NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Email Security Explained: SPF, DKIM, DMARC in Plain English

If your business email uses your own domain, scammers can send email that looks like it's from you, unless you've set up SPF, DKIM, and DMARC. This guide explains each one in plain English, and what to do if your domain gets spoofed anyway.

Why this matters

Without these, anyone can pretend to be your business.

Anyone can fake your domain
Without authentication, scammers can send email that looks like it's from you.

It hurts legitimate mail, too
Without it, your real emails are more likely to land in spam.

Three DNS records fix it
SPF, DKIM, and DMARC, set up once, work in the background.

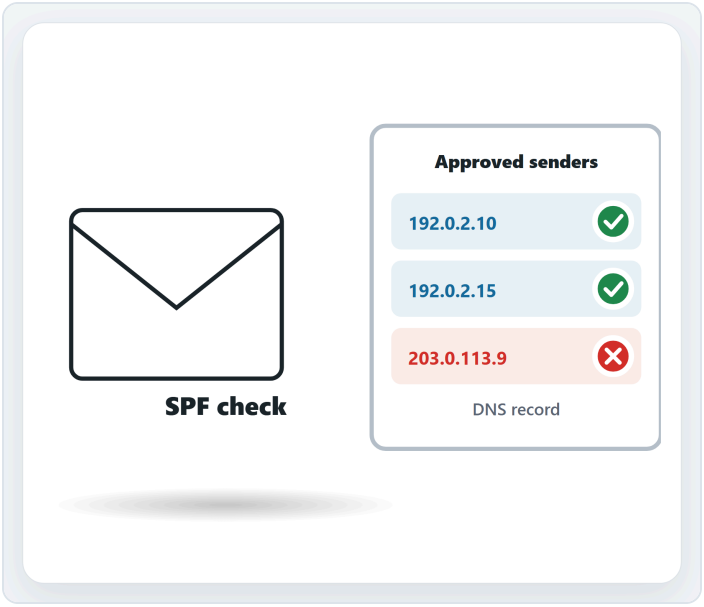
SPF, DKIM, and DMARC, explained

SPF

1 SPF: who's allowed to send

Sender Policy Framework. You list the specific mail servers allowed to send for your domain.

WHAT TO DO
A receiving server checks the sender against that list. Not on it? The email gets flagged.



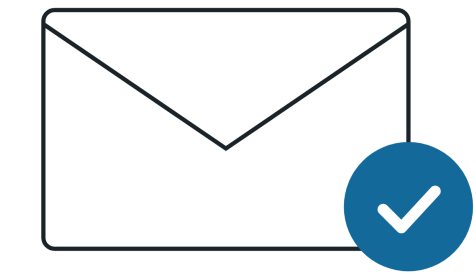
DKIM

2 DKIM: a digital signature

DomainKeys Identified Mail. It signs outgoing mail, so a receiving server can verify it's genuine.

WHAT TO DO

If the signature doesn't check out, the message may have been altered, or isn't really from you.



Digitally signed, unchanged in transit

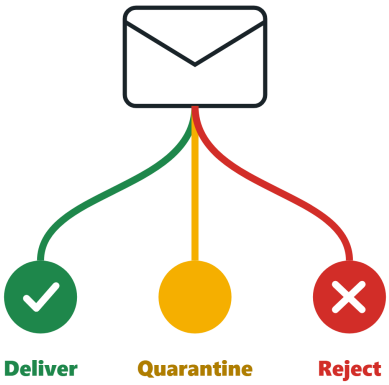
DMARC

3 DMARC: the policy

DMARC checks that SPF and DKIM match the "from" address you actually see, then enforces your rule.

WHAT TO DO

Tell servers to deliver it, quarantine it as spam, or reject it outright, and get notified when it happens.



Your policy decides

NAPLES COMPUTERS

Not sure if yours is set up right?

We'll check your domain, and set up SPF, DKIM, and DMARC correctly, without blocking your own mail.

WHAT TO DO

Call 239-513-1960, especially if you've never checked this before.



Setting it up

- [ ] **These are DNS records**
  Set up with your domain registrar or email host, not an app you click in
- [ ] **It's easy to misconfigure**
  Done wrong, it can block your own legitimate email
- [ ] **Have your provider do it**
  If they won't, or don't offer it, that's worth reconsidering

If your domain gets spoofed

- [ ] **Report it**
  Local law enforcement, IC3.gov, and FTC.gov slash complaint
- [ ] **Notify your customers**
  By mail, email, or social media, with no links, so it doesn't look like another scam
- [ ] **Alert your staff**
  Use it as a chance to review how your team spots a phishing attempt

Recap: SPF, DKIM, DMARC

- [ ] SPF: lists the mail servers allowed to send for your domain
- [ ] DKIM: a digital signature proving mail wasn't altered in transit
- [ ] DMARC: your policy for what happens when something fails
- [ ] These are DNS records; have your provider set them up
- [ ] Not sure yours is set up right? Call Naples Computers

These are DNS records, not something you click in an email app. They're easy to misconfigure, so have your email hosting provider (or an IT provider) set them up, rather than guessing.



Not sure if your domain is protected? We'll check it for you.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**