10 TOP EMAIL SECURITY BEST PRACTICES 2024

As we enter the final quarter of 2024, email continues to serve as the backbone of business communication worldwide. However, the sophistication of cyber threats has reached new heights, making comprehensive email protection more crucial than ever.

Harmony Email & Collaboration is at the leading-edge when it comes to combating evolving email-based threats. Drawing on our experience across this year, we've compiled 10 top email security best practices that have proven exceptionally effective in 2024.

Whether you're a small business or a large enterprise, implementing these strategies will significantly enhance your email security posture for the remainder of the year and beyond.

1. **Implement Advanced AI-Powered Protection.** Utilize Harmony Email & Collaboration Security's True AI technology to detect and prevent sophisticated phishing attacks before they reach your inbox. Our AI is trained on comprehensive datasets to identify even the most subtle threats.
2. **Enable Multi-Factor Authentication (MFA).** Require MFA for all email accounts to add an extra layer of security beyond just passwords. This significantly reduces the risk of account takeovers.
3. **Regular Security Awareness Training.** Educate employees about the latest email threats and phishing techniques. Harmony Email & Collaboration Security offers resources to help keep your team informed and vigilant.
4. **Use Email Encryption.** Encrypt sensitive information sent via email to protect it from unauthorized access. Our solution seamlessly integrates encryption capabilities into your email workflow.
5. **Implement Data Loss Prevention (DLP).** Utilize DLP tools to prevent sensitive data from being accidentally or maliciously sent out via email. Harmony Email & Collaboration Security includes robust DLP features to safeguard your critical information.
6. **Keep Software and Systems Updated.** Ensure all email clients, servers, and security software are up-to-date with the latest patches to address known vulnerabilities.
7. **Employ Sandboxing Technology.** Use sandboxing to safely analyze suspicious attachments and links before they can harm your systems. Our solution incorporates advanced sandboxing capabilities to detect and neutralize threats.
8. **Implement DMARC, SPF, and DKIM.** Deploy these email authentication protocols to prevent email spoofing and improve deliverability. Harmony Email & Collaboration Security can help you configure and manage these protocols effectively.
9. **Regular Security Audits and Penetration Testing.** Conduct regular audits of your email security posture and perform penetration testing to identify and address potential vulnerabilities.
10. **Leverage Inline Protection.** Implement inline protection to monitor and filter incoming emails in real-time. Block malicious content before it ever reaches user inboxes and ensure immediate cyber threat neutralization.

.

Other items to note:

By implementing these best practices and leveraging Harmony Email & Collaboration Security's advanced AI-powered protection, you can significantly enhance your organization's email security posture in 2024. Our solution acts as a complete replacement for traditional Secure Email Gateways (SEGs), connecting via API and blocking malicious emails before they reach the inbox.

Don't leave your email security to chance. Contact Harmony Email & Collaboration Security today for a demo and see how we can help you stay ahead of evolving email threats in 2024 and beyond.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com