "off."
- To click a link or perform an urgent action

In conclusion, Cyber Security Month 2023 seeks to dispel any myths surrounding online safety while providing accessible tools and knowledge necessary for individuals to protect themselves effectively.We can empower individuals and business leaders to navigate the digital landscape with confidence and peace of mind. Book a FREE 10-minute call with us to get your ***FREE Cybersecurity Assessment.***

Prospect Street Studio: Your E-commerce Photography Expert!

The images you choose to represent your business can effectively convey important messages about your brand identity, storytelling, and overall aesthetic. Whether on your website, social media platforms, or marketing materials, visually appealing imagery can capture attention and evoke emotions. Furthermore, well-crafted visuals can enhance the professionalism and credibility of your brand. High-quality images aligned with your branding guidelines showcase attention to detail and signify a commitment to excellence. Conversely, low-quality or inconsistent imagery can create an unfavorable impression and lead potential customers to question the quality of your products or services.

Moreover, choosing the right images can help you establish a connection with your target audience. By selecting visuals that resonate with their aspirations, desires, or values, you demonstrate an understanding of their needs. This emotional connection fosters trust and loyalty towards your brand.

And this is what Carrington Crothers – the owner of Prospect Street Studio specializes in. Prospect Street Studio is a brand photography agency located in Worcester, MA, that specializes in amplifying brands by helping product and service-based businesses create imagery that directly impacts their business.

Prospect Street Studio agency mainly focuses on e-commerce brands in the Consumer Packaged Goods (CPG) industry to strategically improve the visual presence and brand visibility, increase conversation rates, and minimize returns by delivering accurate and professional product photography. The ultimate goal is to understand the brand's purpose, build customer trust, and positively impact business organizations.

Carrington's inspiration to work in the creative industry comes from the passion and the support of the amazing people, businesses, and brands she worked with.

> ***"Being able to help brands create imagery that has a positive impact on their business and customers is an amazing process to watch and to have a hand in."***

Her expertise and professional background help many businesses reach their maximum potential and be more visible and credible, fostering loyalty and long-term relationships.

Businesses must invest time and resources into selecting imagery that accurately reflects their unique selling proposition and resonates with their target audience. Professional photography or graphic design services may be worth considering to create impactful visuals that effectively communicate the essence of your business and leave a lasting impression on potential customers.

Remember: when it comes to visual communication in today's fast-paced world, exceptional imagery is vital in conveying the essence of your brand - make sure it speaks volumes about your business or brand by investing in compelling visuals that genuinely reflect who you are.

Want to know more about leveraging your brand and business through imagery? Contact Carrington and her fantastic team via email at ***info@prospectstreetstudio.com*** or call her at ***508-731-4003***.

Prospect Street Studio