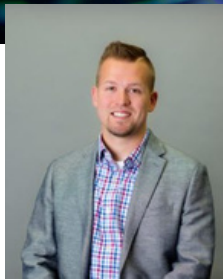


TECH BYTES

September 2024

Stay ahead with our monthly tech and cybersecurity updates. Innovations, tips, and more—stay informed and secure!



Keep yourself informed about the newest advancements and trends in technology.

Matthew DeWees
-President

Enhancing your business with advanced AI is like installing a high-performance engine. However, security must be a priority from the start. Just as you wouldn't install a new door without a lock, don't integrate AI without ensuring security.

Upgrading opens new data access points, which can be vulnerable to cyber threats. Before implementing AI, secure your systems with robust data storage, strict access controls, and continuous monitoring. Remember, a secure AI upgrade is a truly powerful upgrade!

Need some help? Reach out to us at everythingit@virtualdataworks.com to schedule a chat.

Until then, stay safe,



President - Virtual DataWorks

WHAT'S INSIDE?

02 AI DATA BREACHES ARE RISING!

03 AUTOMATION FOR SMALL ENTERPRISES

04 THE TRUE PRICE OF IT DOWNTIME

05 THE TANGIBLE VALUE OF CYBERSECURITY

06 ADDRESSING THE DANGER OF BROWSER EXTENSIONS


07 BEWARE OF DEEPPFAKES


DID YOU KNOW?

The first webcam was set up at the University of Cambridge to keep an eye on a coffee pot, saving researchers from pointless trips to an empty pot!

Virtual DataWorks

 475 Wolf Ledges Parkway Akron, Ohio 44311

 virtualdataworks.com

 (330)800-2186

02

AI DATA BREACHES ARE RISING: HERE'S HOW TO PROTECT YOUR COMPANY!

In this digital age, the integration of artificial intelligence (AI) into our business operations is no longer a novelty but a necessity. However, this advancement comes with its own set of challenges, particularly the increasing threat of AI data breaches. A recent study has brought to light a concerning trend: an astonishing 77% of businesses have reported breaches in their AI systems within the last year

The Growing Concern Over AI Data Breaches

AI systems are akin to a gold mine for cybercriminals due to the sensitive data they hold. The intrinsic requirement of AI to process and analyze large datasets not only fuels its capabilities but also broadens the potential for security vulnerabilities. As AI technologies advance, the methods employed by cybercriminals to exploit these systems become increasingly sophisticated and harder to detect.

Why Are AI Data Breaches on the Rise?

Several factors contribute to the heightened risk of AI data breaches: or years to come.



The expanding attack surface

With the rapid adoption of AI, the number of potential entry points for cybercriminals has multiplied.

Greater damage potential: AI-enhanced phishing attacks can cause more significant harm, leading to substantial data breaches with severe repercussions

Safeguarding Your Company

To combat these threats, companies must adopt a proactive and comprehensive approach to cybersecurity:

- **Be Skeptical:** Approach unsolicited messages with caution. Refrain from engaging with links or attachments from unknown sources.
- **Red Flag Awareness:** Stay alert for signs of phishing attempts. Offers that appear too good to be true often are.
- **Continuous Education:** Keep abreast of the latest AI phishing tactics and educate your team on how to counter them.

The Cost of Complacency

Overlooking the risks associated with AI data breaches can lead to severe repercussions for any business. The immediate financial losses are just the tip of the iceberg. A breach can significantly damage customer trust, drawing the attention of regulatory bodies, disrupting daily operations, and tarnishing the company's reputation for an extended period.

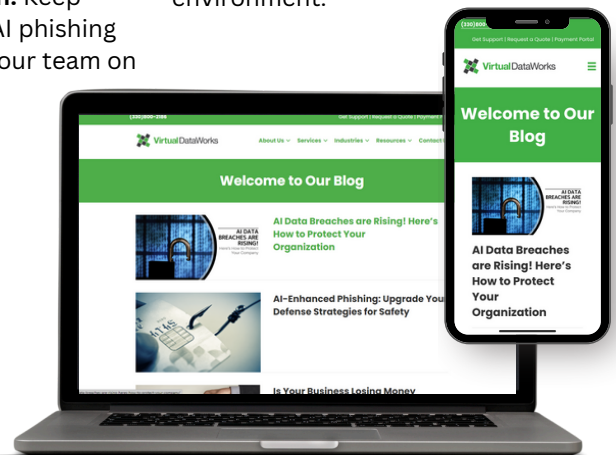
In summary, as AI continues to revolutionize the business landscape, the necessity of robust cybersecurity measures cannot be emphasized enough. By staying vigilant, informed, and proactive, businesses can effectively navigate the complexities of AI data breaches and safeguard their digital future. Investing in advanced security protocols, regular audits, and employee training can help mitigate these risks and ensure a resilient and secure operational environment.

Check Out Our Tech Blogs!

Discover More!



www.virtualdataworks.com



STREAMLINING SUCCESS: A GUIDE TO TASK AUTOMATION FOR SMALL ENTERPRISES

Running a small business is a whirlwind. You juggle a million tasks and wear countless hats. You also constantly fight the clock. What if you could reclaim some of that precious time?

Enter task automation. It's your secret weapon for streamlining your workflow and boosting productivity. By automating routine and repetitive tasks, small businesses can gain many benefits such as freeing up valuable time and resources. Every minute saved can translate to increased productivity and profitability.

What is Task Automation?

Task automation involves using technology to automate repetitive, manual tasks. Imagine software handling data entry, scheduling appointments, or sending out invoices. All this without your constant oversight. This frees you up to focus on strategic initiatives that drive growth.

88% of small business owners say that automation helps them compete with larger companies.

What Tasks Can You Automate?

You can automate many tasks across different departments in a small business. Here are some examples:

- **Marketing:** Schedule social media posts and send automated email campaigns. You can also generate personalized marketing materials.
- **Sales:** Generate quotes and send automated follow-up emails. Track sales performance through automated reports.
- **Customer Service:** Set up chatbots to answer frequently asked questions. Automate email responses for order confirmations. Have automation manage appointment scheduling.

- **Human Resources:** Automate payroll processing and manage employee onboarding tasks. Send out automated reminders for performance reviews.
- **Finance:** Automate data entry for invoices and receipts. Schedule recurring payments and generate automated financial reports.

Getting Started with Task Automation:

Identify Repetitive Tasks.

Analyze your daily workflows and pinpoint repetitive tasks. Ask employees what manual tasks take them the most time.

Choose the Right Tools.

There's a vast array of automation tools available. You'll find everything from simple scheduling apps to complex management platforms. Research and choose tools that integrate seamlessly with your existing software.

Start Small.

Don't try to automate everything at once. Begin by automating a few key tasks and gradually expand as you get comfortable.

Invest in Training.

Provide your team with proper training. You want them to feel comfortable integrating them into their workflow.

The Future of Automation for Small Businesses

Automation technology will continue to evolve. Small businesses will have access to even more powerful tools to boost productivity. Automating now gets you ahead of the competition.

04 UNMASKING THE TRUE PRICE OF IT DOWNTIME

Imagine this: you walk into your office on a busy Monday morning, ready to tackle the week. But something's wrong. Computers are unresponsive. Phones are silent. The internet is a ghost town. Your business has come to a grinding halt – victim of an IT outage.

It's a scenario every business owner fears. But beyond the initial frustration are expenses you may not immediately see. IT downtime carries hidden costs that can significantly impact your bottom line. Let's peel back the layers and expose the true price of IT outages.

The Immediate Impact: Lost Productivity

When IT systems go down, your employees are effectively sidelined. Sales can't be processed. Emails pile up unanswered.

Customer Impact: Frustration and Lost Trust

An IT outage isn't just an internal inconvenience. It directly impacts your customers. Frustrated customers can't place orders or access their accounts.

Reputational Damage: A Hit to Your Brand Image

IT outages can tarnish your brand image. Customers expect businesses to be reliable and accessible.

Hidden Costs: Beyond the Obvious

The financial impact of IT downtime extends beyond lost productivity and sales. It includes:

- Employee Demoralization
- Emergency Repairs
- Data Loss or Corruption
- Compliance Issues

Investing in Uptime: Building Business Resilience

IT downtime is a threat every business faces. By understanding the true cost and taking proactive measures, you can reduce the risk. Remember, downtime has the potential to damage your reputation and customer relationships.

So, focus on IT security and invest in preventative measures. Every minute counts when it comes to technology.

05 THE TANGIBLE VALUE OF CYBERSECURITY

Cybersecurity is essential for safeguarding a company's digital assets. Here's why it's a smart investment:

- **Risk Mitigation:** Strong cybersecurity reduces the likelihood of data breaches, protecting sensitive information.
- **Cost Savings:** Preventing cyber attacks can save a company from hefty fines, legal fees, and loss of business.
- **Trust and Compliance:** Adhering to regulations like GDPR not only avoids penalties but also builds customer trust.
- **Business Continuity:** Effective incident response ensures operations can quickly resume after an attack, minimizing downtime.

07 BEWARE OF DEEPFAKES

Deepfakes are a growing concern in the professional world due to their potential to deceive and manipulate. Here's a condensed version with bullet points:

- **AI-Generated Deception:** Deepfakes use AI to create realistic but fake media.
- **Security Risks:** They challenge sectors like security and privacy.
- **Need for Awareness:** Organizations should educate staff on deepfake risks.

06 ADDRESSING THE DANGER OF BROWSER EXTENSIONS

Addressing the dangers of browser extensions is crucial for online security. Here are some key points to consider:

- **Privacy Risks:** Extensions can access sensitive data, leading to privacy intrusions.
- **Performance Issues:** Poorly coded extensions can slow down or crash browsers.
- **Malicious Extensions:** Some may contain harmful code for financial gain or other malicious purposes.

To mitigate these risks, only download extensions from official marketplaces and stay informed about the latest security practices.

By following these guidelines, you can significantly reduce the risks posed by browser extensions and maintain a safer browsing experience.

- **Verification Measures:** Implementing checks is key to prevent deception.
- **Detection Tools:** Using advanced tools can help spot and stop deepfakes.

By proactively addressing these concerns, professionals can contribute to the creation of a secure and trustworthy digital environment. It is through informed vigilance that we can collectively combat the deceptive potential of deepfake technology.



Managed IT

FOCUS ON YOUR BUSINESS WHILE WE MANAGE YOUR NETWORK.

At Virtual DataWorks, we leverage technology to enhance your business. With our Managed IT Services, we handle your IT needs, allowing you to focus on your customers. Our aim is to be your trusted partner, ensuring your technology works seamlessly for you.

UNLOCK A BETTER BUSINESS



Managed Voice

TAKE YOUR COMMUNICATION TO THE NEXT LEVEL

We aim to meet the demands of modern business communication and collaboration with our reliable, feature-rich, and competitive cloud solutions.

SOLUTIONS THAT MATTER



Managed Cloud

EMBRACE THE CLOUD AND ITS BENEFITS FOR YOUR ORGANIZATION.

New to the cloud? Let us guide you to the right solution. Whether it's Office 365, SharePoint, Azure, Amazon, or another provider, our expert team is here to assist.

EMBRACE THE CLOUD