What Is Email Spoofing

What Is Email Spoofing?

E-mail spoofing (or forging) 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.

What Can You Do?

In order to prevent spoofed email from being delivered, we can add an SPF record to the DNS for your domain. An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain.

The purpose of an SPF record is 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 would like an SPF Record to be added you can do so in cPanel > Email Authentication > SPF

Unfortunately, beyond an SPF Record, there is not much else that can be done to prevent spoofed e-mails from being sent.

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.