7 Data Backed Reasons

That Show Most Email Security Isn't That Secure

sendio®

Most Email Security isn't that Secure.

For businesses of every size, IT security is one of today's biggest challenges. Consider that in 2013, between 68 and 82 percent of all S&P 500 companies were suffering an externally-observable data breach, at any given time.[1]

Each year about 380 million individuals fall victim to cybercrime email is the most common medium for these attacks. With cybercrime costing U.S. companies a total of $38 billion in just 1 year[2] it's clear why email security has become such a priority at both enterprise firms and small-to-medium businesses (SMBs).

$38 billion

in cybercrime costs for U.S. companies in one year.

Around the globe, the majority of businesses invest in email security solutions in an attempt to protect themselves from the rising flood of security threats. However, even with growing use of email security technologies, the number of threats facing enterprise and SMB networks is increasing each year: Through 2016, the financial impact of cybercrime is expected to grow 10 percent a year,[3] with email-based schemes like phishing, spear phishing and malware among the most common threats facing the business community.

With so many email security systems in use today, how could the number of successful email security attacks actually be increasing? The reason is simple: Most email security technologies are falling short in keeping companies secure, despite their claims to effectively prevent spam and malicious messages from landing into employee inboxes. We've identified seven data-backed reasons that show why.

1. Email filtering alone **doesn't work.**

Most email security solutions filter messages based on content, looking for common signs of spam and malware. These include unconventional formatting, a high percentage of numeric text, and certain words and phrases. However, this approach can easily lead to false positives—especially in a business environment where messages with unique formatting and many numbers are common. Not only can false positives cause employees to miss important emails, they often require employees to manually search through their spam folders for any missed messages, and this opens the possibility of them clicking on one of the malicious emails housed there.

Meanwhile, antivirus and other "blacklisting" techniques seek to block messages from potential scammers by defending against the most well-known attack vectors. Unfortunately, these technologies are often ineffective when an attack uses unknown or new malicious code.[4] This is because new and custom malware is unfamiliar to these email security blacklists, so their signatures will go undetected. Since new malware signatures are being created every day, blacklists are becoming increasingly ineffective.

Enter the whitelist. Rather than trying to keep up with everything that is unacceptable, whitelists take a positive security approach and only allow in messages from known senders.

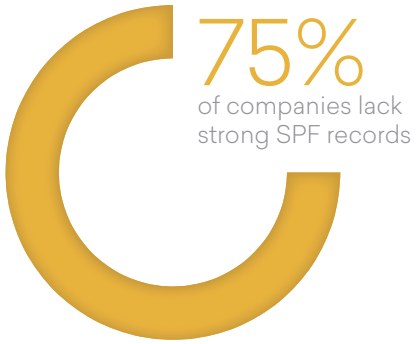
Whitelisting solutions work by comparing the address, domain and IP address of each incoming email against an approved list. But with spoofing and phishing schemes on the rise, whitelisting is becoming less effective at catching malicious emails. If a coworker's account gets spoofed, a whitelist will continue to route their messages straight into your inbox, which increases the chances that whatever malicious link or file they are harboring will be executed.

2. Weak SPF records aren't preventing **email spoofing.**

Most email security solutions use an SPF check, which is a type of Domain Name Service (DNS) record, to guard against spoofing. If the sender is whitelisted, messages from that person are delivered directly to users without being scanned for spoofing, a vulnerability that criminals have started to exploit.

A 2014 survey found that 75% of companies, chosen from the S&P 500, lacked SPF records that were strong enough to prevent email spoofing.[5]

If large S&P 500 organizations aren't well-protected from spoofing, it's safe to assume that many SMBs are likely vulnerable as well, even with email security in place. In an effective email security solution, an SPF record would strictly identify the mail servers that are permitted to send email on behalf of your domain. This helps to keep cybercriminals from sending messages by forging addresses within your domain.

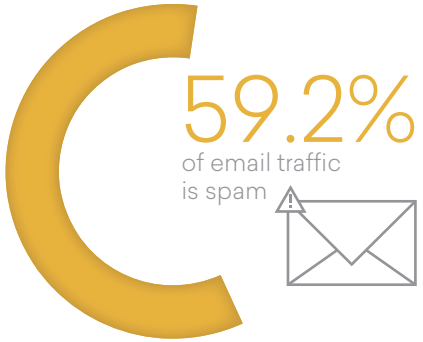


3. **New domain zones** give cybercriminals more flexibility.

In 2014, the new registration program for generic top-level internet domains launched, giving businesses new opportunities to register custom domains that range from .com and .net to .email, .work or even .fashion.[6] While businesses celebrated the flexibility provided by this advancement, cybercriminals immediately began exploiting it. The new domains enable spammers, phishers and other bad guys to more effectively mass-distribute potentially malicious emails.

How? Cybercriminals are no longer limited to basic domains like .com or .org. Now, they can register new top level domains to more effectively trick their victims. For example, a scheme might involve registering the domain wellsfargo.finance, and then sending emails that direct Wells Fargo customers to the site. The criminals could then use wellsfargo.finance to collect their personal and financial data, and the victims wouldn't know until it was too late.

Already, the new domain zones have led to a significant increase in the number of domains sending out malicious email. Amazingly, research has shown that 59.2% of overall email traffic during the first quarter of 2015 was spam.[7]



4. Even with email security in place, unwanted email **is running rampant.**

Even with the vast majority of businesses using an email security solution, three-quarters of each employee's emails are not relevant. With such an influx of bulk messages, the chances are high of an employee accidentally opening an infected attachment, clicking on a malicious link or falling for a phishing scheme.

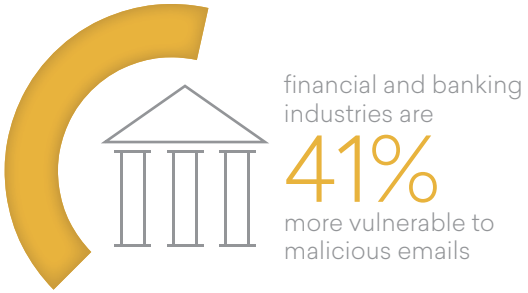
Recent research by Gartner[8] finds that on average of emails delivered to business accounts are unwanted—they are either spam, malware or other bulk mail.

While the overall flood of unwanted email is growing, malicious messages themselves are also on the rise. Instances of phishing, viruses and other scamming emails grew eight percent in 2014, a trend that is expected to continue in the coming years.[9]

5. **People** can be your weakest link.

In many large data breaches, email security technologies are in place—but criminals have developed sophisticated ways to sidestep many security techniques. For example, early in 2015, police in Eastern Europe discovered an expansive cybercrime ring that had stolen upwards of $1 billion over the course of two years by sending spear phishing emails to bank employees at about 100 different financial institutions. The emails contained a Control Panel Applet (CPL) attachment that, when opened, executed a shellcode that enabled the cybercriminals to access the victim's network and steal the employee's credentials. By mimicking various employees, the hackers were able to transfer money to their accounts and even get cash by taking control of the banks' ATMs.[10]

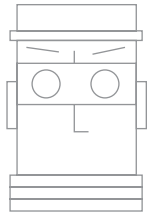
Even with a traditional email security solution in place, these banks and businesses in general are still vulnerable to attacks like these for one simple reason: People make mistakes. They accidentally open infected attachments and fall for email-based schemes all the time. According to one study, recipients click on an average of one in every 25 malicious emails, regardless of the size of the business, with the banking and finance industry 41 percent more vulnerable than other markets.[11]



So-called "social engineering" attack tactics are carefully designed to take advantage of people's natural dispositions. For example, cybercriminals know that email recipients are more likely to click on a link that is personally relevant. A recent malicious message included a link to a website that was customized to each recipient's location with a fake news story claiming an explosion had occurred in their city.[12] Another natural inclination is for users to assume that their company's email security filters are effective enough to protect them from anything serious.

Emboldened by this false sense of security, they can actually be more likely to click on suspicious links and attachments when using their work email than they would be when accessing personal email.

Today, phishing is particularly successful because these messages mimic those from individuals, organizations or businesses that the recipient trusts. Many email security solutions are not able effectively defend against this type of threat, because the content of the message often appears legitimate to email security filters. As a result, spear phishing currently accounts for 91 percent of all successful email-based attacks[13] —proof that most email security filters aren't doing enough to protect people from this growing threat.



6. Cybercrime **pays off big.**

Even as email security solutions continue to grow more sophisticated, the attacks against both enterprise organizations and SMBs are staying one step ahead. And with good reason: Cybercrime is incredibly lucrative.

A standard ransomware campaign offers and most email security schemes do not face prosecution.[14] The FBI's Most Wanted List for cyber criminals includes individuals who have stolen staggering amounts of up to $100 million—all from enterprise businesses, SMBs and consumers.[15]

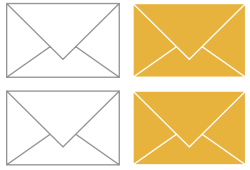
With cybercrime offering such a powerful payoff, experts agree that email security schemes will only continue to become more common and increasingly sophisticated. And today's scammers are very adept at sidestepping many of the traditional email security tactics; that's why so many breaches occur, even with most organizations employing some type of email security solution.

7. Employees sometimes intentionally sidestep **email security measures.**

Even with email security solutions and protocol in place, a business still may be at risk as a result of its employees disregarding the importance of email security. For example, a strong majority of employees admit to accessing personal email from their business computers.[16] In these cases, it doesn't matter how strict your email security technology may be; using personal email on a work computer opens your company's network up to an entirely new set of security threats.

On top of that, about half of all email users reportedly use their inbox as a type of day-to-day file storage repository,[17] even if their company warns against it.

Rather than moving important emails and attachments to a secure location, these messages are stored within the user's email. This puts your business at greater risk for data loss since scammers are able to gain access to such a wealth of company information, simply by infiltrating a single email account.



50%
use email as day to day file storage

Protect Your Company from Today's Email Security Threats

Now that we've looked at some of the leading reasons that email security isn't necessarily secure, consider a few best practices for protecting your company from today's threats. A layered email security solution is a must-have in order to safeguard your employees from scams like spoofing and phishing that cyber criminals work continuously to evolve. It's not enough to simply filter email based on content; scammers have learned ways around those tactics, which is evident in the growing number of data breaches occurring within businesses around the globe.

97%
agree they needed better email protection

Instead, seek out an email security solution that focuses on the sender rather than solely looking at the content. Instead of whitelisting and blacklisting, which can still allow malicious messages into company inboxes, look for a solution that filters based on the sender using SMTP defense techniques. IP address reputation checks also help to continuously protect your employees from evolving threats—even spoofing. Meanwhile, a high level of protection from viruses, identity theft attempts and phishing schemes will help ensure your employees don't fall victim to sophisticated social engineering attacks.

In a recent Gartner survey, 97 percent of respondents agreed they needed better protection from email security threats such as targeted phishing attacks.[18] As cybercrime threats continue to grow and become more sophisticated, now is the time for your company to truly protect itself.

References

1. Kepes, Ben. “Security Statistics Show That We Need to Reinvent Enterprise IT.” Forbes. Forbes, 4 March 2014 Web. 28 July 2015.
2. Paganini, Pierluigi. “The Impact of Cybercrime.” InfoSec Institute. InfoSec Institute, 1 November 2013. Web. 29 July 2015.
3. “Gartner Reveals Top Predictions for IT Organizations and Users.” Gartner. Gartner, 1 December 2011. Web. 28 July 2015.
4. Johnson, Josh. “Finding Evil in the Whitelist.” SANS Institute. SANS Institute, 23 March 2015. Web. 29 July 2015.
5. Kepes, Ben. “Security Statistics Show That We Need to Reinvent Enterprise IT.” Forbes. Forbes, 4 March 2014 Web. 28 July 2015.
6. Claburn, Thomas. “Google Domains Service Opens for Business.” InformationWeek. UBM Tech, 14 January 2015. Web. 29 July 2015.
7. Shcherbakova, Tatyana, et al. “Spam and Phishing in the First Quarter of 2015.” SecureList. AO Kaspersky Lab, 13 May 2015. Web. 29 July 2015.
8. Firstbrook, Peter and Brian Lowans. “Magic Quadrant for Secure Email Gateways.” Gartner. Gartner, 1 July 2014. Web. 30 July 2015.
9. Santillan, Maritza. “Research Reveals Growth in Phishing Scams, Targets PayPal and Major Bank Customers.” The State of Security. Tripwire, 3 September 2014. Web. 30 July 2015.
10. Jackson Higgins, Kelly. “Cybercriminals Target Bank Employees, Steal $1 Billion From Financial Institutions Worldwide.” InformationWeek. UBM Tech, 14 January 2015. Web. 30 July 2015.
11. Muncaster, Phil. “One in 25 Malicious Emails are Clicked On - Report.” Infosecurity Magazine. Reed Exhibitions, 22 April 2015. Web. 30 July 2015.
12. Zeltser, Lenny. “Evolving IT Security Threats: Inside Web-based, Social Engineering Attacks.” SearchSecurity. TechTarget, n.d. Web, 30 July 2015.
13. Chapman, Tom. “Spear-Phishing Could Enable Cyberterrorism Attacks Against the U.S.” TechCrunch. AOL Inc., 22 May 2015. Web. 30 July 2015.
14. Peters, Sara. “Cybercrime Can Give Attackers 1,425% Return on Investment.” InformationWeek. UBM Tech, 9 June 2015. Web. 30 July 2015.
15. “Cyber’s Most Wanted.” FBI.gov. U.S. Department of Justice, n.d. Web. 28 July 2015.
16. Brandeisky, Kara. “5 Things You Didn’t Know About Using Personal Email at Work.” Money. Time Inc. Network, 3 March 2015. Web. 30 July 2015.
17. “The Life of an Attachment.” TinyHacker. TinyHacker, n.d. Web. 30 July 2015.
18. Firstbrook, Peter and Brian Lowans. “Magic Quadrant for Secure Email Gateways.” Gartner. Gartner, 1 July 2014. Web. 30 July 2015.

ABOUT SENDIO

At Sendio, we recognize that businesses of all sizes need a new approach to email security. Our email security and efficiency technology combines a set of tightly integrated layers that eliminate malicious threats and spam campaigns. Rather than relying on content filtering, Sendio's Email Security Gateway™ uses a system of malware filters and reputation scoring technologies to eliminate the spam from your company's inbox without the headache of false positives and lost mail. With our exclusive Server Recon technology and a suite of best-of-breed security tools, our Email Security Gateway™ will ensure your company's email is truly secure.

(949) 274-4375 | www.sendio.com

sendio®