

Communicate
DMARC to
Clients

Table of Contents

Communicate DMARC to Clients	2
Too Small To Be a Target?	2
No In-House IT Team? Your MSP Can Help!	3
Budget Issues? DMARC Is Affordable For SMBs!	4
Email Authentication: 3 Easy Steps to Get Your Customers Compliant	5
4 Crucial Results of DMARC Compliance	6
What Comes After DMARC?	7
Top 3 Client Communication Best Practices	8
Keep It High Level, Don't Overexplain	8
Be Practical While Talking about Threats	8
Show What Compliance Looks Like	9
Don't Postpone the Conversation With Your Clients	9

Communicate **DMARC** to Clients

Email continues to be the primary vector for phishing and spoofing. [KnowBe4 mentions](#) that 96% of social engineering attacks start with an email.

According to the [FBI's 2021 Internet Crime Report](#), phishing is the top cyberattack type. It's been growing rapidly since 2020 and shows no signs of stopping. The same report notes that the 19,954 reported business email compromise (BEC) and email account compromise (EAC) attacks have caused \$2.4 billion in adjusted losses.

This loss amount is, of course, far less than the actual number. While it's hard to find definitive statistics on the exact percentage of reported attacks, we know that SMBs are an excellent target for cyberattacks. According to [Verizon DBIR 2022](#), 43% of all data breaches involve SMBs.

Too Small To Be a Target?

According to [digital.com](#), more than half of their research pool claimed that they don't have cybersecurity measures in place, with 59% of them claiming that their business was 'too small' to be an attack target.

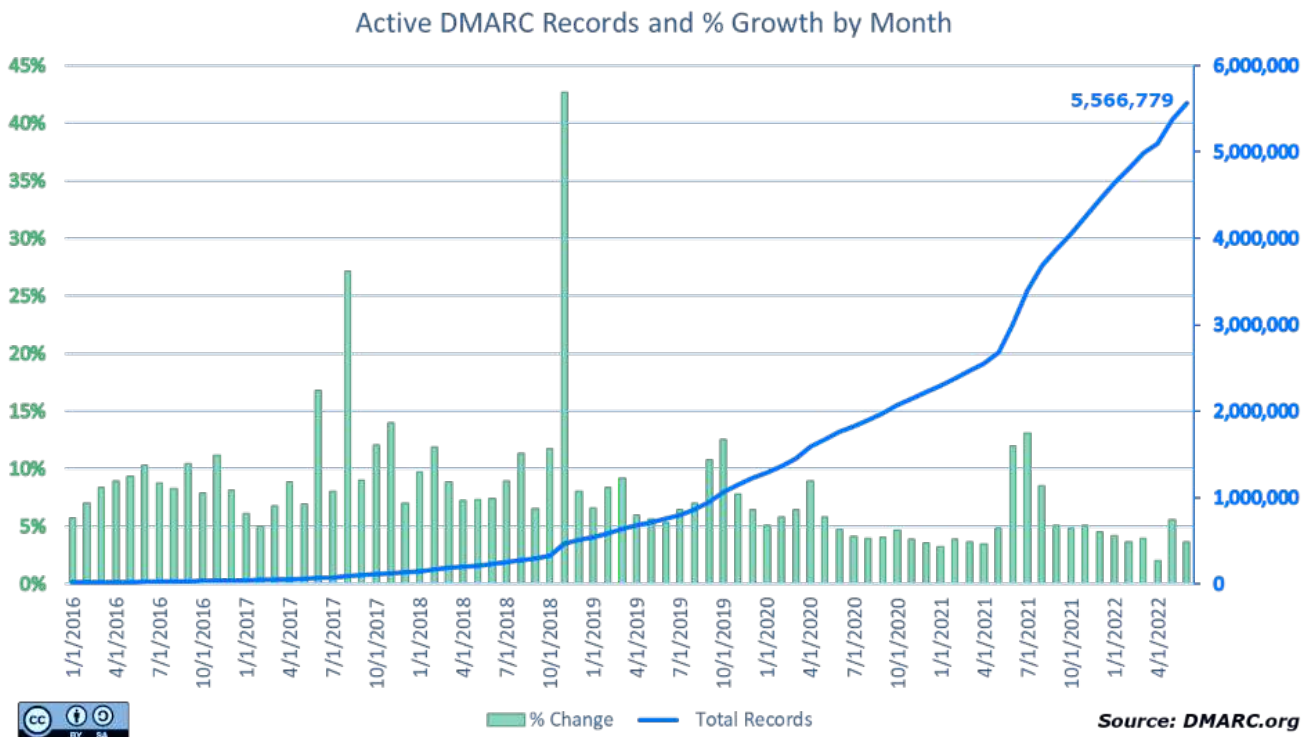
As security experts, we understand how sorely business owners miss the point. There's no "too small" for bad actors. If it's easy enough to break the infrastructure, they will do so. No data is too trivial for a hacker, especially when 87% of the same businesses store highly sensitive customer data such as name, birth date, address, credit card information, and even social security number.



One of your main goals is to help your customers understand that they're missing the crucial tools email authentication provides them against spoofing and phishing.

No In-House IT Team? Your MSP Can Help!

This one is understandable and easy to fix. Many companies don't have in-house IT teams; otherwise, they wouldn't need your help with cybersecurity. However, as the frequency (1 phishing or ransomware attacks [per 11 seconds](#), which amounts to about [3 billion](#) attacks) and cost of cyberattacks rise (predicted to [reach \\$10.5 trillion](#) by 2025), businesses are sure to come around and start asking for easy cybersecurity and email security solutions.



DMARC adoption is also on the rise. [Data on dmarc.org](#) shows that the number of valid DMARC records is growing fast. The 2022 mid-year report counts 5,566,779 domains compared to the 3,461,520 of the previous period.

[DigitalJournal conducted research](#) estimating the global DMARC Software market size at \$254.56 million in 2022. If the growth remains steady at a CAGR of 37.53%, this number will reach \$1722.74 million by 2028.

We won't be wrong to predict that there's a huge potential in the email authentication market, and your MSP should take advantage of the opportunity this growth presents.

Budget Issues? DMARC Is Affordable For SMBs!

Operating on tight budgets is typical for any SMB. Most of them can't spare a dime for hiring a security specialist, pentesting, employee training, or even paying for a proper cybersecurity plan.

This is only one of the reasons that email authentication usually becomes an afterthought. In 2022, [83% of organizations](#) experienced a successful email-based phishing attack due to human error (clicking a bad link, downloading malware, providing credentials, and executing a wire transfer). In 2020, this number was 46% lower. Businesses might go out of business as a result of cyberattacks.

Usually, businesses start paying attention to security issues only after a devastating attack. It's no secret that the COVID-19 pandemic led to a sharp increase in cyberattacks, especially phishing. [According to KnowBe4](#), the first quarter of 2020 saw a 600% increase in phishing attacks.

The [2022 study by UpCity](#) found that 25% of SMBs spent less than \$500 on their monthly cybersecurity plan before COVID-19. During last year, this amount almost tripled among 26% of the research sample. The [Email Security Trends Report](#) from Barracuda also confirms that 1 in 4 organizations increased the budget they spend on email security.



Email Authentication: 3 Easy Steps to Get Your Customers Compliant

Email has always been challenging to protect. Although the domain holder owns the communication channel, email has always stayed non-secure. Each email authentication protocol (SPF, DKIM, and DMARC) has limitations and is challenging for non-technical people.

If taken separately, each protocol can only do as much to protect your domain infrastructure. But together, SPF, DKIM, and DMARC offer ironclad security against spoofing and phishing attacks on your domain's behalf.

As specialists, you might be well-versed in the protocols' technical aspects, such as setting up and configuring them. However, your clients need the answer to the "Why is my business at risk?" question. They need to understand the gist of the protocols and why their implementation is a top priority for their businesses. Here's how we explain each protocol in a simple analogy.

Imagine that your domain is a friend group where any member has a unique identifier for sending physical letters. A rival friend group tries to discredit your name by sending letters to your contacts and trying to fake your communication.

1

As a first step to protect your contacts, you decide to make a list of all the friends in your group and publish it to ensure everyone knows whose letters are the "official" ones and ignore the ones from the rivals. In email authentication, **SPF accomplishes this exact effect.**

2

As the second security measure, you start using a specially engraved "logo" on the letter to ensure that the rivals don't intercept your communication, open the envelope and change the letter's contents. **DKIM is this identifying stamp.**

3

While these measures are secure, more is needed. You set up a checking station where all the letters are submitted for inspection and program it to act on specific rules. E.g., if the letter matches "John's friend list" and contains an engraved eagle, deliver them at once. **DMARC is this checking station.**

After you set up these three measures of protection, hardly anyone will be able to fake your communication. The same happens with your domain infrastructure after implementing email authentication protocols. You secure your email environment from impostors posing as your business.

This example might not be too precise in the technical sense, but it's to the point and helps a non-expert get the gist of email authentication. We urge you to seize the moment and impress on your customer the necessity of having the protocols in place.

Let your clients regain



4 Crucial Results of DMARC Compliance

Becoming DMARC compliant can be challenging and meticulous and takes time and effort. The journey from the policy "none" to "reject" can last between 2 weeks to 6 months, depending on various factors like the size of the organization, number of sending sources, and email sending volume.

However long it lasts and however meticulous the process is, your organizations that reach compliance have what others don't:

Email deliverability and inbox placement

Visibility to the domain infrastructure

Operations and communications security

Business identity ownership and control

Help your clients stand out with DMARC compliance and combat spoofing and phishing protection. Become an EasyDMARC MSP partner to get access to our marketing materials, training, and expert help to boost your customer base.

[Become a Partner](#)

What Comes After DMARC?

Reaching policy "reject" is a crucial milestone. However, it's not the end of your DMARC story.

Constant Monitoring

Keeping an eye on your DMARC reports is one of the best email authentication practices. Email environments aren't set in stone, so you must also adjust the configurations in time. Depending on your organization's needs, new sending sources might be added or removed, and the new ones will need configuring.

In addition to new sources, it's always good to review email sending patterns, deliverability issues, and changes in the system. Staying alert always helps keep the infrastructure up-to-date, register occasional phishing attempts, or manage alerts and anomalies.

BIMI: Crown Your Secure Domain Infrastructure

Having a secure domain environment is excellent, but BIMI could turn your email authentication up a notch. Brand Indicators for Message Identification is a protocol that enables company logos on your emails (in email clients that support the protocol). It's the Crown jewel of email branding.

To start with BIMI, you must reach full DMARC compliance, acquire a VMC certificate, and set up the BIMI record in your DNS. While not imperative, this protocol helps businesses stand out in customer inboxes, boosting brand recognition and enhancing user experience. Your secure branded emails will be unmistakable in the user's inbox.

Top 3 Client Communication Best Practices

Keep It High Level, Don't Overexplain

Your number one goal during the sales process is to make your clients realize their business might be at risk, and email authentication is the way forward to protect them from spoofing and phishing attacks.



The deeper you go on the technical side, the further you drift from selling the product.

Technical details only confuse non-technical people. In the end, you're supposed to be their technical support, and they don't have to know how things work in the background. Explaining the gist of the protocols will keep your conversations light and facilitate the sales process. Your goal is to use simple terms to communicate that you'll protect their domains at the highest levels.

Be Practical While Talking about Threats

Show, don't tell. DMARC can be convoluted to understand, even for a cybersecurity enthusiast.



Use our DNS Checker tool to share a screen and show the existing issues to the customer.

This way, they'll gather a better understanding of the issues their domain infrastructure is facing and be more willing to fix them. Once they see the risks of non-compliant threats against their domains, the value of compliance is undeniable. At this point, you can tell them about the compliance journey and ensure that the information registers.

Show What Compliance Looks Like

The next step is to show the customer a compliant domain and how things stand with it.



Talk about the benefits of an authenticated email environment, a high deliverability rate, and good domain standing.

You can use a compliant domain and show them the authentication process or how things look for that domain, focusing on the fact that the risk of fraud in their business domain has been mitigated. In any case, the demonstration should enforce the idea of visibility, command, and control for their infrastructure and show that their emails can safely navigate to customer inboxes.



Don't Postpone the Conversation With Your Clients

It's time to expand your revenue while ensuring your customers get the added value of email authentication and DMARC compliance. Act as the expert your clients deserve: give them peace of mind by securing their domain infrastructure.

Contact our dedicated DMARC MSP professional today to learn more about our services and get a quote based on your needs.

[Contact Us](#)



673.70

