**Email Spoofing**

**Description 1**

Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). Examples of spoofed email that could affect the security of your site include: [1]

* email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this
* email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

**Description 2**

The idea of email spoofing is that if an email appears to originate from a known sender, the target of the phishing email will be more likely to fall for the scam. Spoofing an email address is a relatively easy thing to do, but it does not pose a major problem for people whose addresses are spoofed.

In order to spoof an email, hackers will use techniques that change the "from" field in an email from the actual spam email address to a legitimate email address. Email spoofers will try to harvest real email addresses online, so it is important not to publicly display your email address. Sometimes though, hackers will simply try combinations of letters and numbers until they find a genuine email address to spoof. In those cases, there is nothing you can do to stop your email from being spoofed.

It is important to understand that just because your email address has been spoofed, it does not mean that your email account has been hacked. Someone may be able to spoof your email address, but it does not mean that they were able to read the messages you have stored in your email account. [2]

**Description 3**

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although most spoofed email falls into the nuisance category and requires little action other than deletion, the more malicious varieties can cause serious problems and pose security risks. For example, a spoofed email may purport to be from a well-known shopping website, asking the recipient to provide sensitive data such as a password or credit card number. Or the spoofed email may ask the recipient to click on a link that installs malware on the recipient's computing device. [3]

**Reference**

[1] <https://www.cert.org/historical/tech_tips/email_spoofing.cfm>

[2] <https://security.illinois.edu/content/email-spoofing>

[3] <http://searchsecurity.techtarget.com/definition/email-spoofing>