Email Authentication & Website Blocking Report

How to check SPF, DKIM, and DMARC records for multiple domains

To check SPF, DKIM, and DMARC records, you can use online DNS lookup tools or command line utilities like 'nslookup' or 'dig'. - SPF: Look for TXT records with 'v=spf1'. - DKIM: Check for a TXT record in the format 'selector._domainkey.domain.com'. - DMARC: Look for TXT records under '_dmarc.domain.com'. For multiple domains, you can script the queries or use monitoring services that automate checking these records regularly.

How to send and compile email authentication reports

Email authentication reports are usually generated by DMARC. To receive them: - Publish a DMARC record with 'rua' and 'ruf' tags pointing to your report address. - Example: 'v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-failures@yourdomain.com'. - Use tools like DMARCian, Postmark, or open-source parsers to compile and visualize these reports for analysis.

How to block websites on a few systems

To block websites only on a few systems (not network-wide): - Use the Windows 'hosts' file located at C:\Windows\System32\drivers\etc\hosts. - Add entries like '127.0.0.1 sitename.com' and '127.0.0.1 www.sitename.com'. - Alternatively, configure Windows Firewall rules on each system to block outbound traffic to the site's IP addresses.

How to verify SPF, DKIM, and DMARC pass when sending emails to Yahoo, Gmail, and Outlook

To verify that SPF, DKIM, and DMARC pass: - Send a test email to a Gmail, Yahoo, or Outlook account. - In Gmail: Open the email → More options (■) → Show Original → Check SPF, DKIM, DMARC status. - In Yahoo: View the email header details to see 'Authentication-Results' lines. - In Outlook: Right-click email → View Message Source → Look for 'Authentication-Results' headers. This ensures your domain is properly authenticated across major providers.