






Email security best practices for SMBs



Table of Contents

	Introduction	3
<hr/>		
	Best practices from an e-mail server/service administrator perspective	5
	General email security best practices for admins	5
	Regularly confirm your employees know all email security best practices	5
	Set strict password requirements for your employees	6
<hr/>		
	Best practices from a user perspective	7
	Learn about current phishing schemes	8
	Use a difficult password	8
	Utilize two-factor authentication	9
	Do not open unexpected attachments	9
	Try to avoid opening your inbox on public wifi	10
	Use spam filters	10
<hr/>		
	The importance of following email security best practices	11
<hr/>		
	Provide secure email to your employees with GFI's solution set	12

Introduction

How many emails do you get per day? Per week? What about per month? Now, multiply that by every person in your company.

The number of emails sent each day isn't in the millions, it isn't even in the billions, but it reaches up to the hundreds of billions every single day, and the number is expected to continue increasing, from about [281 billion in 2018 to 347 billion in 2022](#).

While emails continue to increase, working their way into every facet of business, security becomes more complex and vital. Many people do not even think twice about their email usage, from employees opening discounts from their favorite stores on work computers to CEOs scheduling their private doctor's appointment without a second thought.



Email has become such a ubiquitous part of life, people don't think about the incredibly private information they include in the body or as an attachment--social security numbers, appointment information, bank details, medical records, and more.

Because malicious actors know people send these details, they continually come up with ways to intercept them in more and more believable schemes.

According to a SANS Cyber Security survey, "An estimated [75 percent](#) of identified, impactful threats were initially entered via email attachments and 46 percent of attacks were executed by users clicking web links in email." And, believe it or not, "SolarWinds MSP Mail claims that [almost 70 percent](#) of email traffic is spam or malicious."

Data breaches of all kinds, even involving high-profile companies, are more and more common. According to an [email security survey](#), 74 percent of businesses reported that "email-borne cyber attacks are having a major impact and 78 percent said the cost of email breaches is increasing." Over 80 percent of organizations "claim to have faced an attempted email-based security threat in the past year."

This study found that top concerns included phishing, "with 43 percent of organizations reporting spear phishing attacks in the past 12 months." The actual effects that were most common included "loss of employee productivity, downtime and business disruption, recovery costs, loss of data, financial impact, and damage to the reputation of the IT team."



Financial losses due to unsecure email keeps rising, “with 78 percent of organizations saying the financial impact of email breaches is increasing dramatically.” In fact, about two thirds of participants admitted to attacks having a direct monetary cost to their business.

Even if you think your employees fully understand the risk, [30 percent of phishing emails](#) get opened and 66 percent of malware is delivered in an email attachment. Human error accounts for 25 percent of all data breaches within the U.S.

Even if only one employee misses the proper protocol about following security best practices, your entire company can be put at risk. Getting into your email server (meaning, for simplicity’s sake, backend programs that function as mail transfer or transport agents such as SMTP or mail delivery agents like POP3) or phishing important company credentials could spell disaster for a small or medium business.

Email security needs to be a cornerstone element in your business. This means following security best practices for both employees and admins, making sure you have protection every step of the way.

According to the [Verizon 2019 Data Breach Investigation](#) report, the average business user receives an average of 4,380 potentially malicious emails every year. Multiply this by the number of employees in your business, and you have a potentially massive number.

Even if you think your employees understand the need to perform simple actions like checking that the URL address is correct before typing in any credentials, malicious actors become more sophisticated, even redirecting proper URL addresses to phishing scams.

Email security best practices are more than simply setting a spam filter. A focused email security plan can greatly decrease your odds being part of these statistics.



Best practices from an email server/service administrator perspective

Many businesses host their own email servers, whether by choice or necessity. For example, certain industries require this for regulatory compliance, because third party emails don't offer the same level of security or necessary compliance requirements.

If your mail server is not properly protected, you risk litigation, fines, lost productivity, and worse. Simply following email security best practices can substantially mitigate any risk.

General email security best practices for admins

- **Create email blacklists** - Your IT department should have an ever-increasing list of banned email addresses. This is a fast and effective way to block certain domains, email addresses, and IP addresses from ever getting to your employees. A well-maintained blacklist greatly helps address your spam problem.
- **Always use SSL options when available** - These options are available for POP, IMAP, and SMTP as standard TCP/IP ports and are the preferred option to plaintext email ports. Even if you don't think your data has anything worth seeing, SSL options are always a safer bet. Secure POP3 is port 995, IMAP is port 993, and SMTP is port 465.
- **Limit total number of connections, total number of simultaneous connections, and maximum connection rate in SMTP settings** - This helps to prevent any denial of service attacks. You might have to play around with these numbers until you figure out the right ones for your company.
- **Limit the mail relay for your SMTP server** - Make sure the settings only allow authenticated user email accounts in your system.
- **Prohibit use of personal emails** - This lightens the load of your security measures in place and statistically lowers risk for your business.
- **Always upgrade or update** - Ensure your corporate email clients and servers are always fully up to date.

Regularly confirm your employees know all email security best practices

Even if you have the best cyber security plan possible, an incredible spam filter, and fine-tuned email server settings, employee error could still be the source of a breach. Every single employee at every level of your company needs to regularly demonstrate that they understand common email risks, such as clicking on a malware-ridden attachment or phishing schemes.

Security best practices suggest going beyond a simple meeting or memo on email risks. A short quiz that engages employees ensures they listen and understand the concepts and risks. This should take place with new hires; anytime your company is made aware of new, popular malicious schemes; and on a semi-regular basis to keep the information fresh in everyone's mind.

Your employees should know not only to ignore these malicious emails but also to flag them as spam and communicate with the IT department. In this way, your company will become aware of how threats penetrate filters already in place, helping protect against a similar threat in the future.



It's vital to keep each employee up-to-date on new scams because they are evolving to be extremely credible. Some malicious actors can find a way into your email and send replies to people in their contacts, referencing a subject that was previously discussed, while including a malicious link or attachment.

Letting your employees know about all different types of possibilities, including hyper-advanced ones, helps prevent risk.

Set strict password requirements for your employees

If someone can hack into your employee's email, they can wreak havoc and undermine much of the IT security measures you've put in place. Verizon's 2019 Data Breach Investigations Report (DBIR) displayed a [“98 percent rise of compromise”](#) of web-based email accounts using stolen credentials - seen in 60 percent of attacks involving hacking a web application.”

Make sure your employees have a password that is tough to crack:

- Using a combination of upper and lowercase letters, numbers, and symbols
- Not allowing the use of any words that can be found in the dictionary
- Not including any information that can be found easily online, such as their birthday, in the password.

As additional prevention, you should also put defensive tools in place that ward against any brute-force attacks so password-guessing tools cannot test your email accounts.

As the administrator, you should also change all administrative usernames to make them more secure.

If you have a smaller company, as administrator you may choose to set each employee's password yourself to make sure they meet the stringent security requirements. A larger company should implement a password checker to make sure employees follow these rules when setting their own password.

There is conflicting evidence about the need to change passwords regularly, usually on a schedule of about every three months, but current best practices still advise it.



Best practices from a user perspective

Employees have a significant role to play to ensure they don't accidentally fall into the hands of malicious actors. Here are some best practices for email users.

Learn about current phishing schemes

If your organization doesn't educate you about current phishing schemes, you should take it upon yourself to learn them.

For example, someone receives an email that appears to come from a reputable company where he/she already has an account, like a large bank. Many will click these emails, enter their information, and promptly lose money or access to their account.

You may think you would never fall for something like this, but many malicious actors attack 'smaller' targets. It may not be a bank; it may be a subscription like a newspaper, reminding you that your term is almost up. You click the link and enter your credit card details.



It's important to recognize these common scams. Often, the email will be filled with poor grammar or spelling. Some of the most popular phishing schemes include:

- Deceptive Phishing - scammers pretend to be a reliable company
- Spear Phishing - Uses information about the recipient, building trust and increasing the chances of the target falling for the scam
- Whaling - Targets the head of a company to gain almost full access
- Pharming - When a safe domain is redirected to an unsafe one by playing with the IP addresses.

Use a difficult password

As mentioned above, a difficult password is key to countering someone hacking into your email. If your company doesn't already require this, make sure to follow the guidelines above (combination of cases, numbers, symbols; not using standard words; not using personal information).

Don't reuse a password you've already employed on a different site.

Utilize two-factor authentication

This is useful in almost every online service. Two-factor authentication greatly lowers your risk of scams, phishing attempts, and hacking.

Do not open unexpected attachments

Never open an attachment from a sender you do not know. Malware and viruses are often hidden in these attachments.

Even if you do know the sender, it's best not to open unexpected attachments. Run a virus and malware scan first, or, if you are unsure how, send it to your IT department to check it.

Try to avoid opening your inbox on public wifi

Opening pages, logins, or email on public wifi can leave you vulnerable to hacking by someone else on the same connection. The safest way to open private connections like bank accounts or emails in public is to use phone data instead of shared wifi.

Use spam filters

Most email platforms already have spam filters built in. Utilize these, making sure to mark spam emails that sneak through to your inbox as 'spam' so those filters can continue to evolve.

You need to make sure you are aware and educated about potential risks regarding email. This backs up your company's efforts with their checks, filters and countermeasures at the infrastructure level.

The importance of following email security best practices

From admins to low-level employees to CEOs, everyone must do their part to follow email security best practices. By following these guidelines, you will help your company stay protected, keeping your business from losing productivity, money, and reputation.





Provide secure email to your employees with GFI's solution set

Unlimited | Secure Email

Core secure email capabilities in a value-priced package

- ✔ Email and collaboration tools
- ✔ Antivirus & malware protection
- ✔ Secure archiving

[Learn More](#)

GFITM

Aurea SMB Solutions

All product names and companies mentioned may be trademarks or registered trademarks of their respective owners. All information in this document was valid to the best of our knowledge at the time of its publication. The information contained in this document may be changed without prior notice.



Southeast Europe Regional Manager

nebojsa.stankic@zebra.cz

Cell: 00 385 99 3241 770 (CRO)

Cell: 00 381 61 6231 777 (SER) when in country

I also use the following platforms: WhatsApp, Viber, Signal, Telegram