

Forum:[Hack Forums](#)

Thread: [Hiding sender e-mail address](#)

Impleo - December 28, 2017, 5:23 am

Hi,

I'd like to send e-mail to another person, but he should think that e-mail was received not from me. For instance, let's say my e-mail is "mis.dauntry@gmail.com". I'd like to send e-mail to "np@rndv.no". But when he receives e-mail from me, he should see, that sender was "misdauntry@gmail.com" (similar e-mail, but without a dot). I don't want to hack "misdauntry@gmail.com" and I don't want to actually send e-mail from this address, but I want receiver to think, that he received e-mail from this address. Is it possible to do that?

Nomad.Null - December 28, 2017, 6:56 am

Yes. This is a technique known as Email Spoofing and is quite well-known but not so easily done. The way it is done is by modifying the email header which contains details about the message that you see such as FROM TO CC BCC and Subject. You can freely modify the email to say it is from anywhere or anyone you want by doing this, but it's not likely to be delivered because mail servers (especially gmail) have checks for this sort of thing. About 10-15 years ago, there were no checks against this kind of falsification of email headers, and email would be delivered regardless. However, now most SMTP (Simple Mail Transfer Protocol, used for email) servers, especially Gmail, require an authentication check before it will accept a request to deliver an email. If you cannot pass this authentication check (usually user and password) it will refuse to deliver the message.

There are ways around this however, and you can send messages from other email servers which do not have these checks. These are known as open relays, but they are rare, and largely blacklisted across the internet because they are often used for spam and are considered woefully insecure. There are also other email servers which are configured to allow certain domains to send emails on their behalf, via SPF (Sender Policy Framework) records, which are a form of DNS record that tells the world "These organizations are allowed to send emails on my behalf" and summarizes a list.

This is usually the case for organizations which have their own internal email server and email domains. SPF is designed to prove that you are not a source of spam and also to prevent unauthorized organizations from sending emails pretending to be from your domain, but if poorly configured, they can also make your organization almost as bad as an open relay.

I think I've given you enough material that you can do some further research on your own at this point. Go forth and read.

Impleo - December 29, 2017, 12:17 am

Thanks for your reply. After investigation I decided that open relay would be the best for my purpose. However, I see that open relays are usually blacklisted. Does that mean that receiver won't be able to get e-mail from open relay? Also, my intent is to send only 1 e-mail (not a spam). Will e-mail from open relay go to the receiver's spam folder? Is it possible to send e-mail from open relay and pretend that it's being sent from gmail?

Nomad.Null - December 29, 2017, 6:50 am

It is more likely that the email will not be delivered at all. Any open relay email server is usually

denied by gmail and other email service providers outright, refusing to handle or deliver the email. It is simply dropped.

Impleo - December 30, 2017, 7:30 am

Do you know, where I could find open relays, which would be not blacklisted? Maybe there are some recommendations? Google gives me only blacklisted ones.

Nomad.Null - December 30, 2017, 10:26 am

(Dec 30, 2017 08:30 AM)Impleo Wrote: [\[CITE\]](#) Do you know, where I could find open relays, which would be not blacklisted? Maybe there are some recommendations? Google gives me only blacklisted ones.

Therein lies your problem. If google can find an open relay, it gets blacklisted. Automatically. Same goes for Microsoft, Yahoo, and Protonmail. You will be very hard-pressed to find a legitimate open relay. I'm afraid I can't help you here. From here on, you'll have to do your own research.