DMARCsimple – DMARC for Executives

DMARCsimple – DMARC for Executives

Why DMARC matters at the leadership level

DMARC reduces phishing and impersonation risk, protects your brand and supports security and compliance efforts. Executives do not need to configure DNS themselves, but they are accountable for the risk DMARC is designed to reduce.

What DMARC does in plain language

DMARC adds a policy layer on top of SPF and DKIM. It allows you to monitor who is sending email on your behalf and to decide what happens when a message fails authentication checks.

A simple DMARC roadmap for leaders

1. Visibility: understand which systems send email for your domains.
2. Stabilization: align SPF, DKIM and domains for legitimate senders.
3. Remediation: fix or remove legacy and unauthorized sources.
4. Enforcement: move from monitoring to quarantine and then reject.

Executive responsibilities

Leaders approve DMARC as a priority, align stakeholders, allocate time for fixes, approve enforcement milestones and confirm ongoing ownership of DMARC monitoring.

How DMARCsimple helps

DMARCsimple turns raw DMARC data into domain health summaries, trends and evidence that can be used in security reviews and audits.