TECH BYTES

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Reach out to us for a concise, no-pressure conversation. Discover the ways we can assist in strengthening your data security and fully leveraging your technological capabilities.

- Matthew Dewees
President

GOOGLE & YAHOO'S NEW DMARC POLICY - WHY BUSINESSES NEED EMAIL AUTHENTICATION

Have you been hearing more about email authentication lately? There is a reason for that. It's the prevalence of phishing as a major security threat. Phishing continues as the main cause of data breaches and security incidents. This has been the case for many years.

A major shift in the email landscape is happening. The reason is to combat phishing scams. Email authentication is becoming a requirement for email service providers. It's crucial to your online presence and communication to pay attention to this shift.

Google and Yahoo are two of the world's largest email providers. They have implemented a new DMARC policy that took effect in February 2024. This policy essentially makes email authentication essential. It's targeted at businesses sending emails through Gmail and Yahoo Mail.

But what's DMARC, and why is it suddenly so important?

The Email Spoofing Problem

Imagine receiving an email seemingly from your bank. It requests urgent action. You click a link, enter your details, and boom – your information is compromised. The common name for this is email spoofing.

It's where scammers disguise their email addresses. They try to appear as legitimate individuals or organizations. Scammers spoof a business's email address. Then they email customers and vendors pretending to be that business.

These deceptive tactics can have devastating consequences on companies. These include:

- Financial losses
- Reputational damage
- Data breaches
- Loss of future business

Unfortunately, email spoofing is a growing problem. It makes email authentication a critical defense measure.

What is Email Authentication?

Email authentication is a way of verifying that your email is legitimate. This includes verifying the server sending the email. It also includes reporting back unauthorized uses of a company domain.

Email authentication uses three key protocols, and each has a specific job:

- SPF (Sender Policy Framework): Records the IP addresses authorized to send email for a domain.
- DKIM (DomainKeys Identified Mail): Allows domain owners to digitally "sign" emails, verifying legitimacy.

- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Gives instructions to a receiving email server including, what to do with the results of an SPF and DKIM check. It also alerts domain owners that their domain is being spoofed.

SPF and DKIM are protective steps. DMARC provides information critical to security enforcement. It helps keep scammers from using your domain name in spoofing attempts.

Why Google & Yahoo's New DMARC Policy Matters

Both Google and Yahoo have offered some level of spam filtering but didn't strictly enforce DMARC policies.

- Starting in February 2024, the new rule took place. Businesses sending over 5,000 emails daily must have DMARC implemented.
- Both companies also have policies for those sending fewer emails. These relate to SPF and DKIM authentication.

Look for email authentication requirements to continue. You need to pay attention to ensure the smooth delivery of your business email.

The Benefits of Implementing DMARC:

- Protects your brand reputation
- Improves email deliverability
- Provides valuable insights
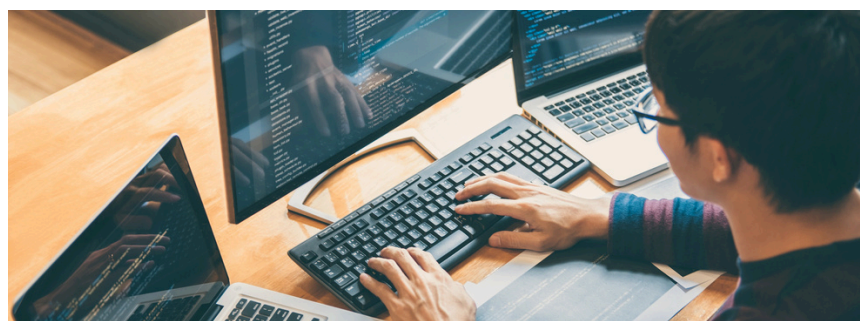
Why Should Your Company Outsource IT?

IT service providers deliver the technical expertise small businesses need at a much lower cost than hiring IT staff. They can recommend, install, and manage technology according to business' objectives and core competencies and ensure that critical data is safe.

Learn More!

BEWARE OF DEEPFAKES! LEARN TO SPOT THE DIFFERENT TYPES

Have you ever seen a video of your favorite celebrity saying something outrageous? Then later, you find out it was completely fabricated?

Welcome to the world of deepfakes. This is a rapidly evolving technology that uses artificial intelligence to create synthetic media. They can appear real but are actually manipulated. Bad actors can use deepfakes to spread misinformation. They are also used in phishing attacks.

So, what are the different types of deepfakes, and how can you spot them?

FACE-SWAPPING DEEPFAKES

This is the most common type. Here, the face of one person is seamlessly superimposed onto another's body in a video.

Here's how to spot them:

- **Look for inconsistencies:** Pay close attention to lighting, skin tones, and facial expressions. Look for subtle glitches.
- **Check the source:** Where did you encounter the video? Be cautious of unverified sources and unknown channels.
- **Listen closely:** Does the voice sound natural? Incongruences in voice tone, pitch, or accent can be giveaways.

DEEPFAKE AUDIO

This type involves generating synthetic voice recordings. They mimic a specific person's speech patterns and intonations. Scammers can use these to create fake audio messages.

Here's how to spot them:

- **Focus on the audio quality:** Deepfake audio can sound slightly robotic or unnatural. Pay attention to unusual pauses or a strange emphasis.
- **Compare the content:** Does the content of the audio message align with what the person would say? Consider if the content seems out of character or contradicts known facts.
- **Seek verification:** Is there any independent evidence to support the claims made? If not, approach it with healthy skepticism.

TEXT-BASED DEEPFAKES

This is an emerging type of deepfake. It uses AI to generate written content such as social media posts, articles, or emails. They mimic the writing style of a specific person or publication. These can be particularly dangerous.

Here's how to spot them:

- **Read critically:** Pay attention to the writing style, vocabulary, and tone.
- **Check factual accuracy:** Verify the information presented in the text against reliable sources.
- **Be wary of emotional triggers:** Be cautious of content that evokes strong emotions.

DEEPFAKE VIDEOS WITH OBJECT MANIPULATION

This type uses AI to manipulate objects within real video footage.

Here's how to spot them:

- **Observe physics and movement:** Pay attention to how objects move in the video.
- **Seek original footage:** If possible, try to find the original source of the video footage.

ENSURING THE SECURITY OF THE ANYWHERE ORGANIZATION.

Remote working is here to stay: Securing organizations in an increasingly virtual landscape requires IT teams to protect users and resources regardless of their location. As bad actors find new and more sophisticated ways to infiltrate, the need for robust security measures becomes paramount.

1. Enable secure connectivity for users to access resources seamlessly from any location, be it their homes, on-site, or in the office.

2. Ensure comprehensive protection for all devices used to establish connections, including desktops, laptops, mobile phones, and tablets.

3. Safeguard the data and workloads that users require access to, whether they are stored in the cloud or on your local network.

4. Simplify management tasks, allowing IT teams to efficiently oversee distributed organizations from any location without adding to their workload.

Fortunately, Sophos offers comprehensive support in all these areas and has partnered with Virtual DataWorks to meet all your security requirements!

SECURE YOUR NETWORK

Secure cloud-based and on-premises networks

Request A Quote

Request Network Assessment

5 DATA SECURITY TRENDS TO PREPARE FOR IN 2024

With cyber threats evolving at an alarming pace, staying ahead of the curve is crucial. It's a must for safeguarding sensitive information.

Data security threats are becoming more sophisticated and prevalent. The landscape must change to keep up.

Here are some key areas to watch.

1. The Rise of the Machines: AI and Machine Learning in Security

2. Battling the Ever-Evolving Threat: Ransomware

3. Shifting Strategies: Earlier Data Governance and Security Action

4. Building a Fortress: Zero Trust Security and Multi-Factor Authentication

5. When Things Get Personal: Biometric Data Protection

READ MORE

HOW TO PROPERLY DEPLOY IOT ON A BUSINESS NETWORK

The Internet of Things (IoT) is no longer a futuristic concept. It's rapidly transforming industries and reshaping how businesses operate. IoT is a blanket term to describe smart devices that are internet enabled. One example is smart sensors monitoring production lines. Connected thermostats optimizing energy consumption is another.

Here are the steps you need to properly deploy IoT on a Business Network:

- **Step 1:** Define Your Goals and Needs
- **Step 2:** Select the Right Devices and Network Infrastructure
- **Step 3:** Focus on Security Throughout the Journey
- **Step 4:** Deployment and Ongoing Management
- **Step 5:** Continuous Learning and Improvement

INTRODUCING THE NEW MICROSOFT PLANNER

Calendars, task lists, and project planning are important business tools. Many people use Microsoft's apps to power these processes including Planner, Microsoft To Do, and Project for the web.

These tools help keep processes on track and enable task accountability. But they're separate apps. Switching between apps can be cumbersome. It adds more complexity to a workflow.

On average, employees switch between 22 different apps 350 times per day. This puts a big dent in productivity and efficiency.

Microsoft is working to solve that. It is rolling out a brand-new version of Microsoft Planner in 2024. The new Planner is packed with exciting features designed to simplify your project management journey. Here are some of the key features:

- Combines the functions of Planner, To Do, and Project for the web
- Enhanced Collaboration
- AI-Powered Insights with Copilot
- Scaling with Your Needs
- Pre-Built Templates
- Integrates with Teams, Power BI, Viva, and more