What is DKIM?

DKIM (DomainKeys Identified Mail) Explained

DomainKeys Identified Mail (DKIM) is an essential email authentication mechanism designed to verify the authenticity and integrity of email messages.

It works by adding a digital signature to outgoing emails, which can be verified by the recipient's email server using cryptographic methods. The sending mail server digitally signs the message using a private key. This signature includes a cryptographic hash of various parts of the email, such as the message body and headers, ensuring that the message has not been altered in transit and originates from a legitimate sender. The sending domain publishes a DKIM DNS record containing a public key that corresponds to the private key used for signing. This record is used by receiving mail servers to verify the authenticity of the DKIM signature.

One of the key benefits of DKIM is its ability to prevent email tampering and forgery. By digitally signing outgoing emails, DKIM provides a mechanism for recipients to verify that the email they received was indeed sent by the claimed sender and has not been modified or tampered with during transmission. This helps in building trust between senders and recipients, as well as in protecting against phishing attacks and other forms of email fraud. DKIM helps improve email deliverability by enhancing the reputation of legitimate senders. Email servers often use DKIM authentication as one of the factors to determine whether an email should be delivered to the recipient's inbox or flagged as spam. By implementing DKIM, senders can demonstrate their commitment to email security and authenticity, thereby increasing the chances of their emails reaching the intended recipients' inboxes.

Another advantage of DKIM is its role in building sender reputation. Email service providers and spam filters take into account the presence of DKIM signatures when assessing the trustworthiness of senders. Emails that pass DKIM authentication are more likely to be considered legitimate and are less likely to be marked as spam. This helps legitimate senders maintain a positive sender reputation and ensures that their emails have a better chance of reaching the inbox rather than being filtered out or blocked.

DKIM is a widely accepted and expected component for reliable email delivery and should be enabled on your web site now. If it is not, make sure DKIM is enabled in your DNS records as soon as possible. DKIM Tools are available by default on all **GlowHost Web Hosting** packages and DKIM records can be set up with a few clicks within your web site's control panel. In many cases is already setup for you by default, or our fast and friendly technicians can help you set it up if you are still unsure on how to do it on your own.

DKIM is also one of the essential building blocks along with **SPF (Sender Policy Framework)** for those seeking to deploy a full-blown **DMARC** (Domain-based Message Authentication, Reporting, and Conformance) policy for their sending domains. While DMARC is not necessarily required to send emails reliably, DMARC is starting to become widely adopted to increase email security and brand trust across the Internet. Larger organizations are encouraged to implement a DMARC as soon as possible, and the process does take some time and technical knowledge to achieve.

You can **learn more about how DMARC, SPF and DKIM** work together as we have created an entire section that tackles DMARC from start to finish within this knowledge base. GlowHost also offers **Managed DMARC Services** for those that would prefer a "done for you" hands-off DMARC approach, or for those organizations that prefer to outsource or supplement their own IT department's management of their DMARC policy. GlowHost's Managed DMARC Services combine experienced DMARC email technicians with a Software as a Service DMARC dashboard complete with graphs and robust reporting options.

Related Topics:

- DMARC, DKIM, SPF and BIMI Info
- DMARC DKIM Alignment (adkim)
