WHITEPAPER

6 email security threats to defuse in 2019

GFI Software™

Table of Contents

Introduction 3

Common email security threats 4

- Spam emails
- Malware
- Phishing attacks
- Business Email Compromise scams
- Email sharing behavior
- Spoofed domains

Impact of email threats 7

Protection from email security threats 8

Try GFI MailEssentials **Free** For 30 Days 8

Introduction

Despite a growing number of tools and alternatives, email continues to be the leader in business and consumer communication.

According to the Radicati Group, 293 billion business and consumer emails will be sent and received each day in 2019. This number will grow to 347 billion by 2023. Over half of the world's population uses email as a means of communication and this number will increase to 4.3 billion users by 2023.

The continuing growth in email use also presents lucrative opportunities for hackers, especially if your email security level is below-par or not kept up to date.

Over 90 percent of cyberattacks start with phishing emails and 92 percent of malware is delivered through emails. Hackers see email as a prime way to enter your corporate network and access confidential data. Hacking strategies and complexity change each year; they are increasing in sophistication and knowledge.

Your security practices must keep pace.

Common email security threats

1 Spam emails

Unsolicited bulk email, also known as spam, contains ads or messages that entice users to click on a link, buy a product, or take other such action. About 130 billion spam emails are sent every day around the world. This accounts for over 40 percent of all emails received by business users.

Spam emails occupy valuable space in your email server. They can clog your network and reduce productivity levels within the organization. Individual employees filtering such emails manually wastes time. More seriously, they can contain viruses and malware that could compromise your network security.

2 Malware

Email is the preferred delivery channel for malware. Hackers prefer email over other communication channels because it is pervasive, easy and effective.

Cyberattackers embed malware in emails with enticing content/offers. When any user clicks on links in the email, the malware can cut across multiple layers of security or protocols to give the hacker access to your network.

Hackers play the odds. If one employee out of hundreds or thousands falls victim to a malware attack, the entire business is compromised. Malware continues to be a key email-security issue compromising organizations. All industries are vulnerable and have been affected by it.

INDUSTRY	Users that had malicious emails sent to them (%)
Wholesale Trade	23.8
Mining	22.6
Nonclassifiable Establishments	20.3
Agriculture, Forestry, & Fishing	18.4
Manufacturing	18.2
Public Administration	16.9
Retail Trade	14.4
Construction	12.9
Services	9.5
Transportation & Public Utilities	7.2
Finance, Insurance, & Real Estate	6.8

Source: Symantec

No level of security will help if the user clicks on a malware email. Specific solutions that address malware coupled with extensive user training are essential to curb this threat.

3 Phishing attacks

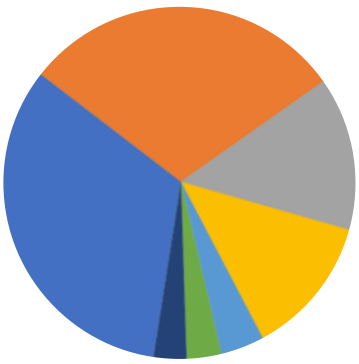
Phishing is the act of tricking someone to reveal his or her personal information voluntarily, with hackers posing as legitimate companies making a reasonable request. Cyber criminals send emails based on a user's online activity and trick users to reveal sensitive personal information such as Government IDs, date of birth, and more. This activity is commonplace; over 75 percent of all businesses and organizations were targets in the last year.

Hackers may use technical subterfuge strategies to steal credentials from a victim's computer, to falsely create seemingly legitimate emails. This first step then increases the potential for others to click on emails.

Anti-Phishing Working Group statistics help capture the problem.

Statistical Highlights for 4th Quarter 2018	OCTOBER	NOVEMBER	DECEMBER
Number of unique phishing Web sites detected	56,815	35,719	45,794
Number of unqiue phishing e-mail reports (campaigns) received by APWG from consumers	87,619	64,905	87,386
Number of brands targeted by phishing campaigns	293	233	310

Most-Targeted Industry Sectors for 4th Quarter 2018



Payment	33.0%
SAAS / Webmail	29.8%
Financial	14.3%
Other	12.9%
Cloud Storage / File Hosting	4.0%
Telecom	3.2%
Logistics / shipping	3.0%

Source: Anti-Phishing Working Group

4 Business Email Compromise scams

According to Symantec, Business Email Compromise (BEC) has become more widespread than ever before. In 2017, 8,000 businesses reported BEC scams. The number continues to grow. At the end of 2018, the US Federal Bureau of Investigation reported that BEC schemes alone have caused a cumulative loss to companies of $12.5 billion in five years. On average, 5.2 BEC emails are sent to a business every month.

BEC scams are difficult to identify because they come in different forms. Perpetrators may impersonate an executive within a company and ask junior employees to do a wire transfer to prevent a possible “shutdown of operations” or other serious consequence for the company. This prompts the unsuspecting victim to transfer company funds to the false—or hacker—account. They may also pose as a bank or individual the victim knows, requesting confidential information.

5 Email sharing behavior

It is estimated that 29 percent of all emails are shared widely within an organization’s sphere of employees, partners, and other stakeholders.

Sharing behavior can lead to problems when email contents include sensitive information such as credit card details or personally-identifiable data. Even company’s source code has been shared or distributed in this way. This could lead to breaches in the referenced application if it reaches the wrong hands.

6 Spoofed domains

Cybercriminals can easily spoof the domain you own and send out emails that seem genuine. For example, if your company name is XYZ and your website is xyz.com, criminals can hack into your domain, create an email ID such as johngalt@xyz.com, and send an email from it. When recipients get an email address from a domain they know, they are more likely to open the email and click on the links in it.

Another common strategy is the use of lookalike domains. Instead of microsoft.com, hackers will create a site called micrsoft.com and send emails from it. When the human brain sees the first and the last letter, it tends to tap into familiar words. Recipients are tricked into thinking the email is from a legitimate domain.

These are some of the email threats that can affect your business in 2019, and they can have organization-wide implications, depending on the nature of the attack.

Impact of email threats

Hackers are extremely successful entering companies through an email door left open. Email-based threats are not going to end soon, nor decrease. According to a survey conducted by Infosecurity magazine, 87 percent of respondents said they faced an email security threat in the past year, while one-third of this number admitted that they experienced a ransomware attack over the same period. Over 80 percent of the respondents believed email attack frequency and severity have been increasing.

In a survey of 2,250 IT executives in the United States, United Kingdom, France, and Germany, 88 percent of companies said they were targeted by at least one instance of email fraud over the past year. Another survey shows that across a broader set of counties, 75 percent of companies were attacked by at least one email fraud over the past two years, and 41 percent of companies experienced two or more email fraud attacks.

The increase in email threat has serious consequences for businesses. Michael Siegel, a research scientist at MIT, says that 75 percent of email threats go undiscovered for weeks or even months. They surface only when a major breach occurs or is detected within the organization. This results in a major financial and reputational loss for the company, as well as leading to negative effects for customers, suppliers and partners.

What actions can responsible organizations take?

We can't ban email. A better option is to look at different email protection processes, tools and software that prevent email-based attacks.

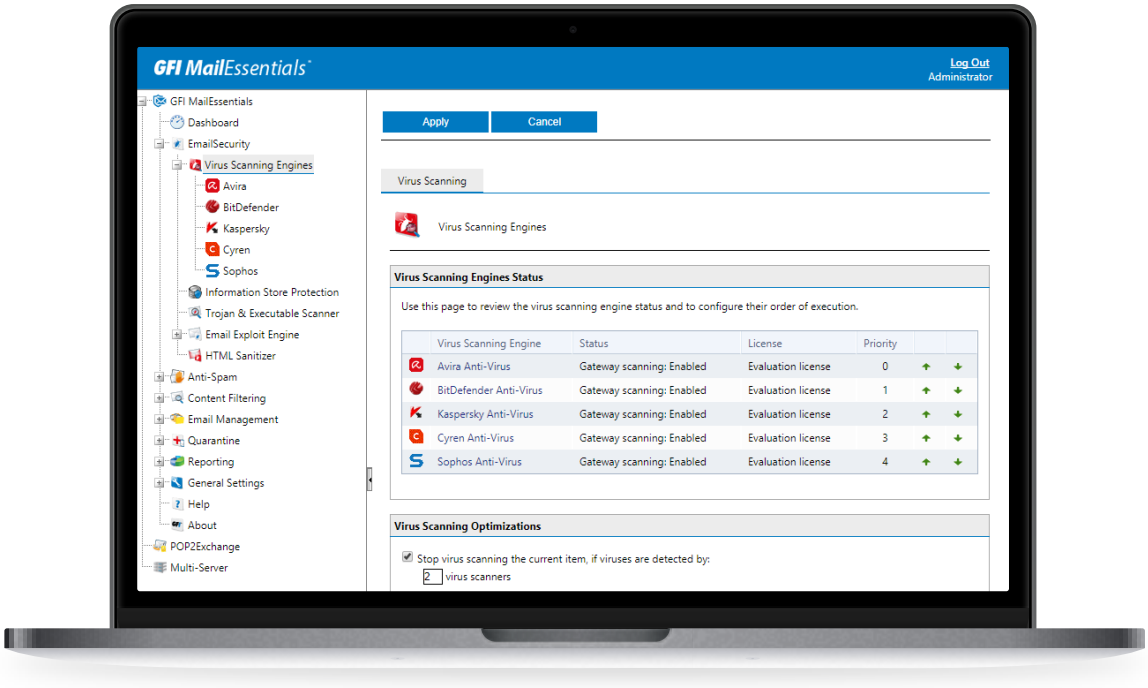
Protection from email security threats

There are many tools and strategies that help strengthen the defenses of your email servers and network so you can proactively stave off email-based attacks. These include:

- Training all employees about the threats from emails, and ways to avoid them.
- Formulating email policies that inform and deter employees from clicking on any link from their email.
- Antispam filters that reduce the number of email marketing and other spam emails.
- Antivirus programs to monitor for Trojans, viruses, and malware.
- Content filtering tools that scan email content for catch phrases like a bank account, urgent, hurry. These filtering tools raise a red flag when such words are present in the content.
- Monitoring tools that examine incoming and outgoing emails to reduce the possibility for email frauds.
- Reporting tools that send periodic reports about the current state of the organization's network and email servers. These tools can also raise alerts when thresholds are breached within the email servers.
- Keeping your email software up-to-date and fully patched so it can catch the known vulnerabilities.
- Deploying anti-spoofing technologies to protect your domain.

Email security threats are a major concern for every organization. They can have serious financial and operational implications. To be proactive and avoid these threats, use the right email security tools and strategies. Follow up tool deployment with regular training on best security practices for your employees.

The combination of tools, awareness, education and vigilance will help your organization avoid email-based threats and fraud.



GFI Software™