CRC Group
Wholesale & Specialty

Email Filtering: A Common Sense Tool for Preventing Cyber Crime

There are currently 3.9 billion electronic mail users around the globe, and most have a love-hate relationship with their email. This might be because the average American worker receives more than 120 emails every day. Even so, email usage is predicted to grow by another 2% - 3% each year through 2023.[4] It continues to be the most frequently used internet-based service for businesses because it's an efficient means of communicating with team members, partners, and clients. On the other hand, email is also a big problem area for cyber security because it's the most frequent avenue of attack for cybercriminals launching phishing scams, ransomware, and malware that can cause devastating harm to a business.[1] As network security measures improve, it's harder for hackers to exploit system vulnerabilities, causing cybercriminals to focus on targeting the human element to gain system access. Businesses can continue to benefit from email while minimizing attack risk by utilizing an email filtering solution to steer malicious emails away from employee inboxes.

WHAT IS EMAIL FILTERING?

Email filtering is a process that's typically as straightforward as it sounds. Inbound and outbound emails are checked and filtered for suspicious links, spam, malware, etc., before messages are sorted into various categories. Filtering solutions help avoid engagement with annoying spam emails attempting to make readers buy something or donate to a cause and graymail people casually opt-in to when making online purchases. However, more advanced third-party filtering also identifies phishing emails that pose more danger to personal, company, and customer data.

Common Email Filtering Solutions*

- **Proofpoint Essentials**
- **SpamTitan**
- **Barracuda Essentials**
- **Cisco Email Security**
- **Cloudmark Safe Messaging Cloud**
- **Cyren**
- **Forcepoint Email Security**
- **Mimecast**
- **Trustifi**[3]

HOW DOES ADVANCED EMAIL FILTERING MAKE A DIFFERENCE?

Many well-known email platforms include basic anti-virus software and email filtering, but most have only minimal filter requirements that are no longer enough to protect against email-based cyberattacks.[1,2] Standard filters also often take time to learn what is or isn't spam, leaving organizations open to attack. Advanced email filtering programs utilize machine learning, artificial intelligence, and employee behavior monitoring to identify and track phishing emails, providing an extra layer of protection above a standard spam filter that remains static.[1,2]

**CRC Group does not endorse any specific company or provider; the specific names listed in this article are simply informational references. Organizations are responsible for researching and selecting MFA and EDM services based on business needs.*

©2022 CRC Insurance Services, Inc., CRC of California Insurance Services, CA Lic No 0778135. No claim to any government works or material copyrighted by third parties. Nothing on this website constitutes an offer, inducement, or contract of insurance. Financial strength and size ratings can change and should be reevaluated before coverage is bound. This material is intended for licensed insurance agency use only. This is not intended for business owner or insured use. If you are not a licensed agent please disregard this communication.

Nine out of ten successful cyberattacks are email-based.[1]

Typically, third-party email filtering can be implemented quickly and doesn't require additional time to learn what is or isn't malicious. These solutions can also identify more complex attacks and isolate them so that only acceptable email is allowed to reach an organization's server. In addition, if an employee regularly receives emails that aren't opened, the third-party filter will start filtering them out, saving time from unsubscribing or deleting unwanted graymail or spam. In the event that a company's email server goes down, these filters also support business continuity by allowing employees to access email through the solution's server. This can be a big plus if an unexpected or prolonged server interruption occurs.[2] Advanced filters also protect businesses from denial-of-service (DoS) attacks that seek to overwhelm the system with a huge volume of requests that can halt operations, resulting in lost time and money, by stopping threats before they ever reach the server.[2]

When a company makes an effort to use a more sophisticated email filtering solution, it monitors millions of email addresses, evaluating content for phone numbers, weblinks, QR codes, other images, brand logos, and credential requests. In addition, every link or attachment is checked for malware when an employee clicks on it or when the email is received. Some also include spoofing protection software capable of identifying emails that initially look like they might be from a trusted company but are actually generated by fraudulent domains. Finally, solutions can include educational banners that inform users of a potential phishing threat and then notify IT administrators if the warning is ignored.[1]

More than 50% of all email messages worldwide are spam.[1]

BOTTOM LINE

Email is necessary for many internal communications and communicating with clients or other companies. However, it's a proven weak spot for many businesses, allowing spam and viruses or malware to put business health at risk. Email filtering can be highly effective when combined with employee training that helps businesses stay vigilant, making it a key piece of a company's risk management plan and a strong cyber insurance policy. When reviewing insurance applications, underwriting wants to see that companies are screening email attachments or links and quarantining suspicious emails for users. Doing so reduces the chance of a data breach, decreases the risk of phishing and ransomware attacks, and can lower cyber insurance premiums. Agents seeking to help clients improve their cyber risk management plan should contact their local CRC Group Producer to learn more about how we can help today.

Contributor

- Mike Edmonds is an Assistant Vice President with CRC Group's Seattle office, where he specializes in Cyber & Technology, E&O, Healthcare, and Management Liability as part of the Seattle ExecPro Team.

ENDNOTES

1. Why You Need Spam Email Filtering, Teknologize, February 18, 2021. https://blog.teknologize.com/spam-email-filtering
2. 6 Reasons You Should Consider an Additional Spam Filter for Your Email, MainSpring. https://gomainspring.com/businessstrategy/6-reasons-you-should-consider-an-additional-spam-filter-for-your-email/
3. The Top Email Spam Filtering Solutions, Expert Insights, March 14, 2022. https://expertinsights.com/insights/the-top-email-anti-spam-filtering-solutions/
4. Email Usage Statistics in 2021, Campaign Monitor, July 11, 2019. https://www.campaignmonitor.com/blog/email marketing/email-usage-statistics-in-2019/
5. Web and Email Filtering, The Bunker. https://www.thebunker.net/layered-security/network-protection/web-and-email-filtering/