Virtual DataWorks

TECH BYTES

December 2024

Stay informed and secure with our monthly tech and cybersecurity updates. Get the latest innovations, tips, and more!

Keep up with the newest advancements and trends in technology.

Matthew DeWees
-President

Integrating advanced AI into your business 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,

Matthew DeWees

President - Virtual DataWorks

WHAT'S INSIDE?

DID YOU KNOW?

The first computer virus, the "Creeper virus," was created in 1971. It displayed the message, "I'm the creeper, catch me if you can!" This experiment led to modern cybersecurity measures.

Virtual DataWorks

475 Wolf Ledges Parkway
Akron, Ohio 44311

virtualdataworks.com

(330) 800-2186

02 WATCH OUT - “MALVERTISING” IS ON THE RISE!

There are many types of malware. One of the most common is called “malvertising.” It crops up everywhere. You can also see these malicious ads on Google searches.

Two things are making malvertising even more dangerous. One is that hackers use AI to make it very believable. The other is that it’s on the rise, according to Malwarebytes. In the fall of 2023, malvertising increased by 42% month over month.

Below, we’ll help you understand malvertising and give you tips on identifying and avoiding it.

What Is “Malvertising?”

Malvertising is the use of online ads for malicious activities. One example is when the PlayStation 5 was first released. It was very hard to get, which created the perfect environment for hackers. Several malicious ads cropped up on Google searches. The ads made it look like someone was going to an official site. Instead, they went to copycat sites. Criminals design these sites to steal user credentials and credit card details.

Google attempts to police its ads but hackers can have their ads running for hours or days before they’re caught. These ads appear just as any other sponsored search ad. It can also appear on well- known sites that have been hacked or on social media feeds.

Tips for Protecting Yourself from Malicious Online Ads

Review URLs Carefully

You might see a slight misspelling in an online ad’s URL. Just like phishing, malvertising often relies on copycat websites. Carefully review any links for things that look off.

Visit Websites Directly

A foolproof way to protect yourself is not to click any ads. Instead, go to the brand’s website directly. If they truly are having a “big sale,” you should see it there. Just don’t click those links and go to the source directly.

Use a DNS Filter

A DNS filter protects you from mistaken clicks. It will redirect your browser to a warning page if it detects danger. DNS filters look for warning signs. This can keep you safe even if you accidentally click a malvertising link.

Do Not Log in After Clicking an Ad

Malvertising will often land you on a copycat site. The login page may look identical to the real thing. One of the things phishers are trying to steal is login credentials.

If you click an ad, do not input your login credentials on the site, even if the site looks legitimate. Go to the brand’s site in a different browser tab.

Don’t Call Suspicious Ad Phone Numbers

Phishing can also happen offline. Some malicious ads include phone numbers to call. Unsuspecting victims may not realize fake representatives are part of these scams. Seniors are often targeted; they call and reveal personal information to the person on the other end of the line.

Stay away from these ads. If you find yourself on a call, do not reveal any personal data.

Don’t Download Directly from Ads

“Get a free copy of MS Word” or “Get a Free PC Cleaner.” These are common malvertising scams. They try to entice you into clicking a download link. It’s often for a popular program or freebie. The link actually injects your system with malware to do further damage.

A direct download link is likely a scam. Only download from websites you trust.

Warn Others When You See Malvertising

If you see a suspicious ad, warn others. This helps keep your colleagues, friends, and family more secure. If unsure, do a Google search. You’ll often run across scam alerts confirming your suspicion.

It’s important to arm yourself and others with this kind of knowledge. Foster a culture of cyber-awareness to ensure safety and better online security.

Your Technical Success Experts

We leverage technology to positively impact your business!

- ✓ Reliability and Customer Service
- ✓ Total Data Protection
- ✓ Business Continuity
- ✓ A Range of IT Services

Contact us

(330) 800-2186

VirtualDataWorks

☎ (330)800-2186

virtualdataworks.com

03 STATE OF AI AT WORK

The pace of technological advancement is accelerating, especially with AI at the forefront. Companies are rapidly adopting AI solutions, and software providers like Microsoft are integrating AI into their tools to:

- Streamline operations
- Automate tasks
- Reduce errors
- Boost business output

The 2024 Work Trend Index by Microsoft and LinkedIn provides insights into AI's impact on the workplace.

Here are some key trends:

Employees Want and Expect AI at Work

75% of knowledge workers now use AI at work. Companies need to adopt AI to attract and retain top talent. Partnering with employees to understand how AI can help them is crucial.

AI Skills are in Demand

New roles like "prompt engineer" highlight the growing need for AI expertise. Companies are actively seeking AI-skilled staff, with 55% of leaders concerned about talent shortages. Employers should prioritize AI training programs to upskill their teams. Investing in AI education ensures the workforce can leverage AI technologies effectively, driving innovation and maintaining a competitive edge.

The Evolving Role of Employees Using AI

There's a notable divide between AI skeptics and power users. Power users save over 30 minutes daily by optimizing tasks with AI tools. They can train colleagues and develop templates for others to follow. Harnessing their expertise enhances productivity and ensures all employees benefit from AI advancements.

The Need for an AI Use Policy

Without a clear AI use policy, employees might resort to using unapproved AI tools, which can pose significant risks. These risks include data breaches, compliance issues, and inconsistent AI application across the organization. To mitigate these risks, companies should create comprehensive guidelines that outline acceptable AI use, specify approved tools, and detail the processes for integrating AI into workflows.

Additionally, it's crucial to provide training on these guidelines to ensure all employees understand and adhere to them. Seeking expert guidance from IT providers can help in developing and implementing these policies effectively, ensuring that AI is used safely and responsibly within the organization.

Final Thoughts on AI in the Workplace

Understanding and embracing AI trends can unlock new opportunities, enhance productivity, and improve employee satisfaction. We can help you navigate AI complexities and leverage its potential to drive your business forward.

Ethical Considerations and Trust in AI

Transparency, privacy, and bias mitigation are essential for ethical AI deployment. Businesses must communicate clearly with employees and customers about AI use to build trust and ensure responsible practices.

04 8 STEPS TO TAKE WHEN YOU GET A DATA BREACH NOTICE

When it happens, you feel powerless. You get an email or letter from a business saying someone breached your data. It happens all too often today.

A business getting hacked is something you have little control over. But you can take important steps afterwards. We've outlined the most important things to do below. These steps can help you mitigate the financial losses.

Change Your Passwords.

The very first thing you should do is change your passwords. Change the password for the service that sent you the breach notification first. Then, change it for any logins using the same password.

Enable multifactor authentication (MFA) for breached services and all other logins. MFA, also known as two-factor authentication or two-step verification, keeps accounts secure even if passwords are stolen.

Common forms of MFA are:

- Text message
- Authentication app
- Security key

Carefully Review the Breach Notification
It's important to understand exactly how the data breach may impact you. Review the notice you received. Additionally, look for updates on the company website.

These are the things you should be looking for:

- The type of data exposed (passwords, card numbers, etc.)
- What reparations the company is making (e.g., credit monitoring)
- Any instructions given to secure your account

Get Good Cybersecurity Protections. There are some simple tools you can use to beef up personal device security. These include:

- A good antivirus/anti-malware program
- DNS filtering to block malicious sites
- Email spam filtering for phishing

Contact us today to schedule a chat about device security.

05 BEST PRACTICES FOR EVENT LOGGING

The Importance of Event Logging in Cybersecurity Businesses face a growing wave of cyberattacks, from ransomware to phishing schemes. A strong cybersecurity strategy is essential, and event logging is a crucial component.

What is Event Logging?

Event logging tracks activities within your IT systems, such as:

- Login attempts
- File access
- Software installs
- Network traffic
- Denial of access
- System changes
- By adding timestamps, you get a clear picture of your IT ecosystem, allowing you to detect and respond to threats promptly.

Why Track and Log Events?

- Detect suspicious activity: Monitor user behavior and system events.
- Respond quickly to incidents: Provide a clear record of breaches.
- Meet regulations: Maintain accurate records of system activities.
- Best Practices for Effective Event Logging
- Log What Matters Most

Focus on critical events.

Logins and Logouts: Track access times.
Accessing Sensitive Data: Monitor file and database access.
System Changes: Record software installations and updates.

Centralize Your Logs

Respond faster: Access all evidence quickly.
Get a complete picture: Identify vulnerabilities.
Ensure Logs Are Tamper-Proof
Protect your logs:

Encrypt logs: Make them unreadable to unauthorized users.
Use WORM (Write Once Read Many) storage: Prevent changes or deletions.
Use strong access controls: Limit log access to trusted personnel.

Establish Log Retention Policies
Balance log retention to meet compliance and business needs without overwhelming storage:

- Compliance requirements: Follow industry-specific rules.
- Business needs: Retain logs for incident investigation and auditing.
- Storage capacity: Ensure your policy doesn't overwhelm storage.

Check Logs Regularly
Regularly review logs to spot anomalies and respond to threats:

- Set up automated alerts: Get notified of critical events.
- Perform periodic reviews: Look for patterns indicating threats.
- Correlate events: Use SIEM to connect different activities and reveal complex attacks.

Need Help with Event Logging Solutions? Virtual DataWorks can help you implement these practices and ensure your business stays protected.

VirtualDataWorks

IT TECHNOLOGY AND SOLUTION SERVICE

In today's fast-paced digital world, staying ahead means having the right technology and solutions at your fingertips.

Our Service Include:

- ✓ Cloud Solutions
- ✓ IT Consulting
- ✓ Voice Solutions
- ✓ Managed IT Services

☎ Call Number:
(330)800-2186

Contact Us: