E-mail Validation: DKIM & SPF

Introduction

- E-mail remains an important form of electronic communication for both business and pleasure.
- However, e-mail security is still of huge concern to many as e-mail threats like spam, malware and phishing are still prevalent even today.
- To improve e-mail security, two forms of e-mail authentication protocols are currently being adopted by e-mail providers globally today: DKIM & SPF
- In this tutorial, we'll discuss more about DKIM & SPF and examine how to enable them for our domain.

SPF Explained

SPF Explained

- SPF stands for **Sender Policy Framework**. It is another e-mail authentication method that allows senders to specify which mail servers they use to send their e-mail from.
- When an e-mail is composed, two “from” addresses is created: the “envelope from” (known as the return path) and the “header from” (visible to all users).
- SPF works by looking at the *Return-Path* value of a domain included in the email’s headers. The receiving server extracts the domain’s SPF record, and then checks if the source email server IP is approved to send emails for that domain.
- If the IP address sending email on behalf of the “envelope from” domain isn’t listed in that SPF record, the message fails SPF authentication.
- *Note: Unfortunately SPF is not perfect as it not able to prevent “header from” misrepresentation or e-mail spoofing*

DKIM Explained

DKIM Explained

- DKIM stands for **DomainKeys Identified Mail**. It is an e-mail authentication method that allows senders to associate a verified domain name with the e-mail message, thus preventing e-mail spoofing (or forgery) from occurring via that domain.
- The sender first needs to decide which elements of the e-mail to include in the signing process e.g. entire message (header and body) or one or more fields of the e-mail header.
- The elements selected must remain unchanged in transit, or the DKIM signature will fail authentication. So if certain parts of the body is forwarded (and not the entire body), DKIM authentication will fail.
- Before an e-mail is sent, a hash is created for the selected elements and that hash is encrypted using a private key. The e-mail provider receiving the e–mail then runs a DNS query to find the public key for that domain – allowing a decryption of the DKIM signature back to the original hash string

LIVE DEMO

Questions?