What Is Email Spoofing

E-mail spoofing is sending an e-mail to another person so that it appears that the e-mail was sent by someone else.

We most commonly see spoofed accounts used to send spam, phishing content, or malicious viruses. Spammers will steal a real person's e-mail address in order to trick anti-spam filters and make the e-mail seem legitimate and written by a real person, possibly someone you know.

If you have received a high volume of 'Mail delivery failed' bounceback emails in your inbox, there is a high chance that your email address has been spoofed.

What Can You Do?

In order to prevent spoofed emails from being delivered, we can add a SPF and DKIM records to the DNS for your domain. SPF and DKIM records are types of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of these records are to prevent spammers from sending messages with forged “From:” addresses at your domain. Recipients can refer to the SPF record to determine whether a message purporting to be from your domain comes from an authorized mail server. The SPF does not actually block spoofing; depending on how the receiving server is set up, usually, the SPF record will only result in mail that does not match the SPF rules will be placed in the Spam/Junk folders.

If you have cPanel email, and would like an SPF and DKIM Record to be added, you can do so in cPanel > Email Authentication > SPF
If you have a chimail email, please contact us in order for a DKIM and SPF record to be implemented.

Unfortunately, beyond these authentication records, there is not much else that can be done to prevent spoofed e-mails from being sent.

If your email address was spoofed, this is usually a temporary issue that will resolve itself in a few weeks once the bad-actor has moved on to using a different email address to spoof. We do strongly recommend running an anti-virus scan on any machines and devices that you have recently used to access your email account, to ensure that they are free of any malicious software. We would also recommend that you update your email account's password, using a secure combination of letters, symbols, and numbers at least eight characters in length.

You can look at the "headers" information to see where the spoofed e-mail actually originated from. Depending on the circumstances, you can help stop spammers by also sending the full headers of these unlawful messages to the Federal Trade Commission at spam@uce.gov.

Related articles

Content by label

There is no content with the specified labels