ADVANCED CYBER DEFENCE SYSTEMS

Email Security for SMBs

Explaining DMARC

Elliott Wilkes and Paige Mullen

Table of Contents

Email attacks are on the rise, and SMBs are the key target.

Why? Because hackers and cybercriminals are infiltrating SMBs to reach bigger companies in the supply chain.

This means that securing your email is crucial to protect not only your *own* business but also the entire network of businesses you work with.

A breach can cause substantial reputational damage, significant monetary losses, and disruption to output.

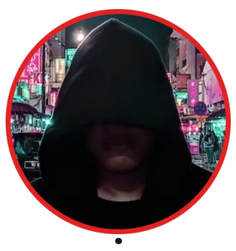
So, why aren't more SMBs implementing email security software to protect themselves and their supply chain?

Unfortunately, many adopt the 'it won't happen to me' attitude. But the risk is real and should not be ignored – once you've been hacked, it's already too late.

ACDS' Email Guard solution analyses your domain's email security technologies (i.e. DMARC, DKIM, SPF, TLS and others) and guides users to the correct configuration, which will help prevent spoofing and other attacks.

In this eBook, you'll gain a comprehensive insight into what DMARC is, its uses, and why it's an essential tool for SMBs looking to secure their email communications.

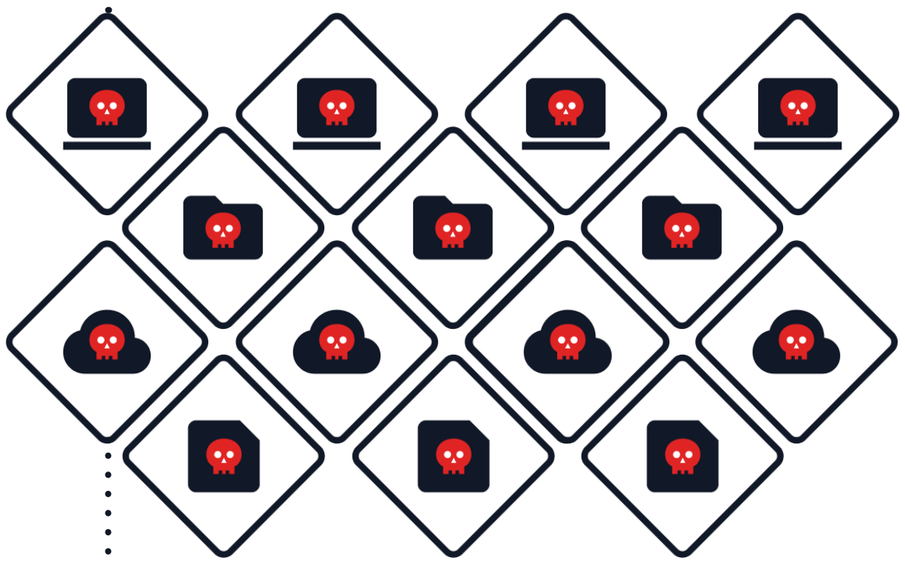
Understanding email threats



Send email
A cybercriminal sends an email containing malware or a phishing link to a target, posing as a legitimate entity like a bank or supplier.

Opening email/link
The recipient opens the email or clicks on the link, unknowingly allowing the malware to enter their system.

Malware takes over system
Once the malware has entered the system, it can take control of files and steal sensitive information.



Potential spread of malware
If a business is infected, the malware can spread to other systems within the network, causing further damage.

Email threats have become the most used method for cybercriminals to infiltrate businesses.

According to a study conducted by Verizon, 94% of malware is delivered through email. This means that, even with advanced firewalls or antivirus software in place, your business is still vulnerable if you don't have proper email security measures.

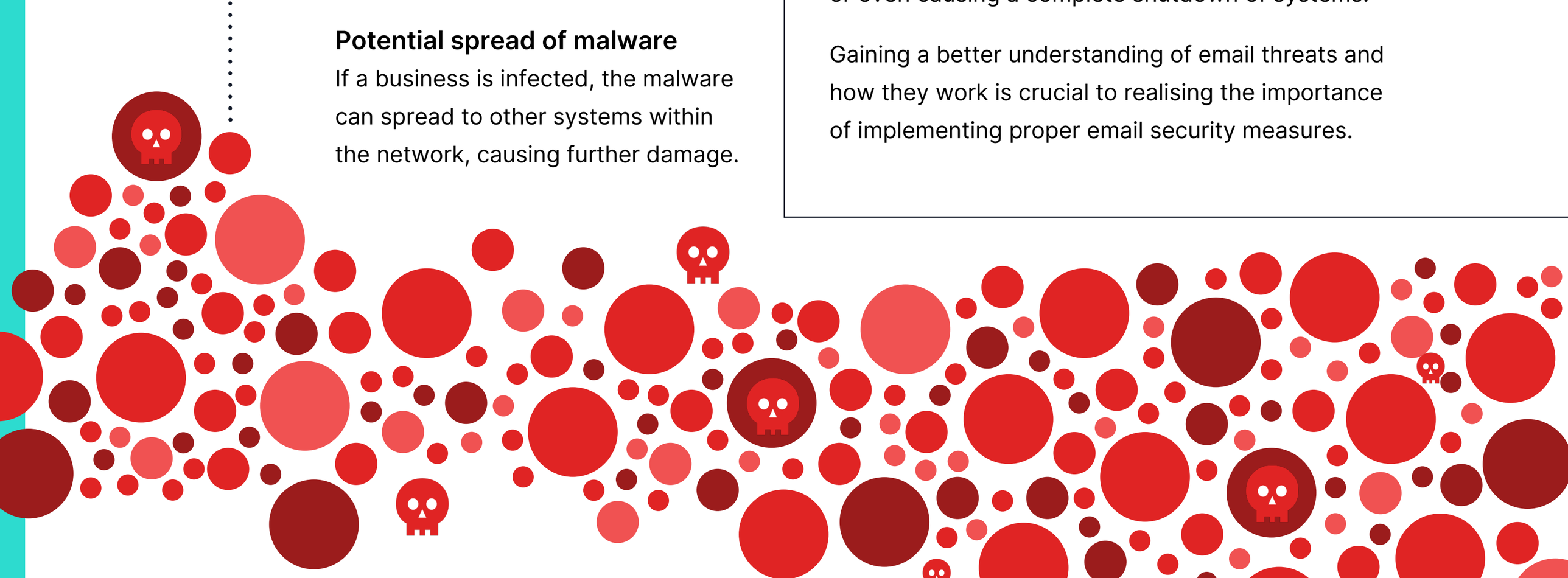
One of the reasons email threats are used is because they're easy to execute and can reach a large number of targets quickly. In addition, email attacks are constantly evolving, making it difficult for traditional security measures to keep up.

The way an email scam works is that a cybercriminal poses as a legitimate entity, such as a bank or supplier, and sends an email containing malware or phishing links. Once the recipient opens the email or clicks on the link, their system becomes compromised.

This table sets out the chain reaction of sending an email threat.

It doesn't take long for an email attack to cause significant harm. This could include accessing sensitive data, compromising financial information, or even causing a complete shutdown of systems.

Gaining a better understanding of email threats and how they work is crucial to realising the importance of implementing proper email security measures.



Types of email threats

The proper email security measures can protect your business from the damaging consequences of email attacks.

Not only that, it also ensures your business is compliant with industry regulations and standards. It can even help if you're trying to obtain or reduce your cyber security premium.

However, cybercriminals use different types of email threats, each unique in how it can cause harm.

Email threats come in various forms, such as phishing emails, spam emails, and malware attachments. Each carries a different danger and requires specific security measures to combat them.

A Real-Life Scenario: BEC Attack

Imagine receiving an email from your supplier informing you of a change in payment details. You follow the instructions and make the payment to the new account number provided. However, when you check with your supplier later, they have no knowledge of this change.

This is an example of a BEC attack where cybercriminals pose as trusted partners and request sensitive information or financial transactions. In this case, the recipient lost money and sensitive information due to insufficient email security measures.

As you can see, email threats come in various forms and can cause significant harm to your business if not properly addressed.

This is where DMARC comes in.

PHISHING ATTACKS

One of the most common types of email threats.

In these attacks, cybercriminals impersonate a legitimate company or individual and send emails containing links or attachments that lead to fake websites designed to steal personal information such as login credentials, credit card numbers, and other sensitive data.

SPEAR-PHISHING

Takes phishing attacks one step further by targeting specific individuals within an organisation, often using information gathered from public sources to make the email appear more legitimate.

These attacks are highly targeted and can be difficult to detect.

BUSINESS EMAIL COMPROMISE

Types of email attack where cybercriminals pose as a high-level executive or trusted partner and request sensitive information or financial transactions from employees.

These attacks can result in siphoning large amounts of money or sensitive data from a business.

SPAM EMAILS

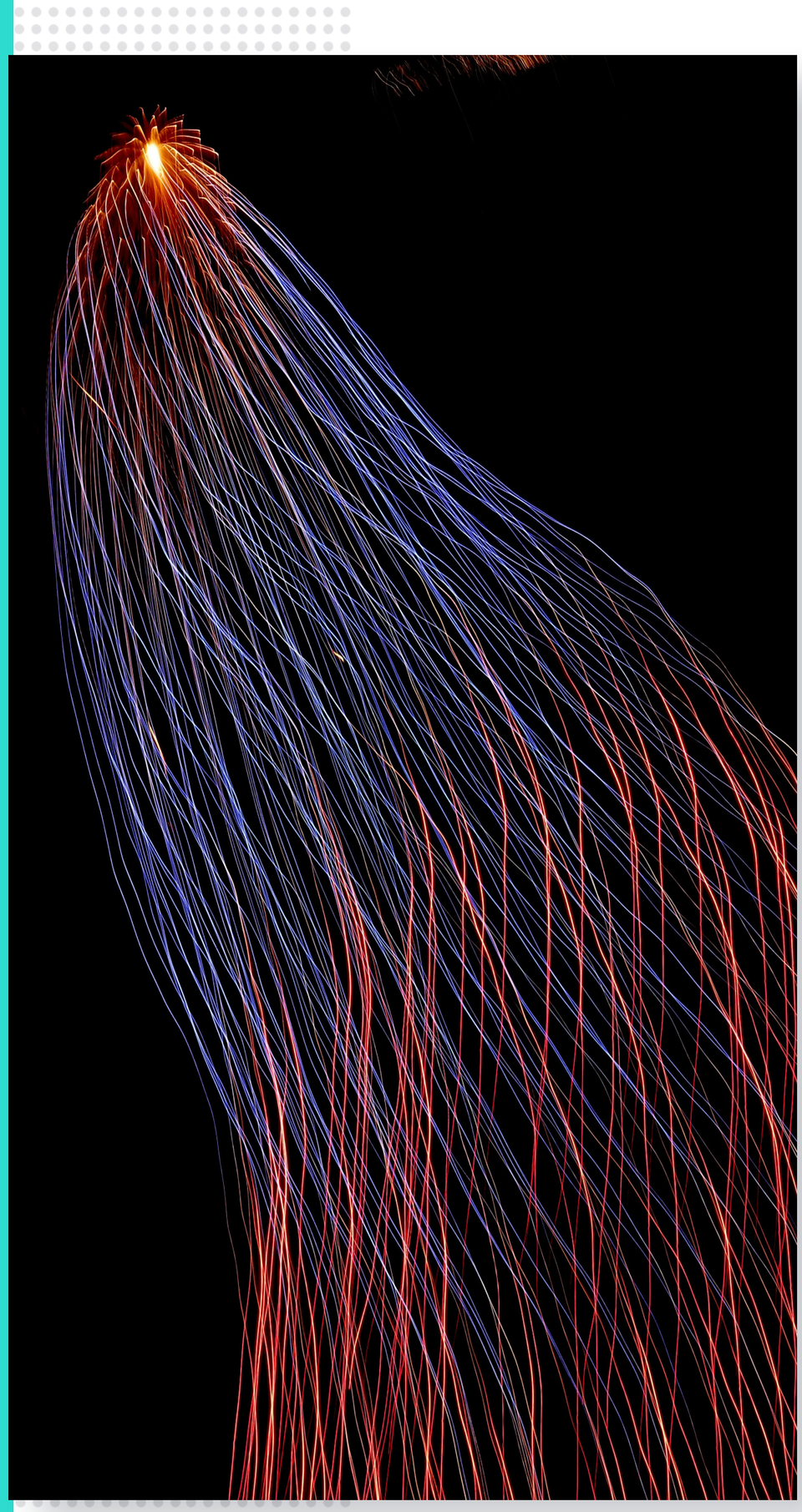
Unsolicited, bulk emails that can carry malicious links or attachments.

These attacks are often sent to numerous targets and aim to spread malware or gather personal information.

MALWARE ATTACHMENTS

Can be delivered through email in various forms, such as infected documents or links to download malware. Once the recipient opens the attachment or downloads the malware, it can take control of their system and steal sensitive information.

What is DMARC?



DMARC is one of the most effective tools to combat email threats and prevent them from infiltrating your business.

It authenticates the sender's identity and prevents unauthorised emails from being delivered to recipients. To do this, it uses a combination of two existing email authentication protocols, SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), to verify the authenticity of an email.

SPF

Verifies that the sending server is authorised to send emails on behalf of the domain.

DKIM

Uses digital signatures to verify that the email content has not been altered in transit.

DMARC policies set out rules for how an email server should handle unauthorised emails. These can include rejecting or quarantining suspicious emails, sending reports to domain owners about failed delivery attempts, and providing feedback on SPF and DKIM authentication results.

The development of DMARC began in 2012 when major email providers such as Google, Hotmail, and Yahoo came together to address the growing issue of email fraud.

Since then, it has become an industry standard for email authentication and is widely adopted by organisations of all sizes.

Why DMARC is crucial for SMBs

- SMBs are targeted in email attacks due to their perceived weakness in the supply chain, but DMARC can greatly mitigate this risk.
- DMARC offers visibility into email senders using your domain, aiding in blocking unauthorised senders and thwarting phishing attacks.
- DMARC provides feedback on SPF and DKIM authentication successes, helping businesses rectify email authentication issues.
- DMARC aids in meeting regulatory compliance like GDPR and HIPAA, which mandate proper email security for data protection.
- Implementing DMARC shows SMBs' dedication to safeguarding customers' and partners' personal information.

SMBs are often targeted by email attacks because they're seen as a weak link in the supply chain. However, implementing DMARC can significantly reduce the risk of falling victim to these attacks.

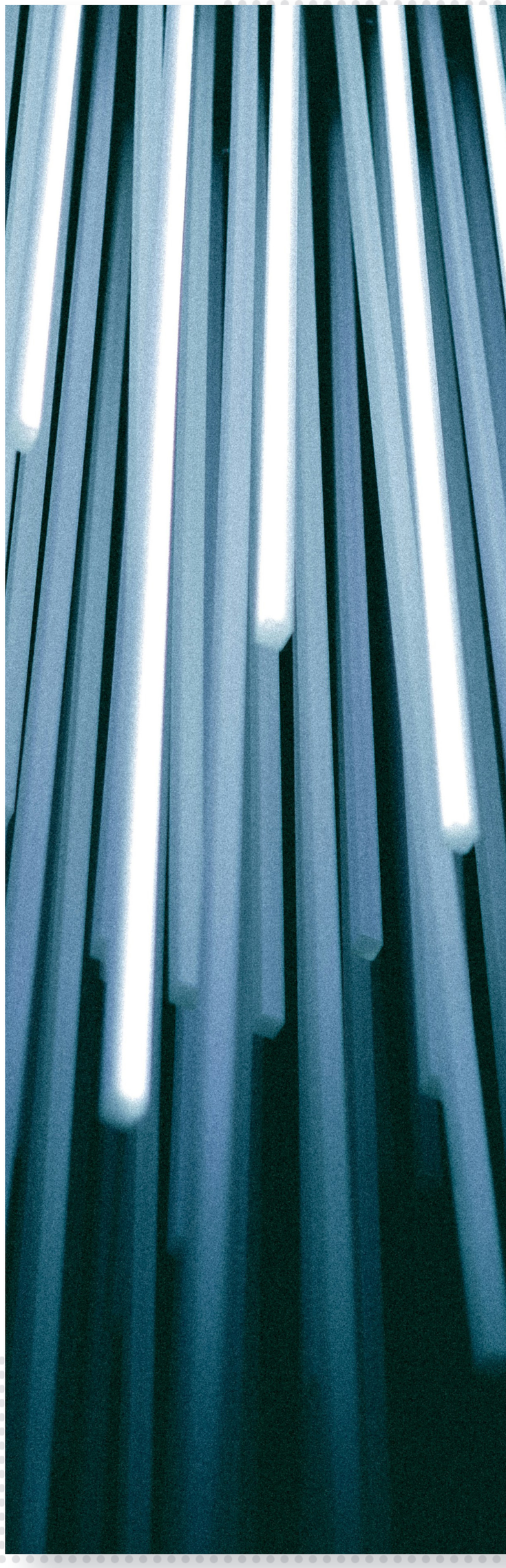
One of the reasons DMARC is so effective is that it provides visibility into who's sending emails on behalf of your domain. Once you know this, you can identify and block unauthorised senders, preventing phishing attacks from reaching your employees and customers.

DMARC also provides valuable feedback on the success of SPF and DKIM authentications. It allows businesses to identify and fix any issues with their email authentication setup and ensure that all emails sent from their domain are legitimate.

When it comes to regulatory compliance, DMARC is an important tool for SMBs. Compliance regulations such as GDPR and HIPAA require businesses to have proper email security measures in place to protect sensitive data.

By implementing DMARC, SMBs can demonstrate their commitment to protecting the personal information of their customers and partners.

Implementing DMARC in SMBs



Implementing DMARC in your business is a crucial step towards securing your email communications. However, it can be challenging for SMBs without proper guidance.

This is where ACDS can support you.

Our team of experts can guide you through the implementation process and provide ongoing support to ensure your DMARC policies are effective and up-to-date. You can focus on running your business while we take care of your email security.

The DMARC Implementation Process

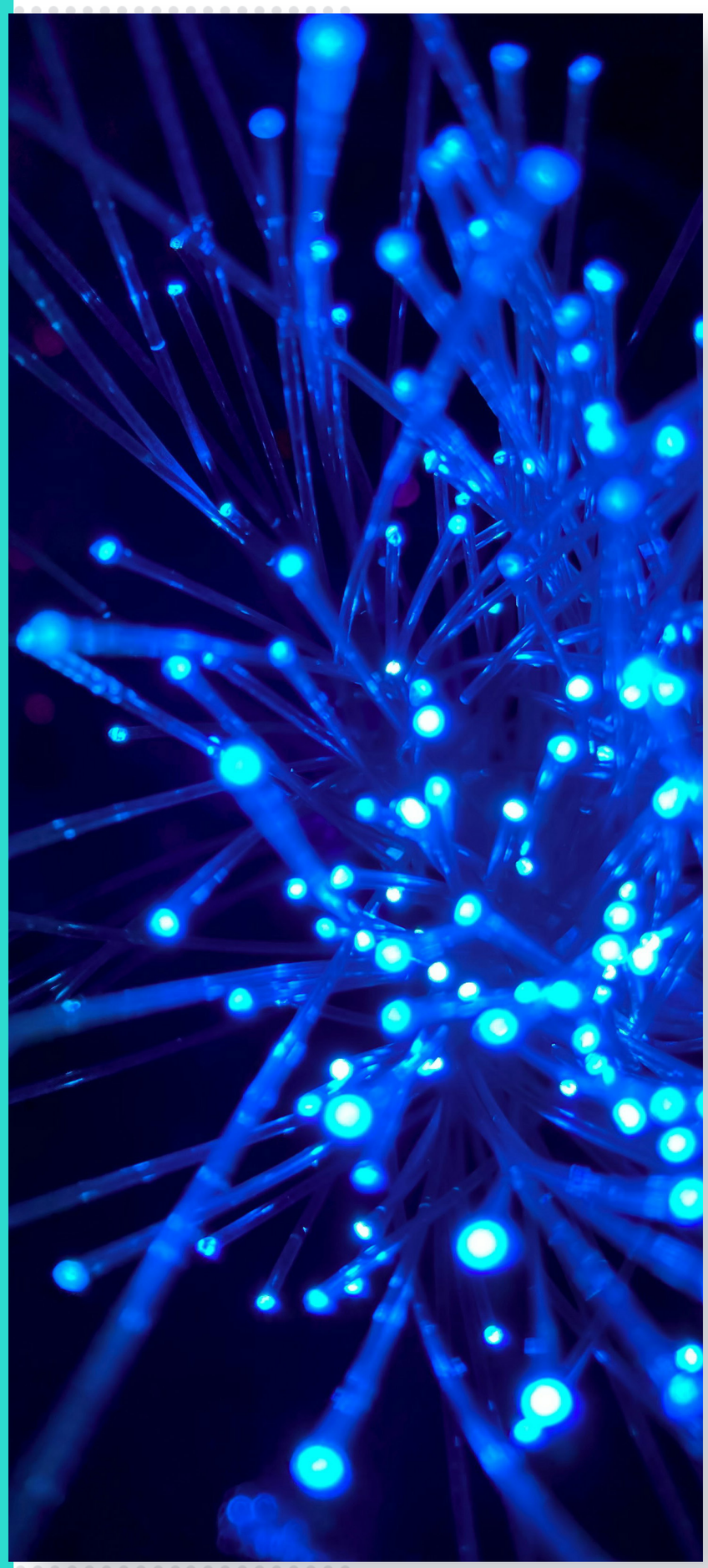
Before implementing DMARC, there are several steps that SMBs should take to prepare and plan for the process.

1. Domain Inventory:
The first step is to conduct a thorough inventory of all domains used by the business. This includes primary domains, subdomains, and any third-party email services used.

2. Determine Policy Decisions:
Next, it's important to decide on the DMARC policy that best suits the business's needs. This can include policies such as "none" (monitoring only), "quarantine" (emails are marked as spam), or "reject" (emails are rejected).

3. Identify Email Sources:
SMBs should also identify all sources of emails sent from their domain, including marketing campaigns, transactional emails, and third-party services. This will help in setting up proper SPF and DKIM authentication for these sources.

Deployment & Management of DMARC



After completing the preparation and planning steps, SMBs can begin deploying DMARC and managing their policies. This involves setting up SPF and DKIM authentication for all email sources and publishing a DMARC record in the DNS (Domain Name System) for each domain.

1. Set Up SPF Authentication:
Sender Policy Framework (SPF) is an email authentication protocol that verifies that the sender's server is authorised to send emails on behalf of the domain. SMBs should set up SPF for all email sources listed in the previous step.

2. Set Up DKIM Authentication:
DomainKeys Identified Mail (DKIM) uses digital signatures to verify that the email content has not been altered in transit. SMBs should set up DKIM for all email sources as well.

3. Publish DMARC Record:
Once SPF and DKIM are set up, SMBs should publish a DMARC record in the DNS for each domain. This record will contain instructions on how to handle unauthorised emails.

4. Monitor & Manage Policies:
After deployment, it's crucial to regularly monitor and manage the DMARC policies to ensure they are effective in preventing email threats. This involves reviewing DMARC reports, making adjustments to policies if needed, and addressing any issues with SPF and DKIM authentication.

5. Timeline to Live:
It's recommended for SMBs to start with a "none" policy and monitor the results for at least two weeks before moving on to a stricter policy such as "quarantine" or "reject." It may take several months of monitoring and adjusting before reaching a "reject" policy.

Conclusion

As email attacks continue to evolve and become more sophisticated, it’s crucial for SMBs to stay informed about the latest in email security.

Regularly reviewing and updating DMARC policies, staying up-to-date on security best practices, and investing in employee training to increase awareness about email threats are all important steps in protecting your business from malicious attacks.

Take action today and speak with an ACDS expert to learn how we can help secure your email communications. We look forward to partnering with you on your journey towards a safer and more secure digital environment.