Domain check: parcodellago.com

Well done! Your domain is protected against abuse by phishers and spammers

Receivers are able to reliably separate and block fraudulent emails that mimic your email domain from your authentic emails.

✓

DMARC

Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

✓

SPF

Your domain has a valid SPF record and the policy is sufficiently strict.

✓

DKIM

Your DKIM record is valid.

DMARC check: parcodellago.com

Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

```
v=DMARC1;p=reject;sp=reject;pct=100;rua=mailto:dmarc-
report@eraclito.it;ruf=mailto:dmarc-report@eraclito.it;ri=86400;fo=1
```

Tag	Value	Traslation
V	DMARC1	The DMARC version should always be “DMARC1” Note: A wrong, or absent DMARC version tag would cause the entire record to be ignored
p	reject	Policy applied to emails that fails the DMARC check. Authorized values: "none", "quarantine", or "reject". "none" is used to collect feedback and gain visibility into email streams without impacting existing flows. "quarantine" allows Mail Receivers to treat email that fails the DMARC check as suspicious. Most of the time, they will end up in your SPAM folder. "reject" outright rejects all emails that fail the DMARC check.
sp	reject	Policy to apply to email from a sub-domain of this DMARC record that fails the DMARC check. Authorized values: "none", "quarantine", or "reject". This tag allows domain owners to explicitly publish a "wildcard" sub-domain policy.
pct	100	The percentage tag tells receivers to only apply policy against email that fails the DMARC check x amount of the time. For example, "pct=25" tells receivers to apply the "p=" policy 25% of the time against email that fails the DMARC check. Note: The policy must be "quarantine" or "reject" for the percentage tag to be applied.
rua	mailto:dmarc-report@eraclito.it	The list of URIs for receivers to send XML feedback to. Note: This is not a list of email addresses, as DMARC requires a list of URIs of the form "mailto:address@example.org"
ruf	mailto:dmarc-report@eraclito.it	The list of URIs for receivers to send Forensic reports to. Note: This is not a list of email addresses, as DMARC requires a list of URIs of the form "mailto:address@example.org".
ri	86400	The reporting interval for how often youl'd like to receive aggregate XML reports. Youlll most likely receive reports once a day regardless of this setting.
fo	1	Forensic reporting options. Authorized values: "O" "1". "d" or"s" "O" generates report if all underlying authentication mechanisms fail to produce a DMARC pass result. “1"' generates reports if any mechanisms fail, "d'" generates reports if DKIM signature failed to verify, "s" generates reports if SPF failed.

SPF check: parcodellago.com

Your domain has a valid SPF record and the policy is sufficiently strict.

```
v=spf1 ip4:173.201.183.100 ip4:92.204.71.1/24 include:_spf.google.com
include:secureserver.net -all
```

7/10
DNS-querying mechanisms / modifiers to resolve the record

This record uses the correct number of DNS query mechanisms/modifiers.

DKIM check: parcodellago.com

Your DKIM record is valid.

```
v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0OPs4hNazupTqxf
Mkl8CaZhiX3tYQzipSV/
F5t4Y7Nv06HmZw4x4SNufIG9oMguAJY22mme0cbl+4HW7hiHQZ2UxEGxAprEzfLdgmQXT
203BAaC+GPlaokFVoluDV+Po+byVdMR8k+Ggbu7iR5+pl0FGl3p+B6CPcvUEYV0UpRwIDA
QAB
```

Key	Name	Value
V	Version	DKIM1
K	Key type	rsa
p	Public key	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0OPs4hNazupTqxfMkl8CaZhiX3tYQzipSV/F5t4Y7Nv06HmZw4x4SNufIG9oMguAJY22mme0cbl+4HW7hiHQZ2UxEGxAprEzfLdgmQXT203BAaC+GPlaokFVoluDV+Po+byVdMR8k+Ggbu7iR5+pl0FGl3p+B6CPcvUEYV0UpRwIDAQAB

There are other DKIM records suitable for signing emails forwarded via other mailing systems like google

CERTIFIED

CERTIFIED