Email Cybersecurity – First Day at CODEWORK AI

Date: 28/08/2025

How Email Cybersecurity Works

Email cybersecurity ensures that messages are delivered from trusted senders to intended recipients without being tampered with or spoofed. It relies on authentication protocols, encryption, and careful analysis of email headers to identify malicious activity. These protections prevent phishing, spam, and unauthorized domain usage.

SPF (Sender Policy Framework)

SPF is a DNS-based email authentication method that specifies which mail servers are authorized to send emails on behalf of a domain. When an email is received, the recipient's server checks the sender domain's SPF record to verify authenticity. Example: If example.com authorizes only 192.0.2.10 as its mail server, any email coming from a different IP will fail SPF validation.

DKIM (DomainKeys Identified Mail)

DKIM adds a digital signature to each outgoing email. The signature is created using a private key, and recipients verify it using the sender's public key published in DNS. This ensures that the email content has not been altered in transit and confirms the sender’s identity. Example: Marketing emails signed with DKIM allow ISPs to trust the email source even if the SPF check fails.

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

DMARC builds on SPF and DKIM to instruct email servers how to handle messages that fail authentication checks. It also provides reporting features so domain owners can monitor unauthorized email activity.

DMARC Policies: none, quarantine, reject

• none – Monitor mode, no impact on email delivery. • quarantine – Suspicious emails are sent to the spam folder. • reject – Emails failing authentication are blocked entirely.

How to Check Real-World Email Headers Manually

To verify SPF, DKIM, and DMARC, you can manually inspect the full email headers: 1. Open the email and select 'View Original' or 'Show Headers' in your mail client. 2. Look for 'Received-SPF', 'DKIM-Signature', and 'DMARC' fields. 3. Analyze these results to confirm if the email truly originated from the claimed domain.