Unbranded PT emails x 3 – Sendmarc toolkit

Email #1

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

**Preview text:** You need to be aware of stricter email security standards.

Hi [NAME],

Email is at the centre of business communications, but are your messages making it to inboxes?

Microsoft is the latest major provider to join the likes of Gmail and Yahoo in tightening their DMARC policies to keep up with the increase in email cybercrime.

If your email domain isn’t properly configured with DMARC, your emails are at risk of being rejected or sent to spam. Worse still, you’re at risk of cybercriminals impersonating your domain and putting your business and customers at risk.

Whether you’ve never heard of DMARC or are unsure if your setup is correct, you’re not alone. We’re here to help. As your trusted service provider, we can support you in assessing your domains current setup and guide you through implementing or updating your DMARC policy.

I’d be happy to book in a call to chat about this further, or I could send over some more information … what would work best for you?

Kind regards,

[NAME]

Email #2

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

**Preview text:** Protect your domain from phishing and impersonation

Hi [NAME],

Is your email domain at risk of impersonation?

If you have a weak or poorly configured DMARC policy then your domain is vulnerable, and you’re at risk or cybercriminals sending phishing emails that appear to come from your business – targeting employees, customers or partners. Would they spot a fake email in time?

It’s not worth taking the risk.

The good news is DMARC doesn’t have to be complicated.

We’ve helped many of our customers simplify the process of securing your domain, improving email deliverability and keeping cybercriminals from misusing their identity.

I can talk you through how we can help over a call. What time that would work for you?

Kind regards,

[NAME]

Email #3

**Subject:** Don’t become spam

**Preview text:** Are you sure your emails are secure and land where they should?

Hi [NAME],

Just checking one last time … are you confident that your business emails are being delivered securely and reliably?

I thought you might find it useful to see the key reasons for getting your DMARC setup right:

* **Protect your brand from impersonation** – Prevent cybercriminals from sending fraudulent emails using your domain.
* **Ensure compliance across platforms** – Apply consistent authentication across all email services and third-party senders.
* **Improve email deliverability** – Help ensure legitimate emails reach their intended inboxes, not spam folders.
* **Enhance trust with your brand** – With DMARC and BIMI, your logo can appear next to authenticated emails, boosting brand visibility and credibility.
* **Get peace of mind quickly** – Most domains can reach full protection in under 90 days with the right guidance.

Need a bit more time? I’d be happy to send over more info or schedule in a call, whichever works best for you.

Kind regards,

[NAME]