Lodestone

MARCH 2023

STATE OF CYBER

monthly newsletter

HOW TO IDENTIFY AND PROTECT YOURSELF FROM EMAIL SPOOFING

Email Spoofing is a technique involving sending emails with a fake sender address, stealing the identity of a real user that is typically trusted in the eyes of the victim. It is important to be sure that your emails are protected from spoofing multidirectional. Spoofed emails could lead to users downloading malware, loss of data, and reputational damage.

To start securing your emails Lodestone recommends considering configuring DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC), and Sender Policy Framework (SPF). While seemingly common Lodestone has found that these protections can be overlooked, not enabled, or misconfigured, especially in smaller organizations.

DKIM shows the legitimacy of the email belonging to the proper user by providing a digital signature in the email header. When the email is received, the signature can be verified to ensure the email is in fact from the domain owner.

SPF enables an authorized list of email senders. When an email is received the recipient email client can confirm that the IP address of the sender matches the SPF list.

DMARC will tell the receiving email server what to do with the results from SPF and DKIM. If an email fails either the SPF or DKIM checks, the DMARC could instruct your mail servers to quarantine, reject, or continue to deliver them despite the risk. It would also contain instructions to send reports to domain administrators about emails passing or failing the checks as a running log for these administrators to react as needed.

While these technologies are increasingly vital in good email hardening, user training remains the most effective form of prevention. Consider a phishing assessment as a means to test both these controls and your user training.

THE STATE OF EMAIL SECURITY 2023

A rising number of victims to phishing with as many as 91% of respondents also reporting attempts of spoofing their email domains. The report found only 27% as having deploying tools such as DMARC.

HOW TO PREVENT EMAIL SPOOFING IN GMAIL?

An article talks about DKIM, SPF, and DMARC and the step-by-step process to turn these tools on in a Gmail workspace.

A PRACTICAL GUIDE TO IDENTIFYING PHISHING EMAILS

An article about various phishing examples and how to quickly detect them to help assist people who may not be aware of the tactics people use to scam via email.

HOW IS CHATGPT AI CHANGING PHISHING EMAIL ATTACKS?

An article about how ChatGPT helps propagate phishing emails in a faster, more cost-efficient way for hackers.

Contact Us: 320 East Main St, Lewisville, TX 75057. Tel: 1-203-307-4984. www.lodestone.com