Saicom

SENDMARC

# SENDMARC

Stop cyber-criminals from sending email using your domain and protect your customers, suppliers and staff from attacks.

## Key Features

- **Security**
- **Compliance**
- **Visibility**
- **Delivery**

## Trust email again

The 2022 State of the Phish report (from Proofpoint) says 86% of organisations experienced bulk phishing attacks, and 77% faced BEC (Business Email Compromise) attacks, or targeted phishing attacks.

The challenge with email is that there is more than one way to spoof or phish:

- **Impersonation**
  Attackers can send email from your domain, defrauding staff, customers and suppliers
- **Interception**
  Emails can be intercepted and changed without the recipient knowing
- **Delivery**
  Legitimate email frequently arrives as spam, and false positives cause service disruption
- **Visibility**
  It is nearly impossible to identify who is sending (spoofing) emails from your domain

# How do spoofing and phishing attacks happen?

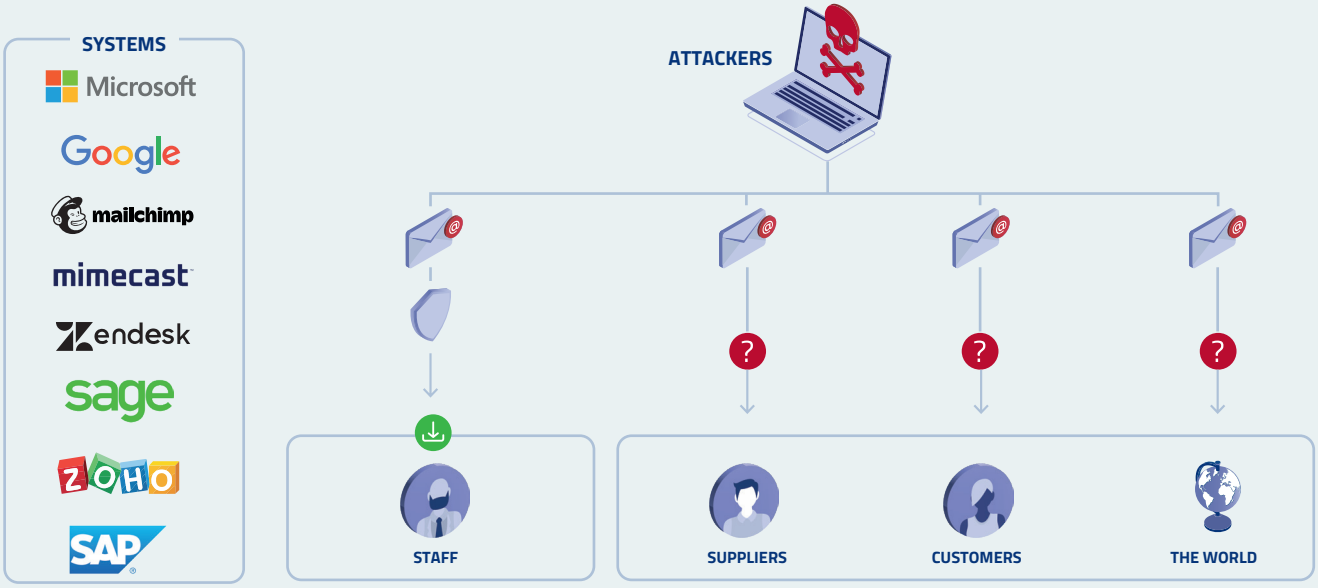
Email spoofing involves sending emails using false sender addresses. Attackers often use email address spoofing in socially engineered phishing attacks hoping to deceive their victims into believing an email is legitimate by pretending that it came from a trusted source.

If the attacker is able to trick their victims into clicking on a malicious link within the email, they can steal their login credentials, financial information, or corporate data. Phishing attacks involving email spoofing may also infect victims' computers with malware or, in cases like Business Email Compromise (BEC) scams, try to trick the victims into initiating a transfer of funds. Variants of phishing such as spear phishing or whaling may be carefully tailored to specific individuals within the company and tend to have a higher success rate.

## Without SendMarc you are exposed to:

- Deposit fraud as a result of incorrect bank details, falsely associated to your company
- Identity theft which tricks users into leaking personal and or corporate information
- Ransomware that lures users into installing malware and is used to encrypt and hold companies to ransom
- Reputational damage in terms of financial loss and brand value

Existing anti-spam solutions protect your employees, but not your customers, suppliers or other external stakeholders. Domain-based Message Authentication Reporting and Conformance (DMARC) is an email authentication, policy and reporting protocol.



# Benefits

DMARC by Sendmarc is compliance software that provides protection of email accounts from spam, spoofing and phishing attacks, protecting customers, suppliers and staff from attacks.

## IT IS DESIGNED TO:

- Stop the illegitimate use of your valid email domain
- Detect and stop spoofing and spammers
- Detect misconfigurations of Sender Policy Frameworks (SPF) and DomainKeys Identified Mail (DKIM)
- Inventorise all the email senders of your domain
- Increase deliverability of legitimate emails
- Provide insights and reporting of all outbound email activity

# Features

- Security to ensure that attackers are not able to send email impersonation or spoofing attacks from your domain
- Visibility of all servers, legitimate or illegitimate that are sending email from your domain
- Monitoring and analysis of email flow from your domain
- Identify, Quarantine and reject Enable your email platform to identify, quarantine and reject non-compliant email
- Compliance so that staff can only send mail via company approved email servers
- Delivery making sure email is delivered to the inbox, and not the spam folder
- Authorise legitimate senders and comply to global email security standards (DMARC, SPF, DKIM)
- Actively protect domains from new impersonation attacks

# Sendmarc works with

**EVERYDAY EMAIL**

mimecast · Office 365 · G Suite

**EMAIL MARKETING AND TRANSACTIONAL MAIL**

mailchimp · Postmark · salesforce · SendGrid · everlytic

**CLOUD SOFTWARE**

freshdesk · Amazon SES · Zendesk · ZOHO