PT emails x 5 – Sendmarc toolkit

Email #1

**Subject:** Are your emails reaching inboxes?

**Preview text:** Google and Yahoo have put new anti-spam measures in place

Hi [NAME],

Like [YOUR BUSINESS NAME], I’m sure email is central to your communications, and it’s important the emails you send don’t end up in junk folders or worse - your email domain isn’t used by cybercriminals.

To keep up with the increase in email cybercrime, Gmail and Yahoo have updated DMARC policies.

These updates can impact whether your emails reach inboxes, which isn’t good for business. If your business uses email, you need to make sure you have a DMARC policy in place.

Not sure where to start? That’s ok. Sendmarc makes DMARC and email security simple.

Sendmarc proactively monitors your entire email ecosystem, detecting threats, preventing your domain from impersonation and ensuring your emails end up in inboxes.

If this is the first time you’ve heard of DMARC, don’t worry, many businesses are unaware of the challenges it presents.

I’d be happy to book in call to chat with you about Sendmarc, or I could send over some more information … what’s best for you?

Kind regards,

[NAME]

Email #2

**Subject:** Don’t let email ruin your brand

**Preview text:** Sendmarc ensures email legitimacy and protection.

Hi [NAME],

Is your email domain at risk of impersonation?

If you have a weak or poorly configured DMARC policy then it is at risk, and you risk your email domain being used by cybercriminals in a phishing attack.

Could your employees, customers, suppliers spot a fraudulent email sent under your name or brand?

It’s not worth taking the risk.

As I mentioned in my last email, Sendmarc takes away the challenges of implementing strong DMARC policies, and ensures your email network is protected against threats as well making sure your emails land in the right inbox.

Would you like to book in a demo?

Kind regards,

[NAME]

Email #3

**Subject:** Don’t become spam

**Preview text:** Are you sure your emails are protected?

Hi [NAME],

Just checking one last time … are you sure you can run the risk of failed email deliveries or even worse, email exploitation?

I thought you might find it useful to see the main benefits of Sendmarc …

* **You’ll be protected from email exploitation –** all inbound and outbound emails are verified, recipients only receive genuine emails.
* **Get global and company-wide compliance –** Sendmarc meets technical authentication and verification standards for all emails using your brand name, across every email service.
* **Emails get delivered to the right place** – authentication rules and policies guarantee that all legitimate emails reach the intended inbox.
* **Improve your brand recognition –**BIMI (Brand Indicators for Message Identification) can display your logo next to emails, improving trust and brand recognition.
* **A 90-day guarantee to reach full protection**.
* **Entire email protection –** integrating with all third-party email providers keeping your entire email network secure.

Need a bit more time? I’d be happy to send over more information about Sendmarc for you to look over, would that be helpful?

Kind regards,

[NAME]

Email #4

**Subject**: Guarantee Email Delivery

**Preview text**: Make sure your emails land in the inbox of your clients

Hi [Name],

I'd like to shed light on a crucial aspect of email security that is garnering increasing attention called DMARC.

While this term may sound unfamiliar, it is pivotal in bolstering the deliverability and security of your business's email communications.

* To understand what is going we have linked a recent impartial article to give more background on this topic outside of **MSP**: https://www.techradar.com/pro/security/north-korean-hackers-crack-dmarc-to-spoof-emails-from-trusted-sources

**Ensuring Email Delivery:** The delivery of your emails to your intended recipients is paramount to business operations. It's worth noting that major email providers like Google and Yahoo are placing greater emphasis on DMARC to verify the authenticity of emails and prevent them from being flagged as SPAM. **By adopting these protocols, you can significantly enhance the likelihood of your emails reaching their destination, fostering smoother communication with your customers and partners.**

**Mitigating Email Spoofing:** Have you ever encountered instances where cybercriminals impersonate your business via email? This form of cyber threat, known as email spoofing, poses a real risk to your business's reputation and security. DMARC aims to thwart such attempts by verifying the legitimacy of senders and detecting any fraudulent emails bearing your business's identity.

Each organisation's email setup is unique, requiring a tailored configuration to ensure compatibility and effectiveness. When setting up these services we must look at all the software and solutions that you have that might communicate via email and need to be included in the DMARC configuration. Implementing DMARC is not a one-time task but an ongoing process. Regular monitoring and maintenance are essential to ensure continued effectiveness and address any emerging threats or issues.

If you are interested in learning more about this and how we can protect you against these threats, please contact XXXXX.

Thanks,

[Name]

Email #5

**Subject**: What security score does your domain get?

**Preview text**: Check how secure your domain is from attacks

Hi [Name],

I am emailing because I wanted to spread awareness of the importance of DMARC with our vendor partner Sendmarc **(rephrase if not specifying the solution).** DMARC is unique in the cyber security space because it not only helps protect domains from impersonation attacks, but also ensures email deliverability from legitimate sources such as Mailchimp, HubSpot, Sage, and other business-critical services.

As such, I thought I would run a scan against the domains of the accounts I manage using Sendmarc’s domain checking tool **(Rephrase if you not specifying the solution).** Any domain that scored 3/5 or lower is open to impersonation, and I can see your score is **X/5**.

If you would like to check your DMARC security, put your email address in this score checker - https://tools.sendmarc.com/.

Interested in finding out more? Let me know as Google, PCI DSS, and Yahoo have implemented DMARC restrictions which may be causing emails to not be sent which can cause serious disruptions within your day-to-day operations.

Please contact XXXX if you wish to have a further conversation.

Thanks,

[Name]