

Secure the emails of your WordPress site with SPF, DKIM and DMARC

Nicola Selenu

#WCBCN






Nicola Selenu

Recognized Leader in Email
Security & Deliverability

15 years of professional
experience as a Consultant
in Email Marketing and
Email Deliverability

 @theVot

 vot

 thevot

Protecting your Domain from the risks of phishing

- Scammers may **impersonate your business**
- Phishing attacks can be **hard to spot**
- Phishing attacks can **harm your brand, finances, and security**
- You can protect your domain from phishing attacks by implementing **email authentication**

WordPress and Email Authentication: the problem

- **Every WordPress website sends emails**
- However, these emails **are not authenticated**
- This leads to many **risks** and **issues**

WordPress and Email Authentication: a new solution

- **Until now**, implementing email authentication fully on WordPress **has been challenging**
- We recently launched a **FREE plugin** makes it **easy to enable email authentication** on any WordPress website with minimum effort
- **But what is email authentication?**



Domain Authentication and protection

Goals:

- **confirm the identity** of a legitimate Sender
- **Prevents brand impersonations** and abuses

3 protocols work together to auth emails:

- Authentication based on IP source: **SPF**
- Authentication based on encryption: **DKIM**
- Policy & Reporting: **DMARC**

What else you need to know about email auth

- authentication is implemented on the **domain**
- Each protocol requires a specific **DNS** record
- each protocol may either "**PASS**" or "**FAIL**"
- **DMARC is your best bet** against domain abuse, but you can't implement it without SPF or DKIM
- marketers often **forget** to authenticate emails sent from **their own website**

Sender Policy Framework (SPF)

- An email authentication method that helps to identify the mail servers that are allowed to send email for a given domain.

How it works

- *The **SPF Record** declares the **IP addresses** authorized to send email on behalf of your organization's domain.*

DomainKeys Identified Mail (DKIM)

- An email security standard designed to make sure messages aren't altered in transit between the sending and recipient servers.

How it works

- ***DKIM** adds a digital signature to the email using a **private** key. A **public** key is used to verify it's valid.*

Domain-based Message Authentication, Reporting & Conformance (DMARC)

- An email authentication, policy, and reporting protocol.

How it works

- ***DMARC** relies on **SPF** and **DKIM** to determine if a given message is legitimately coming from a sender and **tells what to do** if it isn't.*

Implementing Email Authentication on WordPress

- You can find the **Deliverability** plugin in the WordPress repository:

EMAIL DELIVERABILITY MANAGER

- SIGN YOUR EMAILS WITH **DKIM**
- PASS **DMARC** VIA DOMAIN ALIGNMENT
- MONITOR YOUR **DELIVERABILITY SCORE**

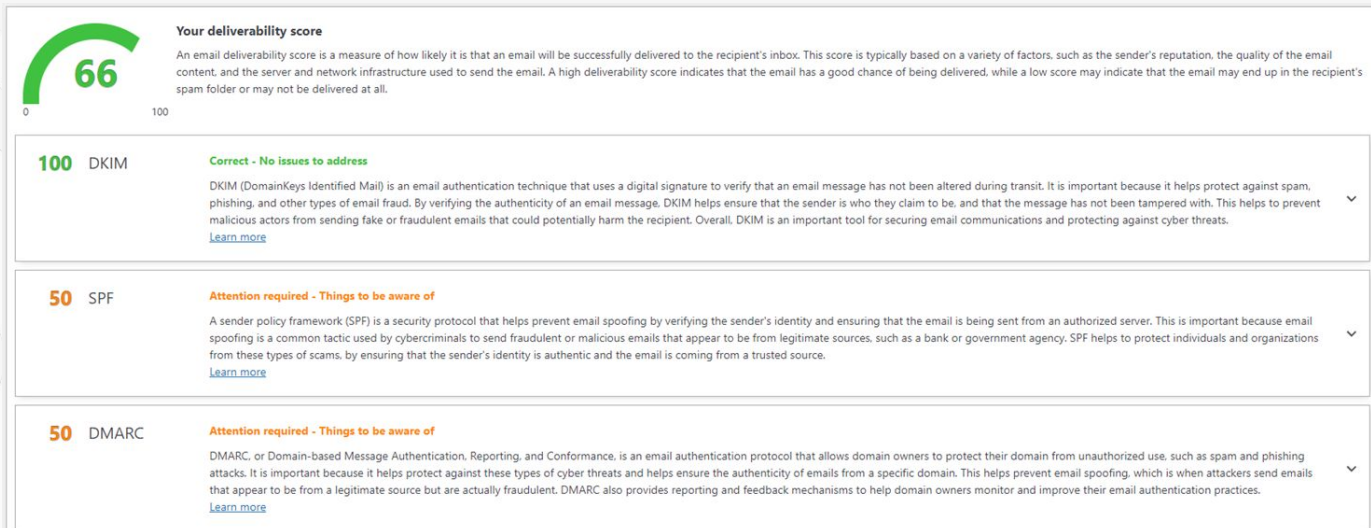
...AND MUCH MORE!

TOP DELIVERABILITY Deliverability
By Top Deliverability

[Download](#)

«Deliverability» WordPress Plugin: Overview

- The plugin provides an overview of the email authentication status of your WordPress



«Deliverability» WordPress Plugin: Troubleshooting

- Error details are provided to help site owners fix issues and achieve a better Deliverability

0 SPF

Critical issues found - please fix immediately

A sender policy framework (SPF) is a security protocol that helps prevent email spoofing by verifying the sender's identity and ensuring that the email is being sent from an authorized server. This is important because email spoofing is a common tactic used by cybercriminals to send fraudulent or malicious emails that appear to be from legitimate sources, such as a bank or government agency. SPF helps to protect individuals and organizations from these types of scams, by ensuring that the sender's identity is authentic and the email is coming from a trusted source. ^

[Learn more](#)

SPF Record is Too Long

The domain's SPF record is too long and cannot be processed. Please review and shorten the record to meet the maximum length requirement.

Everybody should implement Email Authentication

Benefits of Email Authentication

- Prevents unauthorized use of your domain
- Protects and enhance your brand reputation
- Helps with your email deliverability

And now, thanks to **Deliverability** Plugin:

- You don't need to be an expert to implement it
- You don't need to pay a third-party service

Thank You!

Questions?

#WCBCN



#WCBCN

