

THE TECH CHRONICLE

February 2024

www.centrend.com

Friday

WHAT'S INSIDE?

P1 MASTERING EMAIL DELIVERY IN 2024: BEST PRACTICES FOR GOOGLE AND YAHOO'S NEW REQUIREMENTS

P1 BEST PRACTICES TO 'CELEBRATE' NATIONAL CHANGE YOUR PASSWORD DAY: HOW DOES YOUR PASSWORD STACK UP?

P4 SECURING YOUR SMARTPHONE: A STEP-BY-STEP GUIDE AGAINST MOBILE ATTACKS

P5 HOW PARTNERING WITH AN IT MANAGED SERVICES PROVIDER (MSP) ELEVATES YOUR BUSINESS

P6 NAVIGATING THE TRANSITION: QUICKBOOKS DESKTOP PLANS TO CEASE NEW U.S. SUBSCRIPTIONS



Mastering Email Delivery in 2024: Best Practices for Google and Yahoo's New Requirements

In today's digital age, email has become a crucial channel for communication. Whether for personal or professional purposes, the importance of email senders cannot be understated.

First and foremost, the sender of an email establishes credibility and trust. In a world where online scams and phishing attempts are prevalent, recipients are cautious about opening emails from unknown senders. When you consistently send emails from a recognized and trusted address, recipients are likelier to open your emails and engage with your content. >>> *continued on Page 2*

Best Practices To 'Celebrate' National Change Your Password Day: How Does Your Password Stack Up?

Each year, on February 1st, we celebrate Change Your Password Day. While it's not a holiday that gets you off work, it is an excellent opportunity each year to do a quick check-in and ensure you're using strong passwords to protect your accounts.

The suggested 'rule' used to be to change your password every three months. With advanced tools like password managers and data encryption >>> *more on page 3*



Additionally, the sender's reputation plays a vital role in email deliverability. Internet service providers (ISPs) evaluate the reputation of each sender to determine if their emails should be delivered to the inbox or flagged as spam. By maintaining a positive reputation with ISPs through sending relevant and engaging content while adhering to industry best practices, you increase the likelihood that your emails will reach their intended recipients.

Furthermore, personalized communication is highly valued in today's saturated digital landscape. When an email comes from an individual or an identifiable organization rather than a generic account, it demonstrates that an effort has been made to establish a personal connection with the recipient. This can lead to higher open rates, increased engagement, and better results.

As of February 1, 2024, Google and Yahoo implemented new requirements for email senders, particularly those sending bulk emails (over 5,000 messages per day to Gmail addresses). These guidelines aim to improve email deliverability and combat spam and focus on **three key areas**:

1. Email Authentication

- **DKIM (Domain Keys Identified Mail):** This technology verifies that emails originate from your domain and haven't been tampered with. Both Google and Yahoo now require DKIM for all emails.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** DMARC builds upon DKIM and allows you to set policies for how email receivers handle unauthenticated emails from your domain. Starting with a "p=none" policy is recommended, but stricter policies can be implemented gradually.

2. Spam Rates:

- **Maintain low spam rates:** Google's Postmaster Tools tracks your reported spam rate (percentage of recipients marking your emails as spam). Aim for below 0.10% and avoid exceeding 0.30%, as high rates can significantly impact deliverability.

3. Unsubscribe Options:

- **Clear and easy unsubscribe:** Every email must have a prominent and functional unsubscribe link. Make it easy for recipients to opt out of your mailing list.

Additional Tips:

- **Use a reputable email service provider (ESP):** They can help you implement authentication, monitor spam rates, and manage your email marketing effectively.
- **Segment your audience:** Sending targeted emails to engaged subscribers can improve engagement and reduce spam complaints.
- **Comply with CAN-SPAM Act:** This US law regulates commercial email and outlines legal requirements for sending emails.

Benefits of Complying with Google and Yahoo's New Email Sender Requirements

Complying with Google and Yahoo's new email sender requirements offers several benefits, including improved email security, enhanced deliverability, and a better user experience. The specific advantages of adhering to these requirements are as follows:

1. Improved Email Security: The new requirements aim to tighten security measures, ensure email source authenticity, and protect email recipients from unwanted content. By enforcing stricter standards, Google and Yahoo proactively combat spam, phishing, and malware, significantly reducing unauthenticated messages and a cleaner inbox.

2. Enhanced Deliverability: Adhering to the new requirements increases the likelihood of emails being delivered to the inbox rather than being marked as spam. This means legitimate emails are more likely to reach their intended recipients, improving overall deliverability.

3. Better Use Experience: The changes promote responsible email practices, making inboxes less cluttered with unwanted or malicious messages. This ultimately leads to a better user experience for email recipients, as they are less likely to encounter spam, phishing attempts, and other unwanted content.

In summary, complying with Google and Yahoo's new email sender requirements not only helps safeguard email security and reduce the risk of email fraud but also improves the overall deliverability of legitimate emails and enhances the user experience for email recipients.

However, despite all the benefits of the major rollout of changes mentioned, most businesses are still afraid of a possible and potential business disruption that it may bring as they go along with the changes.

To prepare for these requirements and minimize disruption, the following steps are recommended:

1. Set Up Custom Sending Domain. Ensure your emails come from your unique domain.

2. Create a DMARC Record. Implement DMARC to protect your domain from being used in business email compromise attacks and prevent your emails from spoofing.

3. Set up DKIM and SPF. These essential email authentication methods help protect your domain from spoofing, phishing, and other malicious activities.

By adhering to these steps and ensuring high deliverability and compliance with the new email-sending standards set by Google and Yahoo, businesses can minimize the risk of disruption and continue to reach their target audience effectively.

To comply with Google and Yahoo's new email sender requirements, email senders should take the following steps:

1. Authenticate your sending domain by setting up SPF, DKIM, and DMARC records.
2. Set up a DMARC record.
3. Maintain a low spam complaint rate by only sending emails to users with implicit or explicit consent to receive marketing emails.
4. Allow one-click unsubscribes.
5. Stay below a spam-rate threshold.

What are the steps to comply with Google and Yahoo's email sender requirements?

Email senders should also ensure that they are adhering to best practices for email senders, such as using a branded "sent from" address, avoiding spam trigger words, and regularly cleaning their email lists. By following these steps, email senders can ensure that their emails continue to reach recipients' inboxes and avoid being filtered or limited by Google and Yahoo.

In conclusion, understanding the importance of email senders is crucial in maximizing the effectiveness of your email communications. From establishing credibility and trust to enhancing deliverability rates and reinforcing brand identity – investing time and effort into optimizing this fundamental aspect of email marketing is undoubtedly worthwhile for any individual or organization seeking impactful communication strategies in today's digital landscape.

experts now say the type of password you use is more important than how often you create a new one. We're sharing up-to-date advice on creating a strong password that will keep your account secure and hackers guessing.

Make It Complex

Aim for complexity by combining uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable information like birthdays, names, or common words. The more intricate and unique your password, the harder it is for hackers to crack it.

Longer Passwords Are Harder To Crack

Long passwords provide an added layer of security. According to Hive Systems, brute-force hacking can crack an eight-character password in less than one hour! When creating a new password, aim for a minimum of 12 characters, and consider using passphrases—sequences of random words or a sentence—which can be both strong and easier to remember.

A random passphrase is like: cogwheel-rosy-cathouse-jailbreak.

This passphrase was generated from the website useaphrase.com, which will auto-create a four-word passphrase for you if you're stumped.

Use Unique Passwords For Each Account

Resisting the temptation to reuse passwords across multiple accounts is crucial. If one account is compromised, having unique passwords for other accounts ensures that the damage is contained. Consider using a reputable password manager to help you securely generate and store complex passwords.

*Do NOT use Google or your browser's password manager. If your Google account is compromised, all your passwords will be too. Talk with your IT team about what password management tool they recommend for you and your organization.

Update Passwords Yearly

As long as your account hasn't been compromised, you only need to change your passwords once a year to minimize the risk of unauthorized access. A regular password change routine would be beneficial only if someone has access you don't know about. A frequent password change can make it more challenging for attackers to maintain access to your accounts over an extended period.

Engage Multi-Factor Authentication (MFA)

Implementing multi-factor authentication is another easy way to make your password bulletproof. MFA typically combines something you know (your password) with something you have (like a code sent to your phone). Even if your password is compromised, MFA significantly reduces the chances of unauthorized access.

Set Up Strong Password Recovery Alternatives

Leverage password recovery options like security questions or alternative e-mail addresses. It's important to choose questions with answers that are not easily guessable or have publicly available information, so "What's your mother's maiden name?" is out!

Use Password Managers

You don't have to try to remember every password, and you shouldn't write them down on a sticky note on your desk. Instead, use a secure password management tool that will handle keeping track of your passwords for you.

Bonus points for turning off the auto-fill feature. Hackers can infiltrate sites and install code on a page that creates a second, invisible password box. When your password manager auto-fills the login box, it will also fill in the invisible box, giving hackers your password. This isn't overly common, but it still poses a risk.

Regularly Review Account Activity

Monitor your account activity for any suspicious logins or activities. Many online platforms offer features that notify you of login attempts from unfamiliar devices, allowing you to take swift action in the event of unauthorized access.

It's also always good to be aware of phishing attempts, never click suspicious links or attachments in e-mails, avoid public Wi-Fi and only use secure connections, and educate and train your team on what to look for when it comes to cybercrime so they can protect themselves, you and the company.

As cyber threats evolve, mastering the fundamentals of cybersecurity, like creating strong passwords, becomes paramount. You can significantly enhance your online security by making informed choices and staying proactive.

However, as the leader of your organization, it's important to remember that nothing is foolproof. Educating your team on cybersecurity best practices is essential, but mistakes can and will still happen. For most, it's not a matter of if but when. You must have a robust cybersecurity plan in place. The right IT team will ensure you have every protection to keep you safe and a crisis management plan ready if something goes wrong. We'll do a **[FREE Cybersecurity Risk Assessment](#)** to find out what gaps you have in your cybersecurity system. Click below to book yours now.

Securing Your Smartphone: A Step-by-Step Guide Against Mobile Attacks

Securing smartphones is increasingly vital as they hold personal and sensitive data. Key challenges include outpacing evolving cyber threats, balancing convenience with security, educating on risks like phishing and malicious apps, and managing vulnerabilities from connected IoT devices. Proactive security measures, strong passwords, biometric authentication, and regular updates are essential. Awareness and careful management of IoT connections are also critical to safeguard against breaches and malware.

How do you identify if your mobile device has been compromised?

Several signs can indicate that your mobile device has been compromised. These signs include:

1. Unexplained Battery Drain: If your phone's battery is depleting unusually fast, it could be due to background processes initiated by malware or spyware.

2. Spikes in Data Usage: Unexpected data usage may indicate malicious activity, as hackers often transfer data from your phone without your knowledge.

3. Pop-ups or Changes to Your Screen:

Malware can cause spammy pop-ups, changes to your home screen, or bookmarks to suspicious websites. If you notice any of these, your device may be compromised.

4. Unrecognized Outgoing Calls or Messages:

If you see outgoing calls or messages you didn't make, it could be a sign of a hack.

5. New Apps You Didn't Download: If you notice unfamiliar apps on your device that you didn't download, it could indicate that a hacker has access to your phone.

If you suspect that your phone has been hacked, you can take the following steps:

Disconnect from the Internet: Turn off your phone's Wi-Fi and mobile data to prevent further unauthorized access.

Run Security Software: Install and run security software on your smartphone to detect and remove any malicious software.

Factory Reset: If you cannot resolve the issue, consider performing a factory reset. Remember to back up your data before doing so.

Monitor Your Accounts: Monitor your bank accounts, email, and other sensitive accounts for suspicious activities.

Being aware of these signs and taking proactive measures can help protect your mobile device from potential compromise.

Step-by-Step Guide Against Mobile Attacks

To safeguard your mobile device against cyber threats, you can follow a step-by-step guide that includes the following measures:

1. Update Your Device Regularly: Ensure your mobile device's software and applications are updated as soon as possible to patch any known vulnerabilities.

2. Use Biometric Authentication and Strong Passwords: Consider using biometrics (e.g., fingerprint, face) authentication and strong lock-screen pins/passwords to protect your data.

3. Install Security Software: Install security software on your mobile device, including mobile threat detection and protection tools.

4. Monitor User Behavior: Regularly monitor your device for any unusual behavior that could indicate a security breach.

5. Security Awareness Training: Stay informed about the latest mobile security threats and best practices through security awareness training.

6. Avoid Jailbreaking or Rooting Your Device: Refrain from jailbreaking or rooting your device, as this can make it more vulnerable to security threats.

7. Use Trusted Accessories and Networks: Only use original charging cords and accessories, and avoid connecting to unknown or untrusted networks and accessories.

8. Be Cautious of Phishing Attacks: Be vigilant against phishing attacks, which can occur through various channels such as email, SMS, and social media platforms.

By taking these steps, individuals can significantly reduce their risk of falling victim to mobile attacks

How Partnering with an IT Managed Services Provider (MSP) Elevates Your Business

Partnering with an IT Managed Services Provider (MSP) that adheres to industry best practices can significantly enhance your company's operational efficiency, employee retention, and bottom line. Here's how an MSP can transform your business landscape:

1. Aligning Technology with Business Goals: An MSP understands your business needs and expectations, tailoring technology solutions to align with your company's objectives. This strategic alignment ensures that your technology investments directly contribute to your business's success, supporting growth and innovation.

2. Enhanced Operational Efficiency through Proactive Support: Proactive monitoring and support from an MSP can anticipate and resolve IT issues before they escalate, minimizing downtime. This ensures your operations run smoothly, your employees remain productive, and your business stays on track toward achieving its goals.

3. Scalable Solutions for Growth: As your business evolves, an MSP provides scalable technology solutions that grow with you. This flexibility supports your company's development and expansion, ensuring technology is always an enabler, not a constraint.

4. Building Trust with Transparency: Clear, regular communication from your MSP demystifies technology, fostering trust between you and your technology partner. This transparency ensures you are always informed and confident in the technology decisions being made for your business.

5. Exceptional Service Enhances Employee Satisfaction:

Quick response times and effective problem resolution by an MSP mean your employees face fewer frustrations and more up-time. This directly impacts employee satisfaction and retention, creating a more positive work environment.

6. Empowering Your Team: Education and training provided by an MSP empower your employees to leverage technology more effectively, enhancing their efficiency and enabling them to contribute more significantly to business success.

7. Driving Decisions with Feedback: An MSP that implements a feedback loop values your input, ensuring that services are continuously refined to meet your needs. This collaborative approach to service improvement can lead to better service outcomes and higher satisfaction levels.

8. Cost-Effective Technology Management: Competitive pricing and flexible contracts offered by MSPs ensure you get value from your technology investment, directly impacting your bottom line by optimizing IT costs.

9. Deepening Business Relationships: An MSP focused on building relationships understands your business beyond just the technical requirements. This can lead to more personalized service, better support, and advice aligned with your business challenges and goals.

10. Staying Ahead with Advanced Technology: Leveraging the latest technologies through your MSP can improve your operational efficiency, enhance customer service, and position your business as a leader in your sector.

11. Robust Security for Business Protection: Cybersecurity measures implemented by your MSP protect your business from threats, ensuring the safety of your data and maintaining your company's reputation.

12. Reliable Service Delivery: Adherence to service level agreements (SLAs) by your MSP guarantees consistent, dependable service delivery. This reliability ensures a solid technology foundation supports your business operations.

By partnering with an MSP that follows these best practices, your business can enjoy enhanced operational efficiency, improved employee retention, and a stronger bottom line. Discover how our managed services can transform your business landscape. Book a **FREE Consultation** today to explore tailored solutions that drive actual results.

Navigating the Transition: QuickBooks Desktop Plans to Cease New U.S. Subscriptions

Intuit's decision to end new subscriptions for certain QuickBooks Desktop products by July 31, 2024, prompts users to evaluate their accounting software needs. This change affects Desktop Pro Plus, Premier Plus, Mac Plus, and Enhanced Payroll but opens the door to more advanced, cloud-integrated solutions.

Affected Products and Impact:

- After the cutoff, renewal and support continue for existing subscriptions.
- No changes for QuickBooks Desktop Enterprise and specific bundles.

Strategic Shift:

- Reflects a broader move to cloud-based services, aiming to phase out on-premise software.
- Aligns with Intuit's focus since launching QBO in 2001, pushing for a transition to more comprehensive, secure cloud technologies.

Migration Options:

- QuickBooks Online: For those considering QBO, be mindful of migration challenges and limitations, such as a cap on user numbers and potential streaming issues.
- Alternative Accounting Software: Options like Passport Accounting offer cloud compatibility, integration with Microsoft 365, and insights into financial operations without the constraints of desktop solutions.
- ERP Solutions: For broader functionality, including inventory and manufacturing, consider ERPs like Passport Software's integrated system, which supports growth without the limitations of traditional bookkeeping software.

Choosing the Right Path:

- Moving to QBO or similar platforms may restrict future scalability. Alternative software or ERP systems offer more flexibility, integration, and the ability to add comprehensive features, aiding in operational efficiency and growth.

This guidance aims to help QuickBooks Desktop users navigate the transition, offering a comparison of alternatives to make informed decisions about their financial management tools.