Top 5 reasons why a business should be concerned about DMARC

1. **Prevent Email Spoofing**:
    - **Explanation**: Email spoofing is when someone sends an email that looks like it's from your business, but it's actually from a scammer. DMARC helps stop this by verifying that emails claiming to be from your business are actually from you.
    - **Example**: Imagine a scammer sends an email to your customers pretending to be your company, asking for their credit card information. With DMARC, these fake emails would be blocked, protecting your customers and your reputation.
2. **Protect Against Phishing Attacks**:
    - **Explanation**: Phishing attacks trick people into giving away personal information by pretending to be a trustworthy source. DMARC helps ensure that emails from your domain are legitimate, reducing the risk of phishing.
    - **Example**: A phishing email might look like it's from your HR department, asking employees to update their passwords. DMARC can prevent these fake emails from reaching your employees, keeping their information safe.
3. **Improve Email Deliverability**:
    - **Explanation**: Without DMARC, your legitimate emails might get marked as spam because email providers can't verify their authenticity. DMARC helps ensure your emails reach the inbox.
    - **Example**: If your marketing emails are often going to customers' spam folders, implementing DMARC can help them land in the inbox, improving your communication and marketing efforts.
4. **Build Customer Trust**:
    - **Explanation**: When customers know that your emails are secure and authentic, they are more likely to trust your communications. DMARC helps build this trust by preventing fraudulent emails.
    - **Example**: If customers receive a fake email that looks like it's from your company and fall victim to a scam, they might lose trust in your brand. DMARC helps prevent this, maintaining your company's reputation.
5. **Gain Insight into Email Activity**:
    - **Explanation**: DMARC provides reports on how your emails are being handled, showing you if there are any unauthorized attempts to use your domain. This helps you monitor and improve your email security.
    - **Example**: By reviewing DMARC reports, you might discover that someone is trying to send fake emails using your domain. You can then take action to stop these attempts and enhance your security measures.