ProtonSpoof - The Lack & Vulnerability of ProtonMail

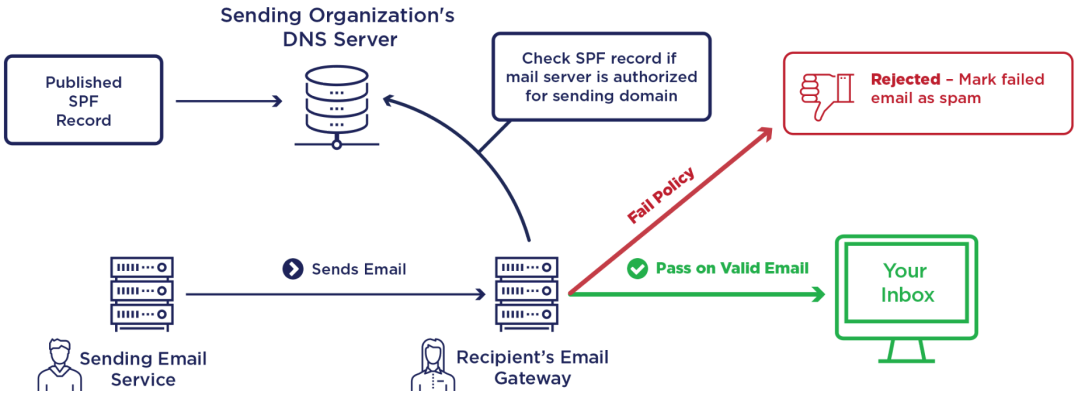
Prv

Overview

Upon testing different email services, and how email servers respond and react to headers and contents of emails, discovered that protonmail- a large encrypted email service with over 100 million+ users, entirely allows the communication and accepts emails for as long as the domain that the incoming email is using exists regardless of if it lacks a sufficient ***DMARC*** header for the email- and quickly, I identified in that by default, protonmail and all associated accounts with emails that use proton, such as "@proton.me" "@pm.me" and "protonmail.com" email addresses had absolutely no mitigation from incoming emails that lacked this crucial header of which virtually all other leading email services do.

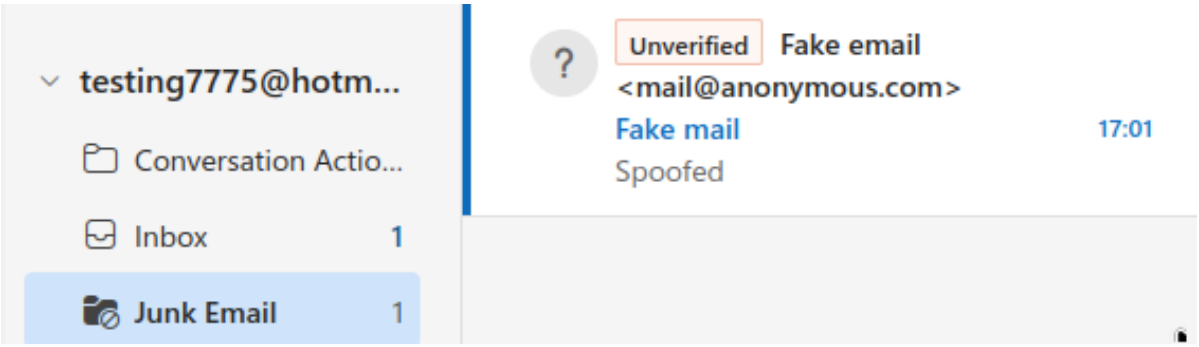
So why is this bad?- well a ***DMARC*** or ***Domain-based Message Authentication, Reporting, and Conformance*** header, is a header which domains use to protect itself from

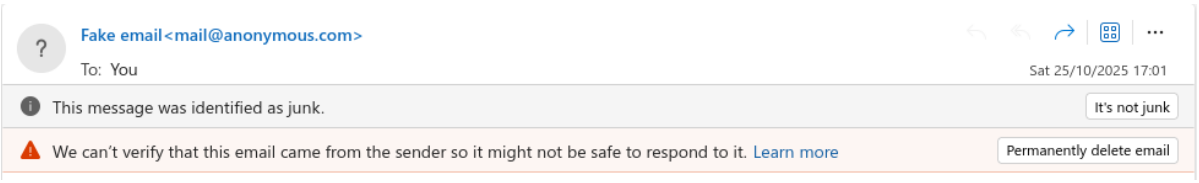
unauthorised usage when it comes to sending emails, essentially a stamp of authenticity which only the legitimate domain can use and produce when sending emails from it and without this, a domain is unable to stop emails being sent from it without authentication.



(via alwaysdata.com)

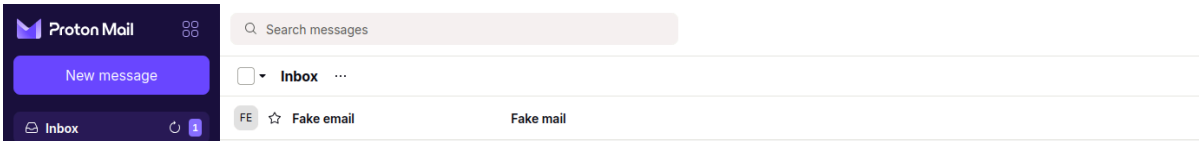
Other email providers, such as google, microsoft and apple all filter for emails automatically that land in their inbox for domains that do not contain an authenticated ***DMARC*** header, and usually put the message into spam or even reject the email all together, for example Microsoft's Outlook mail when receiving from a domain that is registered, but does not contain a sufficient ***DMARC*** header- like anonymous.com

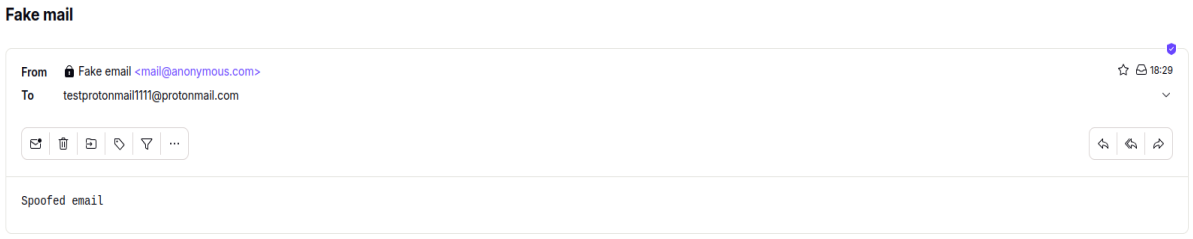




You can clearly see that due to this missing header, the spoofed email has been correctly identified as ***'Unverified'***, and moved into the spam folder with warnings placed as to the validity of the emails origin, letting the user know that this email may not be legitimate and as a result potentially harmful.

Now the same email will also be sent to a protonmail inbox, same content, same headers, different provider





Notice how that same spoofed email sent to the outlook inbox (which was sent to spam and flagged) has just landed into the **main inbox** of the protonmail account, despite missing headers with no warnings or indications that this email received is not real and potentially malicious.

Impact

The findings presented in this report highlight a significant oversight in ProtonMail's inbound email handling process, specifically related to its lack of enforcement or verification of DMARC (Domain-based Message Authentication, Reporting, and Conformance) policies. As a result, ProtonMail accounts—including those under the domains @proton.me @pm.me and @protonmail.com— may be more susceptible to **email spoofing** and **phishing-based social engineering attacks** than users of other leading email providers.

Malicious actors could potentially exploit this behavior to impersonate trusted senders, increasing the likelihood of successful phishing attempts or identity deception. This vulnerability may affect both individual users and organizations that rely on ProtonMail for secure communication, potentially undermining user trust and exposing sensitive information.

While this issue does not constitute a breach of ProtonMail's encryption or internal infrastructure, it represents a **critical gap in inbound authentication enforcement**. The impact primarily concerns user safety, reputation integrity, and overall communication trustworthiness within the ProtonMail ecosystem.

Disclaimer

This report and all related findings were produced strictly for **educational, research, and responsible disclosure purposes.**
No unauthorized access, exploitation, or malicious testing was conducted against ProtonMail's systems, users, or infrastructure. All experiments were performed within a controlled environment, using test domains and emails owned or authorized by the researcher.

The intent of this research is to **raise awareness** about potential risks in email authentication handling and to encourage ProtonMail and other providers to adopt stronger validation mechanisms (such as mandatory DMARC enforcement and clearer user warnings) to enhance user security.