

I'm using Office 365. I don't need DMARC, right?

The short answer = **Wrong**
You still need DMARC!



- ▶ Microsoft's Office 365 is one of the most popular enterprise-grade productivity solutions on the market, which also makes it a **major target for email spoofing attacks**.
- ▶ Attackers **disguising themselves as someone from within the organization** send phishing emails to employees, causing some of the biggest data loss incidents in recent years.
- ▶ There's a **common misconception** among businesses that having an Office 365 solution ensures safety from spam and phishing attacks. In May 2020, a series of phishing attacks on several Middle Eastern insurance firms using Office 365.
- ▶ The thing to note here is that as robust as Microsoft's security is, it doesn't mean that you have no responsibility in protecting your domain. If you really want to step up your email security, you need to prevent malicious sources from sending phishing email from your organization's own domain.

How Do You Make Email with Office 365 Secure?

- ▶ When it comes to securing your organization's email systems, it's not enough to rely on Office 365's in-built security features, because they may only protect you from **inbound phishing attempts** to a certain extent.
- ▶ That means you still need to deal with malicious sources sending phishing email from your organization's own domain.
- ▶ The good news is, that's what we're here for! **PowerDMARC can seamlessly integrate with Office 365**, providing you maximum visibility and securing your domain. Our platform allows you to get information on spoofing attempts, take down malicious IPs, and protect your brand.