GUIDE

The Mailgun guide to email security and compliance

Providing protection in a dangerous digital landscape

Table of contents

Table of contents

INTRODUCTION

Hard truths about email

Time for a reality check. As much as we love it, email is a major security risk for your company. If you're reading this, you're likely involved with protecting those who could be negatively impacted by a breach or from failing to comply with privacy regulations.

Don't kid yourself. Preventing bad actors from using email for evil and following best practices for privacy and security are tough jobs. The team at Mailgun by Sinch knows that as well as anyone else in the industry.

However, **we believe your email program is worth protecting**, and we believe educating others on how to do that promotes a safer digital landscape. In this comprehensive guide, you'll discover valuable insights and get expert advice on how to provide that protection.

But first, let's face the facts. **Here are five hard truths about email:**

1. Email is the biggest threat vector

Email is a top tool among cyber criminals, and the inbox is one of their favorite places to play.

Whether it's standard spam, a phishing attack, or an attempt to launch ransomware and malware, the inbox presents an opportunity for bad actors to do their dirty deeds, and they can do them dirt cheap.

In 2022, the hotel chain Marriott reported its third significant security breach in four years. This time it was a social engineering attack that gave a threat actor access to an employee's computer. Marriot has spent more than $16 million this year to recover from another breach that occurred in 2018.

Bad actors are even finding ways to get around multi-factor authentication (MFA) with adversary-in-the-middle (AiTM) phishing tools and techniques. Microsoft says a recent scheme is targeting thousands of organizations.

Email provides a pathway that allows scammers to infiltrate corporations. It can be used to reach a huge number of potential victims or highly targeted as with spear phishing. Since nearly everyone has an email address, bad actors don't need a high success rate. Fool just one person and it could disrupt an entire organization.

Still, we can't give up on email because we need it.

2. Email isn't going anywhere

Despite constant technological change in the digital age, email remains one of the best ways to communicate with customers and colleagues, reach an audience, and conduct business. From transactional emails containing important information to marketing emails that help drive the growth of a business, it would be tough to function without our inboxes.

Any time someone sets up a new mobile device or opens an online account, they need an email address. It's a key piece of Personally Identifiable Information (PII) that we all use to access applications and digital services. That's why identity theft is easy when a crook gets access to an email account.

It's estimated that more than 333 billion emails are sent and received around the world every day. **By 2025, that number is expected to top 376 billion**. Of course, plenty of those emails come from spammers and scammers.

3. Privacy laws and restrictions are getting tougher

In an effort to make the inbox and the internet at large a safer place, governments are writing laws and major tech companies are introducing new features to protect the people who use their email services.

For example, Apple shook up the email world when it introduced Mail Privacy Protection in 2021. Back in 2017, Google stopped reading Gmail users' emails for targeted advertising purposes. And email experts at Mailgun say Gmail's AI-powered spam filters are the best in the industry.

Consumer privacy laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States are designed to give more power to the people while keeping sensitive data from being abused.

The problem is that most legitimate senders are already following all the rules and best practices. **It's the bad guys who are not**. After all, they're called "outlaws" for a reason.

4. Cybercrime is constantly evolving

No matter what the mailbox providers and ESPs do to prevent malicious emails from reaching the inbox, bad actors always seem to find a way. Their tactics keep getting trickier, and their strategies keep getting more advanced.

Nick Schafer leads Mailgun's Deliverability and Compliance team. Nick and his team work to keep bad actors off our platform, which includes monitoring for suspicious activity and staying up to date on email security trends. He describes it as a never-ending battle:

> *"I hated hearing this, but the truth is you'll never stop them, but you can beat them. Once we figure out a way to stop one scheme, they'll come up with a new tactic. Still, that doesn't mean you shouldn't try. If the best we can do is slow them down, then that's what we'll do."*
>
> Nick Schafer, Manager of Deliverability & Compliance, Mailgun

5. Senders need to stay one step ahead of it all

All of this means senders must remain vigilant about email security and privacy protection. Your organization needs to do what it can to prevent problems while being prepared to mitigate the situation if and when something goes wrong.

Staying ahead of bad actors who want to use email to swindle your subscribers or trick people in your organization requires several important factors:

- An educated workforce that's aware of the risks
- Solid email authentication protocols
- An understanding of privacy regulations and how they relate to email
- Partners who can help your team keep email safe and secure

We'll focus on these areas throughout this guide. Along the way, you'll also hear from Mailgun experts who work closely with users to protect our platform and our customers' email programs.

Why email is worth protecting

Even though spammers and scammers are relentless, focusing on email security and privacy protection is most definitely a worthy endeavor.

Here's who and what you're protecting when you prioritize security and compliance:

1. The business

According to global research from IBM, the average cost of a data breach was more than $4 million in 2021, and **the average financial impact of a phishing attack was $4.65 million**. Business Email Compromises (BEC), which are a form of spear phishing, were the costliest at just over $5 million per breach.

The same IBM study found it typically takes businesses more than 280 days to stop and resolve these kinds of attacks. That includes the time and resources required of IT and cybersecurity teams to identify weaknesses and patch vulnerabilities.

2. Brand reputation

Security breaches and scams connected to your organization lead to bad press and will damage brand reputation, which results in a loss of trust. The IBM study found that **lost business represented 38% of total costs or nearly $1.6 million per breach**.

Of course, the impact on brand reputation can go beyond what's measured in financial costs. Companies that are the target of brand spoofing in the inbox may find that contacts are less likely to open and engage with a brand's emails because they aren't sure the messages are safe.

3. Sender reputation

Besides brand reputation, mailbox providers like Gmail, Apple Mail, and Yahoo Mail have ways of measuring and scoring an email sender's reputation. Failure to properly configure DNS records for email authentication means it's harder for mailbox providers to trust that your emails are legitimate.

That could mean the emails you send are more likely to get blocked or land in spam. So, missing or broken authentication protocols can negatively impact sender reputation and email deliverability.

4. Users and customers

Perhaps the most important consideration is how email security and authentication help protect your customers and/or the users of your applications. The privacy, identities, and finances of the people your organization serves are at risk if you're not prioritizing security and compliance.

Jonathan Torres leads teams of Technical Account Managers (TAMs) for Mailgun and other Sinch products. He reminds us that email is part of an interconnected digital ecosystem.

> *"Compliance, security, and email deliverability are not just problems for the sender. If you're only thinking about how these things impact you, that's looking at it through too narrow of a scope. Mailbox providers, subscribers, customers, employees, and brands; these issues touch every area, and everyone ends up involved."*
>
> Jonathan Torres, TAM Team Manager, Mailgun

PART 1

Email scams: Then and now

To understand why email is the biggest threat vector in cybersecurity, and to grasp the seriousness of the situation, it's helpful to look at where we came from and how we got here.

Let's take a trip back in time to email's younger days. Then, let's explore some common strategies bad actors use in modern email attacks.

The early days of email

In the beginning, email was mainly a form of interoffice communication. Computer programmer Ray Tomlinson introduced what's believed to be an early version of email at ARPANET in 1971. Several years later, a young Shiva Ayyadurai created a software program he called "EMAIL" to replace physical inboxes and paper memos at a New Jersey medical school.

Soon, email was being used to communicate between different organizations, which led to what many call the first email spam message. Marketer Gary Thuerk sent an unsolicited message to hundreds of ARPANET employees in 1978 that promoted a new computer model from Digital Equipment Corporation. Thuerk claims the message netted DEC $13 million.

So, it became clear. Email is an ideal channel for convincing people to spend money. However, when the Wall Street Journal marked spam's 30-year anniversary in 2008, Thuerk explained why he doesn't think he should feel responsible for the monster that email spam became.

> *"If the airline loses your luggage, do you blame the Wright Brothers?"*
>
> Gary Thuerk, "Father of Spam"

As more consumers purchased personal computers and eventually connected to the internet, bad actors saw an opportunity to exploit the inbox for profit even further. And it was easy.

When email was new and exciting, people opened, read, and responded to just about everything. The average internet user was also pretty gullible. Some of the tricks people fell for back then have become jokes because they are so laughable.

The so-called "Nigerian Prince" email scam is a perfect example. There were many similar wire fraud schemes telling recipients lies like they'd won the lottery or received an unexpected inheritance from a long-lost relative. Surprisingly, many of these old-school tactics are still being used today.

Through the 1990s, email was a bit like the Wild West, with outlaw spammers running around wreaking havoc. But a new sheriff was coming to town – or to the inbox to be more precise.

Cracking down on spam

Now, let's flash forward to the early 2000s. It was a time when dial-up internet, stone-washed jeans, and compact discs of the 1990s were on their way out. It was also a time when email spam was skyrocketing, and in response, U.S. lawmakers passed the CAN-SPAM Act in 2003.

Around that same time, Kate Nowrouzi took a job at America Online (AOL). Today, Kate is Mailgun's VP of Deliverability and Product Development. Back then, she was part of AOL's anti-spam team.

In 2003, AOL was still one of the biggest mailbox providers in the world, along with Hotmail and Yahoo Mail. At its peak, AOL had more than 35 million users. It was what most people used for email and internet connectivity. AOL was also on the frontlines of the fight against spam.

Kate and the AOL anti-spam team started realizing how tough it was to determine if a message was spam or a legit email that a subscriber wanted. The type of content or industry wasn't the best signal. Even businesses that deal with adult content or sell Viagra have real reasons to send emails to subscribers.

"We had algorithms built into the filters to catch spam patterns, and we used to do some manual analysis on incoming traffic that was suspicious. But the definition of spam can be very different from one person to another. So, we decided to give some power to the AOL members. Let them decide whether they wanted to receive this mail or not."

Kate Nowrouzi, VP of Deliverability & Product Development, Mailgun

That resulted in the first **report spam feature**, making AOL the first mailbox provider to have a **feedback loop** with its users. Next, the AOL anti-spam team started developing rules to evaluate how many spam complaints (based on a percentage of the volume) a sender could receive before AOL blocked their emails. This eventually led to the email metric known as the **complaint rate**, which is one factor mailbox providers use to judge sender reputation.

Of course, while all of this helped *control* spam, it didn't stop it. Bad actors just had to try some new tactics.

Increasing sophistication

Kate points out that not all email spam is created equal. There are traditional spammers who simply don't have permission to email you and want to make a few bucks. However, it's the senders with potentially harmful goals that present the biggest threat. And those scammers keep getting smarter.

> *"A lot has changed. Spam is evolving. It's a never-ending game. As Mailgun enhances its platform as an email service provider, and as ISPs do the same on the other side, we're all working hard to protect our users from malicious activities. But sometimes the spammers can be very convincing, especially with social engineering."*
>
> Kate Nowrouzi, VP of Deliverability & Product Development, Mailgun

Attackers can pull off these social engineering attacks in the inbox because there's so much information about people and businesses available online. They can learn a lot simply by browsing a target's public presence on social media.

These days, instead of email scams that come from a fake Nigerian prince, **they may appear to come from your bank, your best friend, or your boss**.

Not long ago, Kate donated to a public fundraiser on Facebook. Then she got what *she thought* was an email from the host of that fundraiser, a well-known founder in Silicon Valley. The email thanked her for donating and asked for more support in the form of Amazon gift cards.

At first, Kate missed one of the telltale signs – an underscore in the email address between the sender's first and last name, which was slightly different than the real email address. But as communications with the scammer continued, she noticed more obvious signs like poor English and a strange use of emojis, which seemed uncharacteristic of the individual the scammers were impersonating.

> *If I've been in this industry for 20 years and I fell for this trick, I can't imagine why someone like my mom wouldn't.*
>
> Kate Nowrouzi, VP of Deliverability & Product Development, Mailgun

Inside the mind of a modern scammer

While there are a lot of different types of email scams and many ways to pull them off, one of the more prevalent attacks in recent years is a form of phishing known as "**brand spoofing**." That's when bad actors find ways to impersonate your company's emails and website to trick people into giving them account credentials or other sensitive information. Email authentication with DMARC is the best way to protect against this.

However, if a bad actor gets their hands on SMTP credentials or API keys, they can literally send as your brand, potentially wreaking some serious havoc.

Jonathan Torres put himself in the shoes of a scammer and explained the basic process. Here's the way it often plays out, in just five simple steps.

How email brand spoofing works

Step 1

Find a recognizable brand that's vulnerable to spoofing.

Companies connected to finance, ecommerce, and technology are among those most likely to be spoofed.

Step 2

Look for unprotected API keys or crack SMTP passwords.

These allow bad actors to send as the brand itself, fooling mailbox providers and subscribers.

Step 3

Design a fake landing page or log-in page.

With a few basic tools and the right logo, it's easy to mimic the look of a brand's website.

Step 4

Craft a compelling fake email.

Scammers often use a sense of urgency to convince victims to act without thinking.

Step 5

Collect credentials from victims.

The email points recipients to the fake landing page. There, they attempt to log in but are actually giving up sensitive information.

As you can see, you don't necessarily have to be a super-hacker to get away with brand spoofing. Anyone with tools like Photoshop, a free website builder, and a list of scraped emails can give it a shot. Mimicking a recognizable brand is a piece of cake.

> *"If you can send out an email that looks like it came from a well-known company, you can send people to fake landing pages. And when a scammer has access to your actual emails, they're easy to replicate."*
>
> Jonathan Torres, TAM Team Manager, Mailgun

So, what can technical teams do to prevent brand spoofing? **The best defense against spoofing is the implementation of email authentication protocols**, which we'll discuss in Part 5. But if you don't want to look like a spammer in the eyes of mailbox providers and email recipients, you'll also need to be aware of some important rules and regulations.

PART 2

Compliance and the regulatory landscape

Before homing in on how to stop bad actors from using email for evil, let's make sure you're following all the right rules as a legitimate and trustworthy sender.

First, here's a quick refresher on the parties involved in email and data privacy:

1. Data subjects:

This refers to the consumer or recipient of email communications. Data subjects are the people who have their personal data collected, stored, and used by others. Privacy regulations are meant to protect their rights.

2. Controllers:

Data controllers are the ones collecting, storing, and distributing the data subjects' personal information. They're responsible for protecting that PII no matter where it goes or who touches it.

3. Processors:

These entities process personal data on behalf of controllers. They are usually external third-party solution providers that need access to PII to provide a service. There should be a contract between processors and controllers defining things like data usage, secure storage, and what happens to personal data when the business relationship ends.

As a sender of email, your company most likely falls into the category of "Controller", while Mailgun would be a "Processor." Mailgun's Data Privacy Officer (DPO), Darine Fayed, says that although our company goes above and beyond when it comes to regulatory compliance, ultimately, the burden falls on senders.

> *"Anyone who touches personal data needs to be protective of it. But controllers need to be specific about how personal data should be stored, treated, and transferred to third parties. All of that needs to be done in a way that's strictly compliant."*
>
> Darine Fayed, General Counsel & DPO, Mailgun

Overview of important consumer privacy laws

Let's take a brief look at some key standards and regulations surrounding consumer privacy and how they relate to email.

Because there is a lot to unpack, we'll cover the basics here and point you toward other resources where you can learn more about specific regulations and how they may affect you as a sender.

GDPR

This is the big one. Enacted in 2018, the EU's General Data Protection Regulation (GDPR) did a lot to push consumer privacy in the right direction.

While there was plenty of concern among marketers about how GDPR could impact their efforts, it turned out to be a good thing for everyone. Many of GDPR's requirements were already considered best practices for email senders, and it prompted others to tighten up privacy protection to get in line with the law.

Some important GDPR guidelines for email senders include:

- Obtaining consent to email someone
  - Explicit consent for commercial messages
  - Implicit consent for most transactional emails
- The ability to opt out of email communications (unsubscribe link)
- Safe and secure storage of data used for email personalization
- The ability to provide or delete all PII related to a subject if a data subject access request (DSAR) is made
- Links to a company privacy policy wherever you collect PII such as email addresses

Darine says company privacy policies should be written in a straightforward way and keep the legalese to a minimum.

> *"Any privacy policy needs to be clear, understandable, and transparent. That means you need to tell your subscribers and customers what data you collect, what you plan to use it for, how long it's stored, and if it is transferred anywhere. Your grandma should be able to buy something online and understand the privacy policy behind it."*
>
> Darine Fayed, General Counsel & DPO, Mailgun

GDPR prompted many other countries to take a closer look at their data privacy laws. Looking at the list below, you start to feel like you're swimming in a bowl of alphabet soup.

- India implemented the Personal Data Protection Bill (PDPB)
- China has the Personal Information Protection Law (PIPL)
- Japan uses its Personal Information Privacy Act (PIPA)
- Australia has updated its Privacy Act to address digital concerns
- Great Britain enacted the UK GDPR after Brexit
- Brazil has a General Personal Data Protection Law (LGPD)
- Canada follows its Personal Information Protection and Electronic Documents Act (PIPEDA)

It's important to remember that if your organization does business with people in a specific country, you must abide by that nation's data privacy laws. Thankfully, if you're already following GDPR guidelines, you're going to be covered in most areas.

Find out about Mailgun's approach to GDPR compliance.

Get important details about our approach to GDPR, including storage, security, processing, and how we support customers in dealing with data subject rights.

CCPA

In the United States, the most comprehensive data privacy regulation is the California Consumer Privacy Act (CCPA), which became law not long after GDPR. Again, there are many similarities between the two regulations, and CCPA reflects common best practices for email senders.

Even though CCPA only covers residents of the state of California, many U.S. and international companies have contacts that fall into that category. That means they need to be CCPA compliant.

While there are other states with their own data privacy laws, and other proposals are going through the legislative process, Darine Fayed says a federal law in the U.S. could be on its way in coming years.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is meant to protect credit cardholder information. It's a global standard that applies to any organization that accepts online payments.

PCI compliance includes requirements for protecting data like credit card numbers as it's transmitted across open networks, including email. In most cases, sending cardholder data over email isn't a good idea. If you do have to transmit cardholder data via email for some reason, you must make sure it's encrypted the entire time.

Of course, that's difficult to do, especially if the numbers end up sitting in someone's inbox or Sent folder where a hacker could find it. That's why PCI DSS Requirement 4.2 states that credit card data may not be captured, transmitted, or stored via end-user messaging technologies like email.

Most companies use a third party for credit card processing, and that company handles PCI compliance. For example, Mailgun uses the payment processor Stripe. But even when working with a third party, if you have any cardholder data stored on your own servers or systems, you must be PCI compliant.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law that mainly applies to healthcare companies. It includes requirements that outline how to prevent a patient's personal health information (PHI) from being improperly disclosed.

The most important HIPAA consideration for senders is that any email containing PHI **must be encrypted in transit**. Beyond that, healthcare companies should also get consent to email patients, specify how PHI will be used in a privacy policy, and have a way to securely store email communications containing that information.

Get more in-depth advice from Mailgun on email and HIPAA compliance.

Yet another factor to consider is the software and services you're using to send and receive emails. To find out how an email service provider (ESP) addresses healthcare privacy, ask to see the HIPAA Business Associate Agreement (BAA). The BAA defines the responsibilities of the sender and the processor regarding HIPAA compliance.

Check out Mailgun's HIPAA BAA.

Review the legal document that explains how we approach the division of rights and responsibilities when it comes to protecting personal health information.

Why email compliance matters

While it's certainly true that incompliance can lead to steep fines, Darine Fayed says that shouldn't be the only motivation for adhering to privacy regulations.

> *"Don't respect data privacy because you're afraid of GDPR fines or whatever looming data protection authority is going to come and get you. That's not why you should care. It's a business decision. If you treat people with respect in terms of their privacy, they will come back. People are much more aware of privacy risks as well as their rights. They want to trust brands, but they also expect brands to treat their personal data with care."*
>
> Darine Fayed, General Counsel & DPO, Mailgun

According to Cisco's Consumer Privacy Survey, **89% of people say they care about data privacy and want more control**. However, less than a third have acted on their privacy concerns. The truth is, most people expect the technologies they use to provide them with the privacy protection they need. Staying compliant helps you meet those expectations.

PART 3

The email threat landscape

To help your team understand the ever-changing email security threats your organization faces, let's review some key findings found in recent research from leaders in the cybersecurity space.

While these statistics fluctuate from year to year, and even quarter to quarter, they help paint a picture of the challenges that technical teams are taking on as they work to protect email and everything that's connected to the channel.

Phishing: The biggest cybersecurity problem

According to Deloitte and many other sources, **91% of cyber-attacks begin with a phishing email**. The inbox is the starting point, and from there, scammers can steal credentials, deliver malware such as the Emotet Trojan, or hold a company's digital files and data for ransom.

According to a 2021 report from Cisco, **50% of the organizations surveyed experienced ransomware activity in the previous year**. These can be extremely costly security breaches. Research from Palo Alto Network found **the average ransomware payment in 2022 is nearing $1 million**, which is a 71% increase from the year prior.

Why email is a serious threat

91%

Attacks that start with email phishing

50%

Organizations experiencing ransomware activity

96%

Organizations targeted by email phishing

Mimecast's report State of Email Security 2022 reveals that three out of four companies surveyed experienced an increase in email-based threats while **96% report being the target of email phishing**.

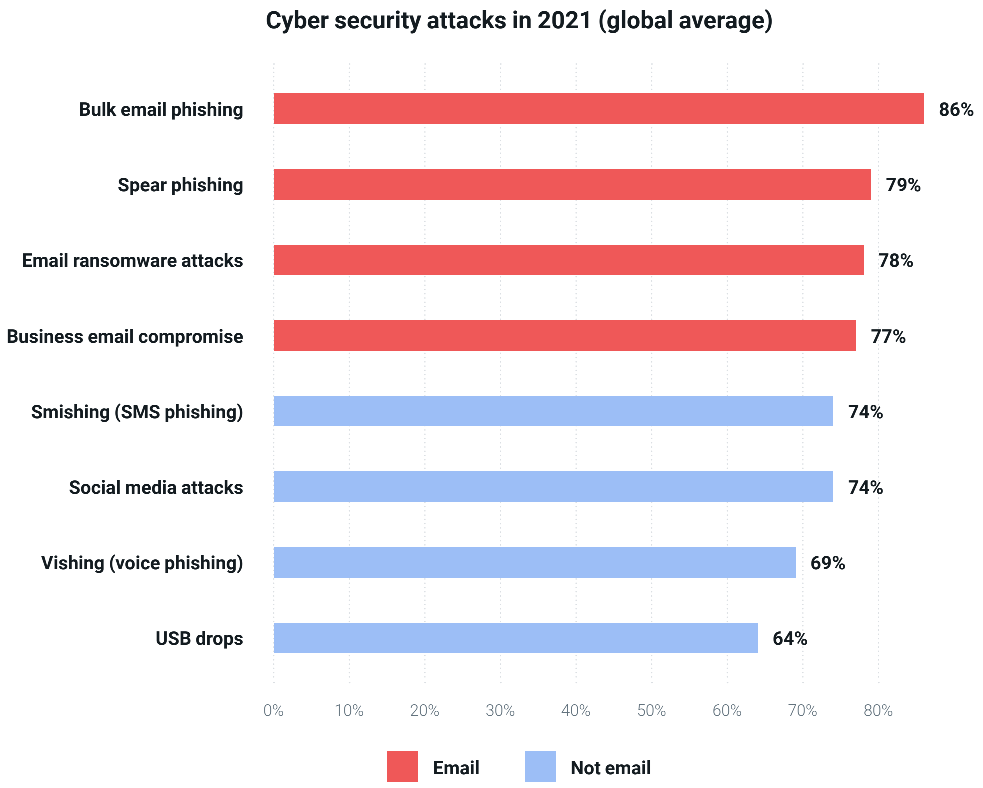
Mailgun's Nick Schafer agrees that ransomware can bring bad actors a big payday. However, he says the sheer number of email phishing attacks should make it a top security priority for every organization

> *"From my perspective, phishing is the biggest problem. I'm sure scammers think about ROI just like anyone else, and they can get that from ransomware attacks. But in terms of what we see, the quantity of phishing attacks is only getting worse. And they're good at what they do."*
>
> Nick Schafer, Manager of Deliverability & Compliance, Mailgun

Comparing email threats to other channels

Proofpoint's 2022 State of the Phish report examined how email and other forms of phishing are affecting companies around the world. It surveyed hundreds of IT professionals and thousands of other workers from the U.S., Australia, France, Germany, Japan, Spain, and the UK.

While companies from these nations experienced all sorts of threats on different channels, **email-based attacks represented the top four spots**. A total of 86% of the organizations in Proofpoint's survey reported at least one bulk email phishing attack in 2021, making it the most common.



Out of all different types of phishing attempts, **83% of global respondents said that at least one of those attacks was successful in 2021**.

The impact of phishing

We've already revealed that the potential monetary impact of mitigating a security breach can be quite costly, but the millions of dollars spent in the wake of a cyber-attack aren't the only ways these incidents affect businesses large and small.

Proofpoint's survey asked IT professionals around the world about the greatest impact successful phishing attacks had on their organizations. The most-cited effects were a breach of customer data (54%), compromised credentials (48%), and ransomware infections (46%).

Top impacts of a successful phishing attack

54%	48%	46%
Breach of customer/client data	Credential/account compromise	Ransomware infections

Not far behind ransomware infections, Proofpoint found **44% of respondents cited "loss of data and intellectual property" as another negative impact of a successful phishing attack**. The truth is, all these factors can have a lasting impact on a business, eroding trust, increasing costs, and even exposing the trade secrets that give companies a competitive edge.

Prioritizing security projects

So, where are technical teams focusing their efforts when it comes to thwarting security breaches? Given the stats we've just reviewed, it should come as no surprise that protecting **email is a prime security concern among many organizations**.

GreatHorn surveyed hundreds of IT and cybersecurity professionals to find out what worries them most. The top three types of projects cited by respondents in 2021 were email security (48%), security around remote work and telecommuting (41%), and cloud security posture management or CPSM (40%).

Top security projects in 2021

48%	41%	40%
Email security	Telework security	Cloud security posture management (CPSM)

A more specific IT project that relates to all these security concerns is the move from an on-premise email solution to a cloud-native approach. GreatHorn found that while just 24% of survey respondents still use an on-premise solution, **77% of those organizations planned to move to providers with cloud-native email infrastructure**. Doing so allows senders to find vendors with more advanced security measures in place, including partnerships with reliable public cloud computing services like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

Of course, improving cybersecurity around email or any other area will require the investment of time, resources, and budget. A shortfall in cybersecurity budgets, however, can leave technical teams with their hands tied.

The 2022 State of Email Security report from Mimecast found that **95% of those with a cybersecurity budget shortfall believe it impaired resilience and resulted in a lack of preparedness**. The report says efforts such as security awareness training and new technology are two areas where sufficient funds were lacking.

Dan Ross leads the Governance, Risk, and Compliance (GRC) team at Mailgun by Sinch. He says our organization's commitment to investing in strong security is an advantage for his team, our customers, and all our employees.

"Leadership has done a really good job giving us the budget to protect our company and our customers' data with the best technology in the industry. I think what positions Mailgun as a leader in security is how we react to known threats and the tools we use to make sure that bad actors stay out of our network. And internally, we have things in place to essentially protect employees from themselves."

Dan Ross, Sr. Manager GRC, Mailgun

PART 4

On the frontlines of email security

There are several different places where email security could be compromised:

1. In the location where email data and contact information are stored
2. On shared platforms for email sending
3. When messages are in transit or being sent from an ESP to recipients
4. When an email arrives at an inbox for authentication and filtering
5. After a message is received and sits in a recipient's inbox

Certain parties have specific responsibilities for security and privacy along the way. Let's explore each of the areas above and find out more about what it takes to achieve solid email security across the board.

Email security and data storage

Whether email data is stored on-premises or in the cloud, it should be protected with encryption when at rest. For example, **Mailgun utilizes AES-256 encryption-at-rest for all customer data**. That means a 256-bit key is required to encrypt and decrypt blocks of messages.

AES is an open-source method used around the world. It is considered effective at preventing brute force attacks, and it is what government agencies such as the U.S. National Security Agency (NSA) use for data encryption. Leading public cloud providers such as GCP, AWS, and Azure also use AES-256 encryption.

Most high-volume senders have turned to cloud-based solutions for email. When you choose partners who will store email addresses or any other sensitive data on your behalf, there are other security measures that will help protect that information inside data centers. This includes steps such as controlling access to data centers with 24-hour surveillance and biometric control systems.

Data processing at Mailgun.

Check out our DPA. Dig into the legal details, and find out how we handle data processing and compliance for both our company and on behalf of our customers.

Email security and sender reputation

When using an email service provider like Mailgun, you'll often have the option of choosing plans that utilize either dedicated or shared IP addresses for email sending.

Unless you're a high-volume sender, a shared IP address is usually adequate. But what happens if you're sending email from the same IP as a bad actor? **That could mean your sender reputation takes a hit**.

Mailbox providers use a variety of factors to score sender reputation. Two of the most important are IP and domain reputation.

It seems that mailbox providers like Gmail have started placing a higher importance on domain reputation. That's because it's much more targeted toward specific senders. Many domains could send from a single IP address. So, the reputation of a domain is more closely connected to a certain business or brand. IP reputation, however, is still a factor, especially with the Outlook email client, which means **IP reputation could have an outsized effect on B2B emails**.

For that reason (among others), Mailgun works hard to keep bad actors from using our platform to send email from shared IPs. Nick Schafer and the Deliverability and Compliance team will review and vet new users before they're allowed to use the platform.

"If bad senders come on to one of our shared IPs, the mailbox providers will notice. The sending reputation of other customers on the same IP could be negatively impacted because now the mailbox provider views the shared IP as a place where senders do shady things. That's why we care about stopping bad actors as well as keeping customers in line. It protects Mailgun's reputation as a sender, which is really important for users on shared IP addresses."

Nick Schafer, Manager of Deliverability & Compliance, Mailgun

Mailgun customers are also required to abide by our Acceptable Use Policy (AUP), which is another way we protect the sending reputation of all users. **Our AUP includes (but is not limited to) the following stipulations**:

- Bounce rate at or below 5%
- Unsubscribe rate at or below 1.4%
- Spam complaint rate at or below 0.8%
- No purchased, rented, or scraped contact lists
- Obtain express consent before sending non-transactional emails
- Include an unsubscribe link in every email
- No storage, transmission, or publishing of prohibited content (payday loans, illegal gambling, defamatory material, content that promotes violence, etc.)
- Avoid excessive use of the platform's shared resources

The AUP ensures we're all working together to follow best practices as senders in a shared digital environment. It's not meant to threaten anyone. The AUP is more like a code of conduct.

> *"These are the guidelines we monitor among Mailgun's customers, but if someone crosses one of those thresholds, we're not necessarily going to kick them off the platform. We know things happen from time to time. So, we'll first recommend that they clean up their act."*
>
> Nick Schafer, Manager of Deliverability & Compliance, Mailgun

Encryption: Email security in transit

Simple Mail Transfer Protocol (SMTP) is the standard protocol for email transmission. SMTP servers process mail, sending, receiving, and relaying messages from one server to another. But SMTP has a pretty big problem... it's not secure.

SMTP in its basic form doesn't support encryption or authentication algorithms. That's another reason spammers and scammers use email and why separate email authentication protocols, like SPF and DKIM, were created.

Spammers and phishers have often exploited SMTP servers configured with open relays. But password-protected SMTP servers can also be hacked, exposing data inside of emails. Bad actors may use SMTP to spread viruses and malware as well as carry out DoS attacks. It's even possible to modify an email message while on its way to a recipient. So, data also needs protection while emails are in transit.

That's why senders and ESPs add encryption protocols like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to SMTP. Mailgun stopped supporting SSL back in 2014 due to a vulnerability known as POODLE, which enabled man-in-the-middle (MTM) attacks.

TLS uses asymmetric encryption to establish a secure session between a client and a server. Then, it uses symmetric encryption to exchange data within the secured session. This is known as the TLS handshake: the process by which communication between a client and server is established and defined.

By default, Mailgun now uses what's known as **opportunistic TLS encryption** (TLS version 1.2) on emails, which will try to upgrade receiving servers to TLS if needed, but switches to plaintext SMTP if TLS is unsupported, which ensures deliverability.

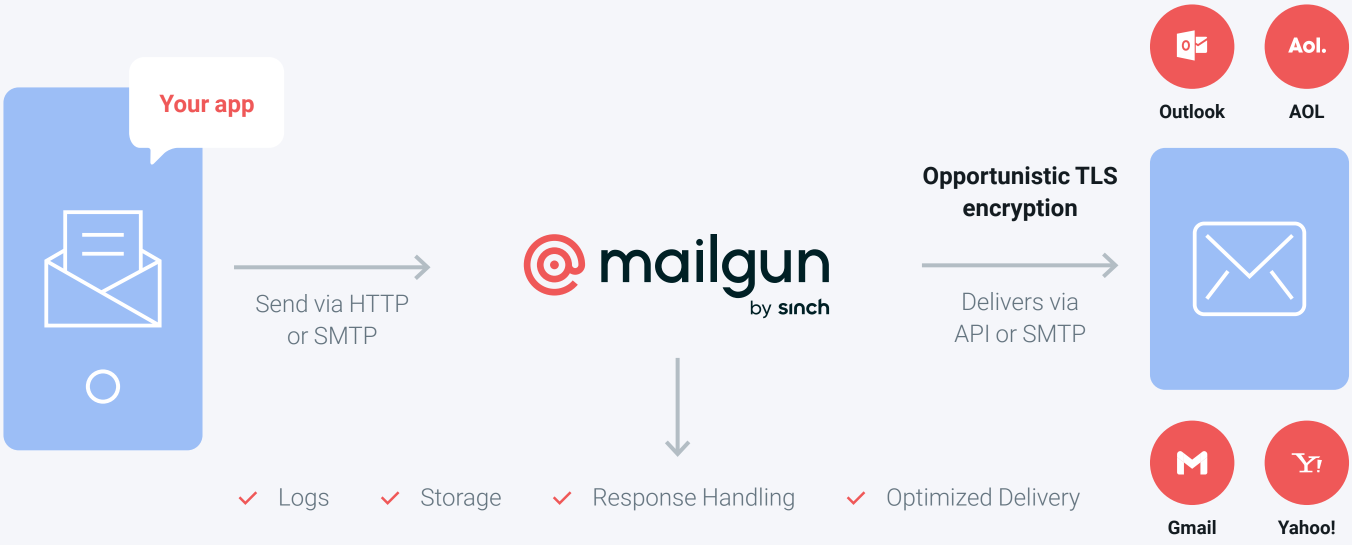
You can also add flags to opportunistic TLS encryption to customize connection settings for mail delivery. They are `require tls` and `skip verification`.

- `require tls:`
  - When set to TRUE, the receiving server will only deliver a message if the receiving server supports TLS.
  - When set to FALSE, we will try to upgrade but then deliver plaintext SMTP if that's unsuccessful.
- `skip verification:`
  - When set to TRUE, we won't attempt to verify the certificate and hostname when trying to establish a TLS connection.
  - When set to FALSE, we'll try to verify the certificate and if we can't, a TLS connection won't be established.

Find out more about TLS and email.

Get essential information on email communication encryption and how TLS connection control works at Mailgun.

Mailgun often recommends using our Email API instead of SMTP. The API is up to three times faster, easy to use, and ideal for large volume batched sends. Plus, Mailgun offers the possibility to use different domain sending keys when managing multiple senders. However, hackers may be able to access both SMTP credentials as well as API keys.



That's why it's so important to regularly rotate API keys and protect your SMTP passwords. Mailgun's Jonathan Torres says accidental exposure of API keys and SMTP credentials are among the most common ways email security gets compromised.

Dan Ross points out that email data also needs protection when you're moving contact lists between platforms. That's another situation in which sensitive data is at risk during transit.

"It's important to understand how email addresses and contacts get into the tools you use to send messages. Mailgun has a secure API, which is one item that sets us apart in the industry. Our customers use the API to upload emails and email addresses at an incredible rate. If you have a secure tunnel, it reduces the risk of that data getting intercepted during transit."

Dan Ross, Sr. Manager GRC, Mailgun

Email security and authentication

If bad actors try to spoof your brand using phishing emails, there are some highly effective ways to stop those emails from reaching the inbox. **Email authentication protocols help mailbox providers decide if emails might be faked or forged** before those messages are delivered to recipients.

Email authentication protocols emerged in the early 2000s as a way to enhance the security of SMTP and thwart the rise of email spam. SPF and DKIM were the first widely adopted methods. DMARC soon followed as a policy to confirm and extend SPF and DKIM. We'll cover these protocols in-depth in the next section.

At Mailgun, we require users to set up both SPF and DKIM records on their domain name system (DNS) servers. If you haven't done that, or need help, we can assist. We also strongly recommend enforcing a DMARC policy and can point our customers towards trustworthy service providers if needed. **Setting up DNS records for authentication will also improve sender reputation and email deliverability.**

> *"Mailbox providers need ways to identify who a sender really is. Without email authentication, it's hard to tell where email traffic is really coming from. What authentication does for senders is it makes it possible for them to say, 'This message is from us, it's our email traffic, and we're allowed to do this.'"*
>
> Nick Schafer, Manager of Deliverability & Compliance, Mailgun

Email security and awareness

In email security, what recipients don't know can *definitely hurt* them. But a well-educated workforce and savvy subscribers are going to be much more likely to catch spammers and scammers before they make a big mistake.

Mailgun's Dan Ross says an **employee awareness program is vital for email security**. Don't forget how prevalent spear phishing and business email compromises have become. These attacks target employees inside your organization. In an ideal situation, training and testing should take place yearly and with all new hires.

Throughout the year, you can also put that training to the test by sending your own "phishing" emails to employees as a test (faking fake emails in a sense). This helps you evaluate how aware people are, keeps employees on high alert, and gives you the opportunity to remind everyone what to watch for in a phishing attempt.

"At Mailgun, we do have phishing tests that are sent out, and if someone clicks on one, we have a conversation with employees to explain why they need to be more careful. We track these metrics and do what we can to keep our employees aware of phishing."

Dan Ross, Sr. Manager GRC, Mailgun

To paraphrase a common saying... your email security is only as strong as your weakest link. And in almost every organization, the weakest link is a human being, not technology.

Mimecast's State of Email Security 2022 report states that **employees with cyber awareness training are five times more likely to spot and avoid clicking on malicious links**. However, even though almost all the organizations surveyed have some sort of training, only 34% offer it on a regular basis. That's despite the fact that four out of 10 respondents cited employee naiveté as a major email security challenge in 2022.

Customer and subscriber awareness matters too. If your company is susceptible to phishing attacks and spoofing, or if you become aware of fraudulent emails misusing your brand, be proactive about the situation. Don't wait for people to fall victim. Inform them and warn them about these schemes. Make it clear what kinds of information you will and won't ask for via email.

Unfortunately, most companies don't think of educating customers about the risks of brand spoofing until they start getting bad press. Still, Jonathan Torres says a brand spoofing incident is an opportunity to be transparent and regain some trust in your brand.

"The last thing you want is for your company to be named in an email that looks legitimate, but it puts the recipient in a bad spot. I think that's something senders often realize after it's too late. Then they need to backtrack. So, if you get spoofed, be transparent. Communication is key. Tell people what happened and what you're doing to shore things up, so it doesn't happen again."

Jonathan Torres, TAM Team Manager, Mailgun

So, how exactly can you "shore things up", as Jonathan says? If your credentials accidentally get leaked, and someone starts sending spam from your account, it's likely Mailgun will know before you do, and we'll put a stop to it. Mailgun also helps senders restrict access to API keys and SMTP credentials by letting you assign user roles within the platform.

No matter what email sending platform you use, we highly recommend resetting API keys and SMTP passwords immediately as well as checking to see if your sending domain has been blocklisted due to the leak. Setting up two-factor authentication (2FA) will also help prevent this issue from happening ever again.

But is there anything else senders can do to fight back against brand spoofing? There is. **It's all about email authentication**, and we're about to explore that important subject next.

PART 5

Authentication: The last line of defense

The moment of truth in email transmission occurs when a mailbox provider such as Gmail or Outlook must decide how to filter a message. Is the sender of this email really who it claims to be? Is it spam? Is it dangerous? Should we block this message, send it to the junk folder, or deliver it to the inbox?

As Kate Nowrouzi mentioned earlier in this guide, it's not always easy to answer those questions, even if you're an anti-spam specialist. That's why the email industry developed **email authentication protocols** and other technical specifications to essentially ask for a sender's identification before being allowed inside the inbox.

For each protocol or specification, there is a DNS TXT record that must be added and correctly formatted on domain name system servers. Let's take a look at four key areas of email authentication, including how they help, how they function, and how they work together.

1. Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is a protocol that lists the IP addresses of mail servers and domain names that are authorized to send mail on your behalf. The SPF record acts like a bouncer at a nightclub. If you're not on the list, you don't get in.

For example, if you're sending transactional emails through Mailgun, a different ESP for marketing emails, and use Google Workspace for internal emails, all three need to be identified on your SPF record. This way, if mailbox providers notice mail coming from an unauthorized sender, they can choose to block those messages or send them to spam.

The technical details

Here's an example of an SPF DNS record:

```
v=spf1
ip4:61.949.100.188 ip6:98.422.200.766 a:smtp.example.com -all
```

Here's a breakdown of the sample DNS TXT record for SPF above:

The version of SPF utilized:

This should always be "`v=spf1`" (the first version) because all others have been discontinued.

The list of authorized senders:

Any domain that is sending mail on your behalf should be listed using mechanisms such as IP addresses, hostnames, or "`a`" records. You can choose to use all of the same type of mechanism or mix and match.

There are a few different mechanisms to choose from:

1. The `ip4` or `ip6` mechanism lists the actual IP addresses authorized to send on your behalf.
2. The "`a`" **mechanism** allows the incoming server to reference the "`a`" records of a domain, instead of a specific IP. As long as the IP where the email originates is found among the "`a`" records, the email will pass SPF authentication.
3. The `MX` mechanism indicates the IP addresses that your domain uses to receive mail, if an email is sent from one of those IPs, the incoming mail server should accept it.
4. The "`include`" mechanism is also used to include the SPF record of the given domain. This is what Mailgun uses as a means for customers to add all Mailgun IPs to their SPF.

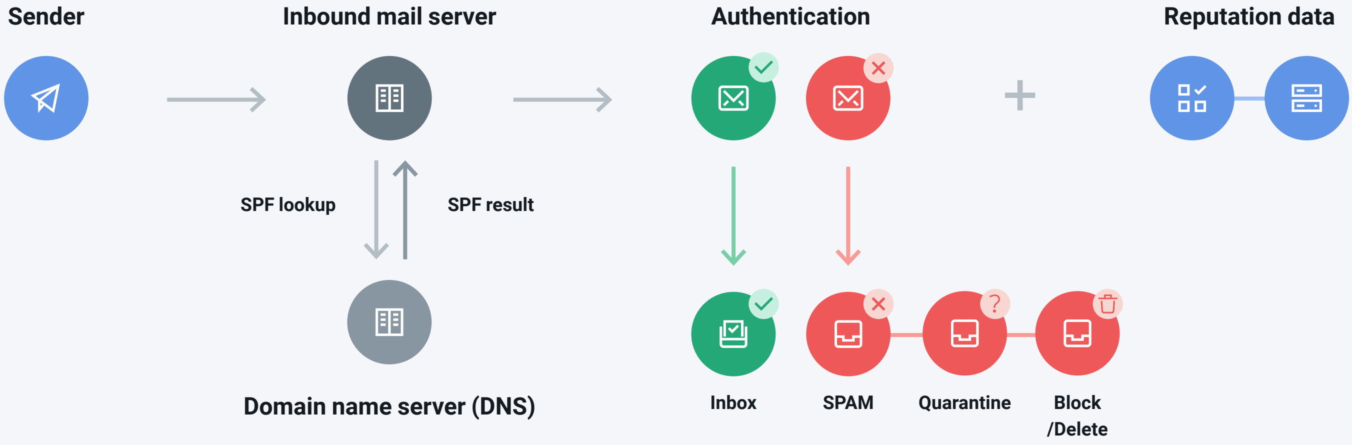
The "all" mechanism or fail qualifier:

An "all" mechanism is found at the end of every SPF record. It informs incoming mail servers on what to do if a message fails authentication.

- `–all`: If an exact match is not found; the email has failed. The message will be blocked and won't make it to the inbox in any capacity. This is the best way to use SPF to stop spoofing.
- `~all`: If an exact match is not found, the email fails but will still be delivered. However, it is marked as suspicious and will likely go to the spam folder.
- `+all`: This allows any server to send from your domain. It should rarely be used because everything will pass SPF authentication. That means anyone could spoof you as a sender.
- `?all`: This is a neutral setting. The messages don't pass or fail SPF authentication if the IP isn't listed. It leaves the decision up to the mailbox provider.

> ***Note that a domain can only have one SPF record:*** *Having multiple SPF records on a domain will cause messages to fail authentication. While ISPs don't always take action on SPF failures, it is an important part of DMARC alignment, which we'll explore later*

How SPF authentication works



When mailbox providers use SPF authentication, the incoming mail server checks the return path in the email header. It then verifies that the email originated from one of the IP addresses listed in the DNS TXT record.

If the incoming mail server verifies the sender, it will deliver the email to the inbox. If it's not found, the email will be blocked or sent to spam depending on how the fail qualifier (`all` mechanism) is defined.

SPF does have a couple of drawbacks. For one thing, it breaks when an email is forwarded. That's because it's now being sent from an IP that's not listed in the record. **SPF is also limited to 10 mechanisms (or approved IPs)**, which may not be enough for large organizations and high-volume senders with many parties sending on behalf of the main domain.

2. DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is an authentication protocol that combined two methods designed to prevent email forgery: Yahoo's "DomainKeys" and Cisco's "Identified Internet Mail."

As with SPF, DKIM authentication involves a DNS TXT record that incoming mail servers will reference when verifying the authenticity of a sender, but it's a bit more advanced. DKIM also helps determine if a message was altered in transit. Today, all major mailbox providers check emails for DKIM.

As the name suggests, DKIM involves the use of encrypted keys, also known as digital signatures. The secret key gets added to an email header in order to associate the message with a certain domain and verify the sender. The encrypted DKIM key is paired up with a public key found in the DNS TXT record.

The technical details

Here's an example of DKIM DNS record:

```
dk1024-2012._domainkey.example.com TXT "v=DKIM1; t=y; k=rsa;
p=MIGfMA0GCSqGSiuTHjQWercnvEr54A2CA;"
```

Here's a breakdown of the sample DNS TXT record for a DKIM signature:

- `v=` The version of the protocol used
- `t=` This optional tag indicates the sending domain is *testing* DKIM
- `k=` The key type, which is usually rsa
- `p=` The public key, which pairs with the encrypted DKIM signature
- The only required tag in the DNS record is the public key (`p=`). The DKIM record also includes the sending domain and the selector, the latter of which is a name or number the sender uses to tell receiving mail servers where to find the public key. **The DKIM signature header** gets added to email messages and includes the information receiving mail servers need to verify the authenticity of a message.

Here's an example of a DKIM header:

```
DKIM-Signature v=1; a=rsa-sha256; q=dns;
d=example.com;
s= dk1024-2012; t=1117574938; x=1118006938;
h=Content-Type: Mime Version: Subject: From: To: Sender; Date: List-Unsubscribe
bh=PV3AoaeTApQYJwe3qgbuUFFTVhjwhv1q2gGNBL+KHU=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

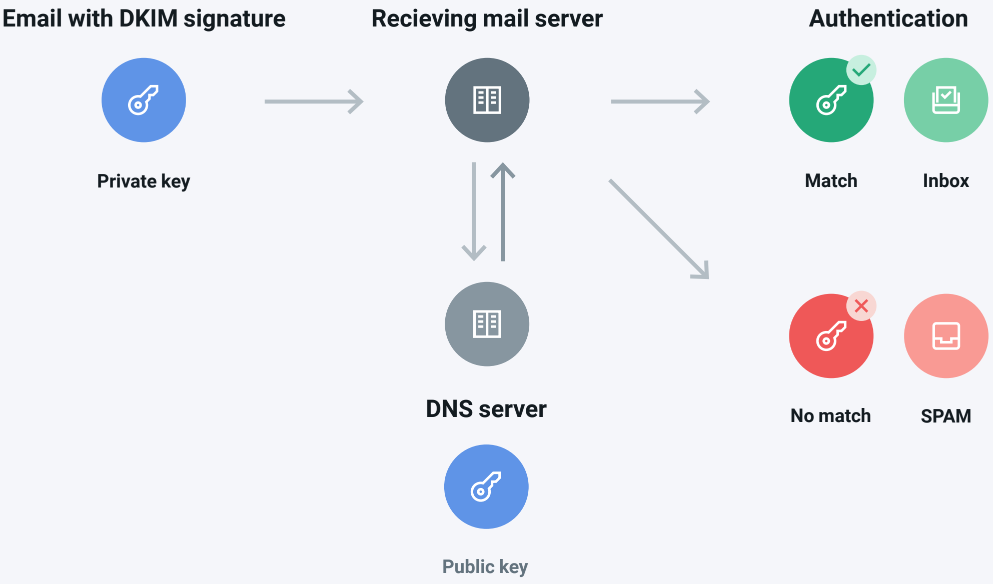
Here's a breakdown of the tags found in the sample DKIM header information above:

- `v=` The version of DKIM
- `a=` The signing algorithm
- `q=` The default query method
- `d=` The signing domain associated with a selector record to locate a public key
- `s=` The selector, which is used to lookup the public key and allows multiple keys on a domain
- `t=` The signature timestamp

- `x=` The expire time
- `h=` The list of headers that will be used in the signing algorithm
- `bh=` The body hash after being canonicalized by Base64, which turns binary code into text
- `b=` The actual DKIM signature of headers and body, which is encoded with Base64

There are also some optional DKIM tags that can be added to the header information. Other DKIM header tags are required: `v`, `a`, `d`, `s`, `h`, `bh`, and `b`. Still others, like `t` and `x`, are optional but recommended.

How DKIM authentication works



A DKIM signature lets mailbox providers and mail transfer agents (MTAs) know where to retrieve the public key. If the public key pairs with the encrypted signature, mailbox providers are more likely to deliver it to the inbox. If there is no match, or if there's no DKIM signature at all, the email is more likely to be rejected or filtered into spam.

DKIM itself does not filter emails. However, it helps receiving mail servers decide how to best filter incoming messages. A successful DKIM verification often means a reduced spam score for a message.

3. Domain Message Authentication Reporting (DMARC)

Strictly speaking, Domain Message Authentication Reporting (DMARC) isn't an authentication protocol. It's a technical specification that defines a policy for email authentication. DMARC helps senders and mailbox providers get the most out of both SPF and DKIM while providing reporting that gives insights into who's trying to send as your domain.

The main purpose of a DMARC policy is to check for SPF and DKIM alignment, and it's considered the most effective way to keep bad actors from impersonating your brand via email. When DMARC is implemented, mailbox providers check for both SPF and DKIM and then refer to the policy the sender defines in the DMARC DNS record.

DMARC policy options are:

- **Reject:** Messages that fail DMARC will not be delivered (`p=reject`).
- **Quarantine:** Messages that fail DMARC will be filtered into the spam folder (`p=quarantine`).
- **None:** Allows messages through regardless of passing or failing. Used only for reporting or during DMARC setup and testing (`p=none`).

The technical details

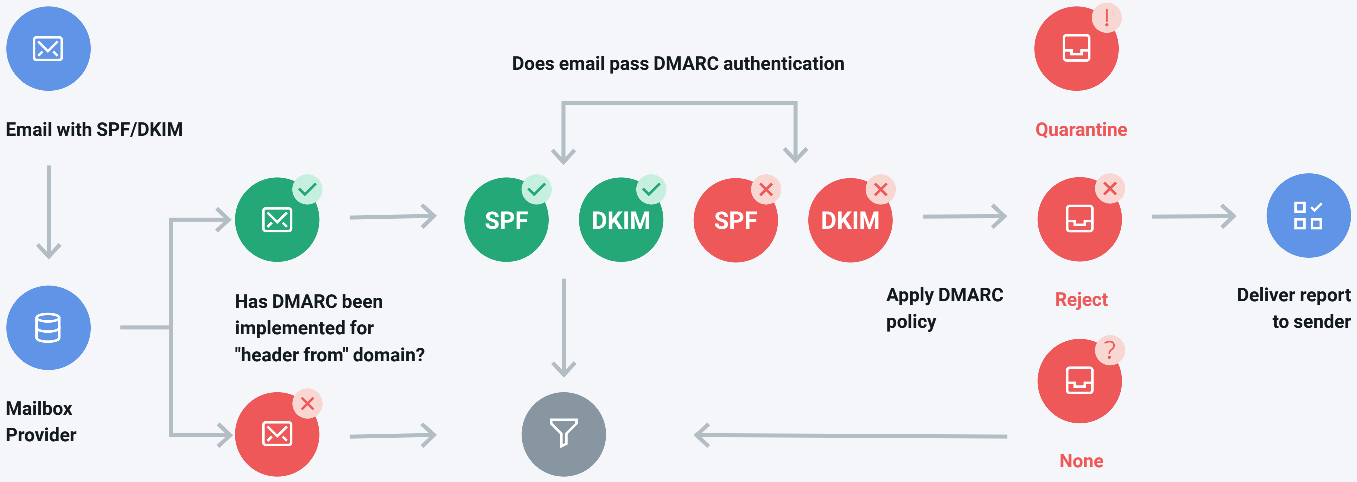
```
v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@example.com; pct=100; aspf=s; adkim=s
```

DMARC records can be somewhat simpler than this as well as more complicated, depending on how many tags a sender decides to use. Here's a complete list of possible DMARC tags with explanations:

- `v=` The version of DMARC used.
- `p=` The DMARC enforcement policy: none, quarantine, or reject.
- `rua=` A list of email addresses where DMARC aggregate reports are sent.
- `pct=` The percentage of messages that are subject to the enforcement policy. Default is pct=100.
- `aspf=` Defines the alignment mode for SPF, which could be strict or relaxed with pass/fail scenarios.
- `adkim=` Defines the alignment mode for DKIM, which could be strict or relaxed with pass/fail scenarios.
- `sp=` Represents different enforcement policies for subdomains.
- `ruf=` Lists email addresses for sending DMARC failure/forensic reports, which are more detailed than aggregate reports.
- `fo=` Indicates the options for creating a DMARC failure/forensic report.
- `rf=` Declares the forensic reporting format for message-specific failure reports.
- `ri=` Sets the interval for sending DMARC reports, which is defined in seconds but is usually 24 hours or more.

So, in our DNS TXT record example, the sender has a DMARC policy set to quarantine with no difference for any subdomains. There's an email address for receiving aggregate reports. 100% of messages are subject to the DMARC policy, and both SPF and DKIM alignment modes are set to "strict." When set to "strict", if either SPF or DKIM fails authentication, then the entire DMARC check fails.

How a DMARC Policy Works



When a sender has implemented DMARC, the mailbox provider checks to see if it passes SPF and DKIM. Then it enforces the policy listed in the DNS record and filters the email accordingly. Finally, a report is delivered to the sender with information about the email traffic sent on behalf of the domain and how it was handled.

DMARC reporting

DMARC reports provide powerful insights into how messages are moving through the email ecosystem as well as how often bad actors are trying to forge emails and impersonate your brand. As you may have noticed, there are two types of DMARC reports: aggregate and forensic.

Aggregate DMARC reports are sent daily unless otherwise specified. They will include:

- All domains that are sending mail using your domain in the "From" field
- The sending IP address for each domain in the report
- Results of SPF and DKIM authentication
- Emails that were quarantined (if your policy is `p=quarantine`)
- Emails that were blocked (if you used `p=reject`)
- Information on overall daily email traffic

> ***Note:*** *You'll probably want to set up a dedicated email address for receiving your DMARC reports. That's because daily emails are sent from every ISP that gets messages with your domain in the From field. This can end up being a lot of email for some senders.*

Forensic DMARC reports are sent every time an email fails DMARC authentication because SPF and/or DKIM are not aligned. Also known as **failure reports**, they are very helpful when you're investigating cases of spoofing and need additional details about specific messages. For example, forensic DMARC reports will include the subject line of failed messages, the `To:` and `From:` fields, as well as information about attachments and URLs in those emails.

If your team oversees email security, DMARC reports are like regular briefings that help you catch and stop problems before they get out of control.

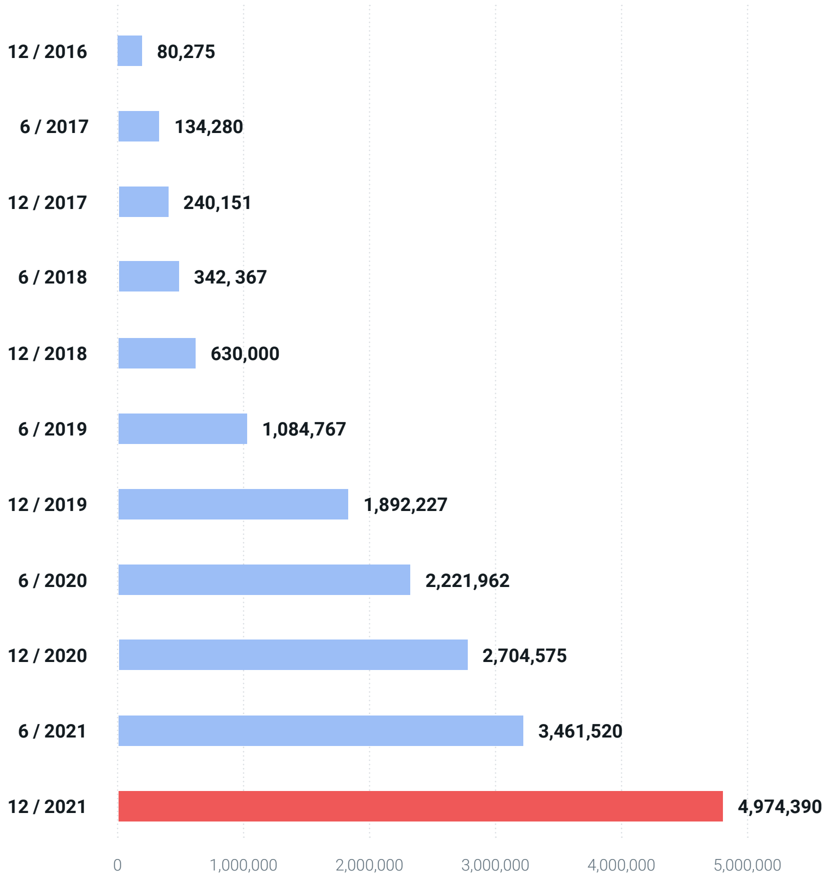
"When we first set up DMARC policies for Mailgun, it was really interesting to get those reports and see all the traffic. We started noticing all these places using Mailgun.com as the sending domain. A lot of it actually was our traffic, but we just didn't know about it. For example, our marketing team could try out a new service and the protocols aren't aligned. But, at least with DMARC reports, we can see what's happening."

Nick Schafer, Manager of Deliverability & Compliance, Mailgun

What’s the best DMARC policy?

More and more senders are seeing the value in DMARC. Recent numbers from DMARC.org indicate adoption of the specification jumped 84% in 2021 with nearly 5 million unique records at the end of the year.

DMARC adoption growth (Valid records via DNS)



However, DMARC.org also claims that **nearly two-thirds of these records (65.6%) have relaxed policies set to p=none**. That could be because some senders only want to see their DMARC reports, and they are hesitant to enforce a strict policy that rejects or quarantines failed messages. A p=none policy will give you the benefits of reporting, but it will do absolutely nothing to stop phishing attacks and brand spoofing.

Kate Nowrouzi says Mailgun encourages its users to enforce stronger DMARC policies. While it's perfectly acceptable to start with a relaxed policy, at some point senders should take the next step to improve email security.

The `pct=` tag in your DMARC record allows you to **specify a percentage of messages to which your policy should be applied**. That means you can evaluate the impact that a `p=quarantine` or `p=reject` policy might have on email deliverability without DMARC impacting all of your outgoing mail. Then, you can troubleshoot any problems using DMARC reports and gradually increase the percentage to which the policy is applied.

Kate believes the ultimate goal of DMARC is to implement a policy that actually helps mailbox providers verify legitimate senders and protects recipients from those trying to impersonate your company. But first, senders must get over their fear of DMARC.

> *"A lot of recognizable, traditional brands still consider DMARC to be new, and they have some concerns. They worry, for example, that if the policy is set to p=reject, their emails will get blocked because DMARC isn't set up right. I see a lot of brands brag that they have DMARC implemented. But if their policy is set to p=none, it's basically like not doing anything."*
>
> Kate Nowrouzi, VP of Deliverability & Product Development, Mailgun

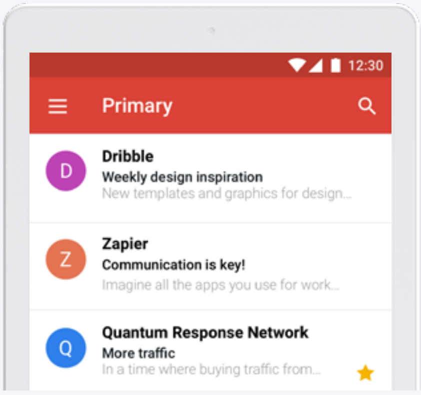
4. Brand Indicators for Message Identification (BIMI)

Another reason some senders hesitate to enforce a DMARC policy is that it may seem that there aren't many big benefits for them. It's easy to assume there's only the downside of having legitimate emails blocked or sent to spam because your email authentication records aren't perfectly configured.

To encourage stronger DMARC policy adoption, the email industry introduced Brand Indicators for Message Identification (BIMI). The result of BIMI implementation is a brand logo that appears in the inbox and at the message level. But to be "BIMI-ready" you must have DMARC with a policy set to reject or quarantine.

Here's a mockup of how BIMI logos look:

Before BIMI



12:30

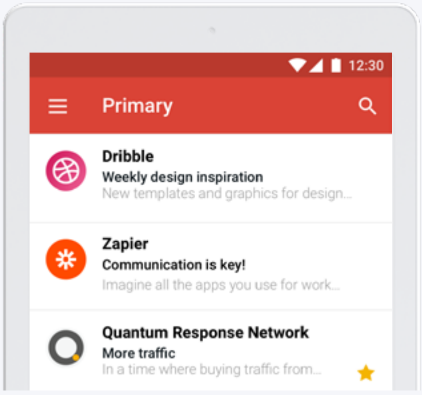
Primary

D **Dribble**
Weekly design inspiration
New templates and graphics for design...

Z **Zapier**
Communication is key!
Imagine all the apps you use for work...

Q **Quantum Response Network**
More traffic
In a time where buying traffic from...

After BIMI



12:30

Primary

Dribble
Weekly design inspiration
New templates and graphics for design...

Zapier
Communication is key!
Imagine all the apps you use for work...

Quantum Response Network
More traffic
In a time where buying traffic from...

When a mailbox provider receives a message from your brand, it first uses the DMARC record to look for SPF and DKIM authentication. If it passes DMARC, the mailbox provider may look for a BIMI DNS record, which is where an SVG image file of the brand's logo is stored.

BIMI logos are something that marketers and anyone else who cares about branding will want. However, it's the technical teams who are asked to set up BIMI records. And the first step is making sure you've got all the other email authentication protocols set up correctly, including an enforced DMARC policy.

For that reason, you could view BIMI as a sort of reward for senders who get serious about email authentication. Mailgun's Jonathan Torres says the email industry "hit the mark" with BIMI as a motivator for DMARC implementation.

Gmail started supporting the standard in 2021, making it a much more attractive incentive. This summer, Apple announced BIMI support for the Apple Mail email client in iOS 16. It will also be part of macOS when the Ventura operating system is released in October 2022.

However, Jonathan also believes it's possible that mailbox providers could move from rewarding senders with DMARC authentication to making it a requirement for inbox placement.

> *"At some point, mailbox providers may decide to prioritize messages from senders that have DMARC policies set to reject or quarantine, because those are the ones they can verify and trust. We haven't seen anyone take that step yet, but the groundwork is there to require senders to have a DMARC policy set to something besides p=none. That might be what it takes for adoption."*

Jonathan Torres, TAM Team Manager, Mailgun

Email authentication and reputation

Let's be honest. While inbox logos are nice to have, they're not much more than a vanity symbol for CMOs and email marketers. There are more important reasons to focus on email authentication: **sender reputation and brand reputation**.

Sender reputation is like a credit score for organizations sending email. It's basically a measure of your trustworthiness and the quality of your email communications.

Mailbox providers are paying attention and keeping score. They use spam traps to find senders who acquire contacts in shady ways. They know how often subscribers are opening and engaging with what you send. They know if messages are being ignored, deleted, or marked as spam. That's why **the better your sender reputation is the better your email deliverability will be**.

It's also why Mailgun includes metrics like unsubscribes and spam complaints in the Acceptable Use Policy, and it's why the platform includes tools and services for monitoring sender reputation. We want trustworthy senders on our platform, and we want to help users improve their email sender reputation.

The use or lack of email authentication will also impact sender reputation and deliverability. Use email authentication correctly and you'll increase the chances of your messages getting successfully delivered. But fail to focus on authentication and mailbox providers are less likely to view you as a trustworthy sender. That's one reason why Mailgun requires DKIM and SPF while we strongly recommend DMARC implementation.

Technical teams may not believe that **brand reputation** is their responsibility. So, it might be easy to feel a disconnect between brand spoofing and your job. However, if your role touches cybersecurity in any way, one of the primary things you're protecting is brand reputation. You don't have to be a marketer to care about the brand.

"I think the importance of protecting a sender's brand is becoming a bigger topic in the email space because of the way the industry is changing. Brand is everything. If people lose confidence in your company because they're unsure if emails that appear to be from you are safe, it can permanently damage your reputation."

Jonathan Torres, TAM Team Manager, Mailgun

PART 6

Picking the right partners

Trust is certainly a crucial factor when it comes to security. It's crucial to all sorts of relationships and partnerships. Just as mailbox providers need ways to identify trustworthy senders, you need ways to find trustworthy vendors in the email space.

Mailgun's email security and compliance experts offered their perspective on what to look for in a SaaS partner who follows best practices.

Audits and certifications

Perhaps one of the most obvious ways to evaluate a potential partner is to examine the standards they adhere to and the certifications they've earned. As luck would have it, Dan Ross, Mailgun's Sr. Manager of governance, risk, and compliance was going through some major audits at the time.

Dan has insights into what these audits and certifications are as well as what they mean to you as an email sender.

SOC 2 Type I and II Audits

A SOC 2 report will provide you with assurance about an organization's security, availability, processing integrity, confidentiality, and privacy controls. It is based on compliance with Trust Services Criteria (TSC) from the American Institute of Certified Public Accountants (AICPA).

- **The SOC 2 Type I audit** assesses the design of security processes and looks at whether security controls are in place at a specific point in time.
- **The SOC 2 Type II audit** evaluates how well those security controls work while observing operations over the course of six to twelve months.

For example, when auditors put together the SOC 2 Type II report on Mailgun, they evaluated things such as employee cybersecurity awareness training. The auditors took 25 names and checked to see if those employees underwent training and completed the test.

Auditors also examined 25 different code changes to the Mailgun platform to see if each of those changes followed best practices, which included whether Mailgun conducted quality assurance (QA) on it, and that the new code was reviewed for security vulnerabilities.

Another aspect of SOC 2 Type II is the ability to add HIPPA controls to the audit, which Mailgun does. Finding an email service provider with a SOC 2 Type II report is relatively rare. However, Dan says that report is what you really need if you care about finding partners who follow privacy laws. His team gets grilled with questions from auditors as they build the full report.

"The SOC 2 Type II actually audits whether security controls are working efficiently. When Mailgun goes through a SOC 2 Type II audit, it is 12-hour days for a couple of weeks. It gets pretty intense."

Dan Ross, Sr. Manager GRC, Mailgun

ISO 27001 and 27701 certifications

International standards (ISOs) help consumers and B2B buyers gauge safety, quality, and in this case, the security of products and services. ISO 27001 and ISO 27701 are international standards that evaluate information security and privacy controls.

If a potential partner has an **ISO 27001 certification**, it shows they've established, implemented, are maintaining, and continually improving an information security management system (ISMS). Essentially, the standard certifies that a partner has the right processes and policies in place, and they are building upon information security year over year. In a SaaS partnership, this means the platform keeps getting more secure for customers and users.

Dan says that includes factors like a security budget and team that keep growing annually rather than being reduced.

An **ISO 27701 certification** expands on the ISO 27001 standard by covering areas of privacy controls in a privacy information management system (PIMS). This standard was introduced in 2019 to help evaluate an organization's compliance with laws such as GDPR and CCPA because it maps against these and other privacy regulations.

While these two ISO certifications don't guarantee a potential partner is fully compliant, it is a strong signal that the organization is doing everything it can to protect customer data. And finding a compliant partner for email is important, because it is directly connected to your own organization's compliance.

> *"There isn't a specific GDPR certification because it's the law. You can't be certified in that because you have to follow the law. But the way we prove that's happening is by having certifications like ISO 27701, which we can give to our customers and show that we are actually doing what we say we do."*
>
> Dan Ross, Sr. Manager GRC, Mailgun

Other certifications and security policies

Beyond the major security audits and standards, there are other questions you'll want to ask potential partners. Dan says that may include things such as how they manage access to your data, how they respond to cybersecurity breaches, as well as data backups, geographic redundancy, and disaster recovery.

You may also have questions about user security, including things like single sign-on (SSO) and multi-factor authentication (MFA). There could be specific concerns with PCI certification, you may have questions about security inside physical offices, or perhaps you want to review a network diagram. **A reliable partner will answer all your security questions and deliver any documentation you need.**

Get the details on Mailgun security.

At Mailgun, we provide a comprehensive security portal that is home to all sorts of documentation that our customers and prospects may ask us about.

Protecting the product

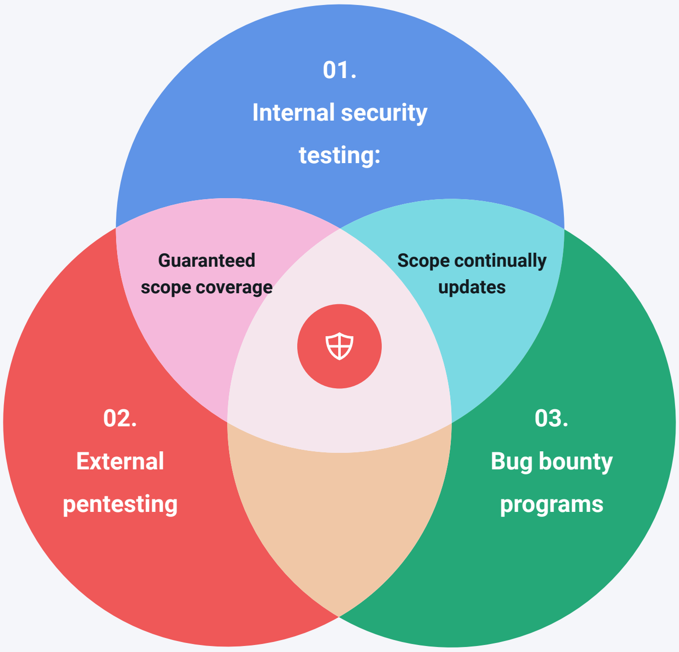
Steve Proud is Director of Security Engineering at Mailgun, which means he's in charge of protecting our platform and keeping it safe for senders to use. He says the controls we covered in the previous section (ISO 27701 and SOC 2 Type II) are important factors no matter what type of technology partner you're evaluating. That's because cybercriminals are relentless.

> *“Hackers are constantly attacking applications exposed to the internet. Whether it be an email sending platform or a social network, organizations should leverage partners that have a robust security program in place to ensure there is governance and structure in the way security is implemented across people, processes, and technology."*

Steve Proud, Director, Security Engineering, Mailgun

Before signing a contract with a partner that provides email solutions get some details on how they protect their application from cybersecurity threats. The Mailgun Security team applies a three-pronged strategy to protecting our platform.

Product security "triple threat" approach


01.
Internal security testing:
Guaranteed scope coverage
Scope continually updates
02.
External pentesting
03.
Bug bounty programs

1. **Internal security testing:** Does the prospective partner have in-house security experts who test product updates prior to rollout?
2. **External pentesting:** Is the prospective partner using a third-party cybersecurity testing service that goes beyond the standard audits and reports?
3. **Bug bounty programs:** Are security researchers and white hat or “good guy” hackers invited to look for unknown security vulnerabilities on the prospective partner’s platform?

In this guide, you've already met some of the people involved with Mailgun product security. They include Dan Ross, who says asking about "change management" is an important part of evaluating a potential technology partner. **Are the product and security teams testing new code for vulnerabilities before it's pushed live?** Here at Mailgun, they always are.

Steve Proud says constant vigilance is needed in his line of work, and just as important, your potential partners should have a plan for remediating security situations quickly and efficiently.

> *"Email senders need to carefully consider who they choose to partner with when evaluating email marketing and deliverability tools... It is not a matter of if vulnerabilities and misconfiguration will be discovered, it's simply a matter of when and it's important to ensure your partners have a methodology in place that allows swift action to occur to push new, secure code out to the environment, thus mitigating the effect of that vulnerability."*
>
> Steve Proud, Director, Security Engineering, Mailgun

Security and automation

Even with the best and brightest information security team, it's tough to stay on top of trends and stay ahead of bad actors. That's why a strong partner will also **automate security measures so they can respond to threats quicky and effectively**.

Dan Ross explains that, while Mailgun has a talented team, we're all human and sometimes humans miss things that machines don't. So, Dan and his colleagues have worked to "take the thinking out of security." That may sound odd, but it simply means there are automated tools in place to alert the security team to an issue almost instantaneously.

Mailgun utilizes internal security tools that enable us to monitor threats on the network and on endpoints in real-time with staff dedicated to investigating every alert that comes in. For example, if a remote employee's computer is behaving strangely, the security team knows and addresses it before the employee has any idea that something is wrong.

Nick Schafer says that sort of automation extends to what happens inside the Mailgun application, because we want to make sure the emails that leave our platform are safe, secure, and legitimate.

> *"If we had to rely on manual human actions alone, we'd be too slow. Even if we think we're acting quickly, thousands of potentially harmful messages could be getting out the door. So, we have all sorts of alerts and automations in place to notify us and stop malicious stuff from happening."*
>
> Nick Schafer, Manager of Deliverability & Compliance, Mailgun

Customer education

Finally, a good partner in email security will share their knowledge and expertise with you. As we've seen, cybersecurity threats are always evolving, and email is at the center of the action. So, an email solution provider that keeps you and your organization in the loop is very valuable.

At Mailgun, there's a lot of education that goes into place to make sure our customers aren't accidentally doing something that goes against best practices or potentially breaks the law.

Jonathan Torres explains that we do this proactively by making sure email security issues are addressed during onboarding as well as with the customer's Technical Account Manager (TAM) on an ongoing basis.

> *"Not every vendor brings up the topics of security and compliance. We want to talk to customers about these issues, and we're more than willing to advise them on best practices, even when a problem isn't directly connected to our product."*
>
> Jonathan Torres, TAM Team Manager, Mailgun

PART 7

How Mailgun can help

Hopefully, we've convinced you that a secure platform for sending email is of extreme importance. From user security measures to stopping the bad guys to our strict adherence to compliance standards, it's all in a day's work here at Mailgun by Sinch. Call us weird if you want, but we love what we do.

"Our team is really passionate and experienced. We legitimately enjoy the job of keeping bad actors off the Mailgun platform. It's fun because it's kind of like a superhero thing. I like to tell my kids that we're the good guys protecting the platform."

Nick Schafer, Manager of Deliverability & Compliance, Mailgun

By now, you should also understand how having a partner that places email security and compliance at the top of its priority list is a valuable asset to any organization. Mailgun by Sinch is ready and willing to be that partner for you.

Here's a recap of how we partner with our users on email security and compliance:

- **Secure data centers:** Mailgun's cloud-based services are built on top of industry-leading GCP infrastructure. All data centers are equipped with around-the-clock surveillance and biometric access control systems.
- **Redundancy, data recovery, and backups:** Data centers are equipped with at least N+1 redundancy for power, networking, and cooling infrastructure. Within a region, data processing occurs across at least three distinct availability zones. Daily account data back-ups with incremental/point-in-time encrypted recovery occur on all primary databases.
- **Encryption:** Mailgun utilizes AES-256 encryption-at-rest to protect customer data and applies opportunistic TLS encryption to protect messages sent from the platform in transit.
- **Regulatory compliance:** Mailgun meets or exceeds GDPR and CCPA compliance to protect the privacy and integrity of customer data. Rights and responsibilities for HIPAA compliance are defined in a Business Associate Addendum. Stripe serves as our PCI-compliant payment processor.
- **Reports and certifications:** We are ISO 27001 and 27701 certified. Mailgun also has SOC 2 Type I and SOC 2 Type II reports, which means our security controls are mapped against regulations including GDPR, CCPA, and HIPAA. Additionally, all providers are SOC Type II and ISO 27001 certified.
- **Employee access and awareness:** Mailgun limits access to data and systems based on job roles. Administrative access to Mailgun systems and services follows the principle of least privilege. All employees are required to undergo annual cyber-awareness training including a yearly individual assessment.
- **Application security:** SAML and 2FA are available for customer logins. An intrusion detection system (IDS) is in place to catch unauthorized account access. Product code changes are tested for security vulnerabilities, and a third-party bug bounty program helps Mailgun identify unknown issues.
- **Platform protection:** Mailgun has tools, automated systems, and employees dedicated to keeping bad actors off the platform and monitoring our network for suspicious activity. An Acceptable Use Policy outlines expectations for users.
- **Email authentication:** SPF and DKIM authentication are required when using the Mailgun platform. In addition, an enforced DMARC policy is highly recommended.

Security, compliance, and email authentication are complex issues. That's why Mailgun provides Technical Account Managers (TAMs) to help during onboarding and throughout a customer's contract. We can even assist with tasks such as DKIM and SPF implementation. Plus, we're more than willing to talk about these topics and provide helpful advice.

"We have a very close relationship with our customers, which includes a deep-dive education on best practices for things such as email authentication and compliance. Then every year, we meet with our customers to re-educate them and inform new people who've come on board. We do all this because we really care about their success as a sender and making sure they know the risks."

Kate Nowrouzi, VP of Deliverability & Product Development, Mailgun

Still need some answers? Find out more about security and compliance at Mailgun by Sinch when you visit our dedicated security portal. Don't hesitate to contact us with questions about security, compliance, or any other matter. We're always happy to explain how Mailgun keeps email safe.

PART 8

Resources

Dive deeper into email security, compliance, and authentication with detailed information, articles from the Mailgun blog, studies cited in this guide, and other helpful external resources.

Resources on Mailgun.com

- The Mailgun Security Portal: View or request access to our policies, certifications, and reports. That includes ISO 27001, ISO 27701, and SOC 2 Type I and II reports.
- GDPR Hub: Find out how Mailgun complies with the European Union's consumer privacy law.
- HIPPA Business Associates Addendum (BAA): Get information on rights and responsibilities regarding the protection of private health information.
- Data Processing Agreement: Get the details on how Mailgun handles customer data.
- Acceptable Use Policy (AUP): Review the guidelines required of users on the Mailgun platform.

Helpful Mailgun content

- Email security best practices: How to keep your email program safe
- Email scams glossary
- How does Mailgun keep your emails protected?
- Vulnerability management: Working with the community to patch security threats
- TLS basics: What is TLS connection control?
- Understanding DKIM: How it works and why it's necessary
- Implementing DMARC: A step-by-step guide
- Which SMTP port should I use?
- Phishing emails: How to identify them and protect yourself
- Case Study: Optimizing data privacy for scalable and secure email

Email authentication resources

- Open-SPF.org: Find out more about the Sender Policy Framework project.
- DKIM.org: Find out more about DomainKeys Identified Mail authentication.
- DMARC.org: Find out more about Domain-based Message Authentication, Conformance, and Reporting.
- BIMIGroup.org: Find out more about Brand Indicators for Message Identification.
- The path to BIMI implementation: Get more on BIMI setup from Email on Acid by Sinch.

External sources in this guide

- IBM: Cost of a Data Breach Report 2021
- Cisco: 2021 Security Threat Trends
- Mimecast: State of Email Security 2022
- Proofpoint: 2022 State of the Phish
- GreatHorn: 2021 Email Security Benchmark Report

mailgun
by sinch

Over 100,000 companies worldwide use Mailgun by Sinch to create elegant email experiences for their customers through world-class infrastructure. Brands like Microsoft, Lyft, and Dell trust Mailgun's innovative technology and reliable infrastructure to send billions of emails every year. Built with development teams in mind, Mailgun makes sending, receiving, and tracking emails effortless for email senders of all sizes.

Mailgun was founded in 2010 as a response to the lack of developer-friendly, API-based email services. Since then, Mailgun has joined **Sinch**, a leading Communication Platform as a Service (CPaaS) provider, to become the developer-first email solution for their global customer base. GDPR, HIPAA, and SOC I & II compliant, Mailgun aims to provide the best email service possible with the utmost security and privacy.

For more information, please visit **mailgun.com**.