

DMARC policy (p)

Contents

- [Problem](#)
- [Solution](#)
- [Related articles](#)

Problem

Why it is so important to set the DMARC *p*-switch to *reject*.



It is a common mistake to configure DMARC for reporting and to forget about it afterwards. Loss in reputation comes gradually over time and is often only noticed when it's already too late. By thumb of fist it takes about as long to fix a broken reputation as it has taken this reputation to break.

Solution

Three things to remember:

1. The main purpose for DMARC is to set a **policy (p)**. This policy contains the action that should take place **when unauthenticated mail from this domain is received** (and in no other case). The options are:
 - a. **none**: to do nothing when authentication fails
 - b. **quarantine**: to put the mail in the SPAM folder when authentication fails
 - c. **reject**: to the message when authentication fails.

Only by using the *reject* policy can a domain be fully protected.

2. DMARC allows ISPs to rely not only on IP reputation, but also on **domain reputation**. Especially when sending via shared IPs, a good domain reputation can be helpful in delivering your emails to the right place. Without a DMARC record it is impossible for ISPs to reliably measure reputation for a domain.
3. Any domain owner that does not protect with DMARC is vulnerable for phishing and spoofing abuse. Whenever your domain can be abused by a third party, your **overall reputation** is likely to suffer.
4. DMARC [reporting](#) alone - as in the following example - does not provide **protection against phishing and consequent loss in reputation**. It provides reporting functionality only. Such a setting can be useful when evaluating the impact of switching the policy to *reject*. It is not useful in protecting your domain.

```
# host -t txt _dmarc.sub.domain.TLD
_dmarc.sub.domain.TLD descriptive text "v=DMARC1; p=none; rua=mailto:dmarc@mailmike.net;"
```

Related articles

- [Authentication results](#)
- [Subdomains vs. organisational domains](#)
- [DMARC reporting \(rua / ruf\)](#)
- [On which domains to set a DMARC record](#)
- [IP grouping](#)

Account

- Register a [test account](#).
- [Login](#) to app.inboxsys.com.

Support

- Create a ticket for our [service desk](#).
- Book a [consultant](#).

Website

- Check our [website](#).
- Read the [resources](#).