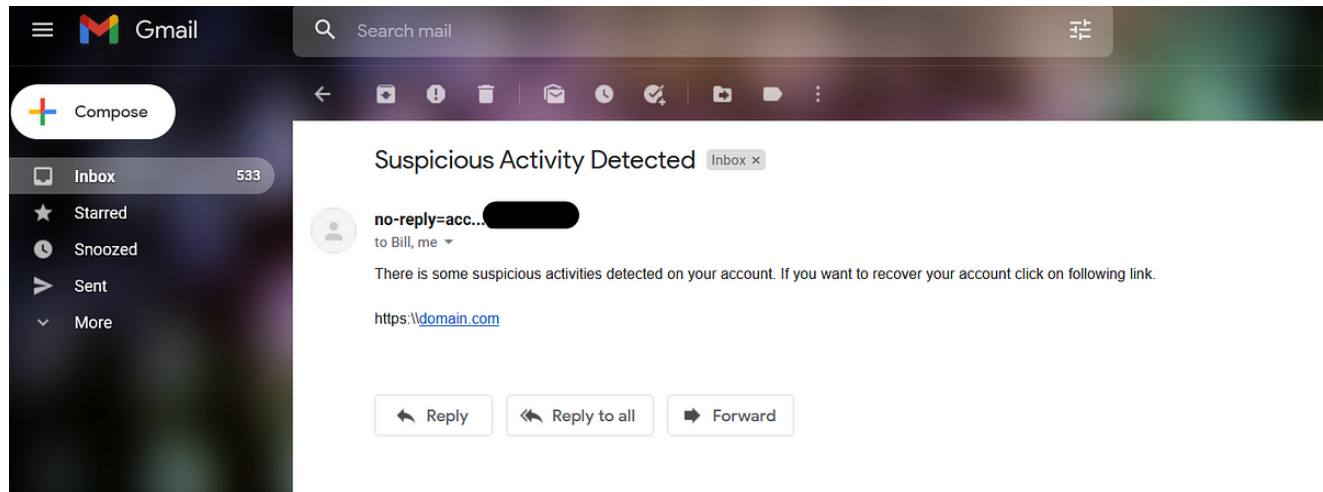


The art of defense evasion — part 4 — Spoofing

osamaellahi.medium.com/the-art-of-defense-evasion-part-4-spoofing-3a3d6ece5ff

Osama Ellahi

July 2, 2022



Tricking the real entity to do some malicious tasks.



Osama Ellahi

--

Introduction to Spoofing

Spoofing is mimicking some entity and asking the user to perform certain action according to the intention of an attacker. It includes both technical and non-technical stuff. Mostly it is dependent on the information that you use for tricking the victim. If the information is more related to the victim than there is more chance that he/she can be tricked. Spoofing is a major part of phishing, without better spoofing phishing campaign may result in failure.

Almost every organization have great security control but when it comes to spoofing every organization is vulnerable, just need the right information. In this blog I will show you how its done and how to mitigate them. Well there is one mitigation that you may have already known which is proper awareness but it needs to be updated because the techniques in phishing are also being updated.

Nowadays attackers did not just message you and pretends like your friend and ask for some money, it could be way more worst than that.

Email Spoofing

Cyber criminals use a lot of techniques when it comes to email spoofing because this is the main entry point for their attack path. Email spoofing can be done through many sources, there are public tools available for spoofing. But I will show you the spoofing which will not be blocked by the email-gateways because it will be a legitimate email to email-gateways also. Actually let's first understand how the email spoofing is done.

When you are sending email from your public server from "PHP" or some other language you have to tell the server to put this email in header in place of "From email" and send the mail using the following function.

```
mail($to,$subject,$txt,$headers);
```

With this function email can be sent from anybody's email to anyone's email. But there is some limitation behind it. There is "email-gateway" and "email scanners" who check every email, when they see that the sending mail's domain is not matching the real server, they mark it as suspicious and then this email goes to spam or in a junk mail box. There are other checks also for email scanning like they even check the reputation of the sending domain and most importantly if the email is signed or not. There are flags used for this all process like **DKIM** which is "email receiver will run a DNS query to search for the public key for that domain." **Sender Policy Framework (SPF)** is an email authentication protocol that domain owners use to specify the email servers they send email from, making it harder for fraudsters to spoof sender information.

So this email function could not help us here in email spoofing. But wait, there is legitimate use of the mail() function is also there. So let's understand it once again.

Some websites have a API/interface for inviting the friends to their website using email and everyone can send the email to invite the friends. These APIs are vulnerable because the user can even set the "FROM email" in headers which makes them dangerous.

This is not only one case, there are thousands of websites publicly available and open for attackers. Like look at this case this website required a user to sign up and it is actually a well known conference by famous publishers. For test case I send a dummy paper and

These messages come straight to your inbox

Now let's look at the original message of over mail. As you can see it shows nothing malicious because the message is signed by the website and it also has some popularity. You can also see the flags and subject of mail which we send "Suspicious Activity Detected". By the way you need to avoid some words like "suspicious" and "click on link" etc to get more accuracy.

In this mail still they are sending their domain name which may look suspicious for some users. But there are thousands of websites who work very fine with spoofing.

Message Spoofing

We sometimes see a suspicious message that comes from a legitimate number, so start believing that it is not suspicious. Like let me give you a practical example here the OTP (One Time Pass-code) that you have set up for Facebook or Google or some other domains, they send you a message from 56789. Using online messaging services we can send a message anybody from "56789". This shows that this number did not belong to any entity and everyone can use it for their own benefits.

Only thing that can be copyrighted is the name like if you see a message from "Google" that might be legitimate. But some attackers can even bypass human eye with character playing. Like they can send you a message from "g00gle" or "G00GLE". For demo you can use any online messaging service.

IP and UserAgent Spoofing

The request identifies the user. If user is using a browser there will be a user agent which tells the server that user is using which browser, which OS and which version of (OS / browser). But when it comes to IP, some servers use them for identification and logs. Like if an attack happened on an organization, there will be IP which tell the location of the user. Yes and attacker might be using VPN but let me show you another very interesting aspect of it which is IP spoofing. There are IPs that be set up in your browser and some servers use these IPs as the primary source of the user information. These are called **X-Forwarded-For**.

The **X-Forwarded-For** (XFF) request header is a de-facto standard header for identifying the originating IP address of a client connecting to a web server through a proxy server.

The amazing part is if we can change them to whatever we want, we can set our XFF to Google's public IP or even our victim's public IP.

And user-agent can also be easily changed, if you are sending the request from any programming language you can set user-agent to whatever you want, if you are using browser there are add-ons and extensions available just search "user-agent switcher" and you are good to go.

Let's see this example it is same example from email spoofing. So apparently they are even recording my IP and user agent also for the record.

For user-agent switching I use "user-agent switcher" and set me like I am a Google Bot.

For IP switching I use "X-Forwarder-For header". But keep in mind if server is getting the real client IP it can't be changed only x-forwarded-For, X-Originating-IP, X-Remote-IP and X-Remote-Addr can be changed because these are send in request headers.