Email Spoofing: In Today’s Era

Prashant D. Chauhan (✉ prashant.chauhan-cc@msubaroda.ac.in)
The Maharaja Sayajirao University of Baroda
Apurva M. Shah
The Maharaja Sayajirao University of Baroda

Research Article

Keywords: Email Spoofing, SMTP, SPF, DMARC, DKIM

Posted Date: December 5th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2328294/v1

Additional Declarations: No competing interests reported.

Email Spoofing: In Today's Era

Mr. Prashant D. Chauhan
Department of Computer Science and Engineering,
The Maharaja Sayajirao University of Baroda,
Vadodara, Gujarat, India
prashant.chauhan-cc@msubaroda.ac.in

Prof. (Dr.) Apurva M. Shah
Department of Computer Science and Engineering,
The Maharaja Sayajirao University of Baroda,
Vadodara, Gujarat, India
apurva.shah-cse@msubaroda.ac.in

Abstract- **Email spoofing has been there since many years making it one of the main choices of the attackers or spammers who wish to gain access to some private information of victims to misuse it or to get some kind of financial benefit. We all know that email spoofing is possible only because of the fact that the entire email system works on SMTP which doesn't provide any mechanism to check authentication of the sender of the email. With the increasing research in the field of security many protocols have been designed to overcome the problem of spoofing of email address. In this paper, we try to find out whether email spoofing is still possible or not by the end of the year 2022.**

Keywords – Email Spoofing, SMTP, SPF, DMARC, DKIM

Statements and Declarations

- **Competing Interests**

  No funding was received to assist with the preparation of this manuscript

  The authors have no relevant financial or non-financial interests to disclose.

I. INTRODUCTION

Email has now a days become one of the most widely used means of communication which is quick as well as cost-efficient [1]. With the increasing use of email, the cases of email spoofing have also been increasing. To prevent email spoofing many protocols have been developed like SPF, DKIM and DMARC [8]. With time, adoption of these protocols has also increased drastically [2][3]. Now, it is a mater of question whether the problem of email spoofing has been resolved completely or partially after the use of these anti-spoofing protocols [4][5].

In this paper, we try to find out whether as of today, spoofing of email is possible or not even after the usage of anti-spoofing protocols by majority of the email servers and the domain owners. For this, we first created our own email server, and configured the anti-spoofing protocols on it to prevent email spoofing. Then, we tried various approaches to bypass one or more of the anti-spoofing protocols in order to check whether our spoofed email reaches the inbox or spam of the recipient user or gets rejected completely by the receiving email server.

We detected top 10 email service providers and performed our experiment on them. The selected service providers for our experiment were Gmail, Outlook, Proton Mail, AOL Mail, Yahoo Mail, Zoho Mail, iCloud Mail, Rediff Mail, mail.com and Yandex Mail [6][7]. We made various test cases and tried to spoof emails sent to these 10 email service providers. By performing this experiment, we analyzed the success ratio of spoofed email on the selected email servers.

II. THE EXPERIMENT

To prevent and detect spoofing of email, many SMTP protocols are developed. Out of these most effective ones are SPF, DKIM & DMARC. For email server we used Modoboa version 1.17.0 installed on Ubuntu 20.04.3 LTS

A. *Scenario – 1: Spoofing with SPF, DKIM & DMARC from own email server*

In this case, we selected our own email server domain as the sending email domain i.e., **mail-server.in.** The selected sending domain has implemented all three authentication protocols i.e. Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC). We selected **prashant@mail-server.in** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC
Gmail	Inbox	Pass	Pass	Pass
Outlook	Spam	Pass	Pass	Pass
Proton Mail	Inbox	Pass	Pass	Pass
AOL Mail	Inbox	Pass	Pass	Pass
Yahoo! Mail	Inbox	Pass	Pass	Pass
Zoho Mail	Inbox	Pass	Pass	Pass
iCloud Mail	Inbox	Pass	Pass	Pass
Rediffmail.com	Inbox	Pass	Pass	Pass
Mail.com	Inbox	Pass	Pass	Pass
Yandex Mail	Inbox	Pass	Pass	Pass

Table1: Experiment results for prashant@mail-server.in

From the above table, we can conclude that our email server can successfully deliver email to the inbox of all major email service providers and the sent email passed all 3 protocols successfully. Only in case of outlook.com, our email was sent to spam instead of inbox.

B. *Scenario – 2.1: Spoofing with SPF, DKIM & DMARC*

In this case, we selected **gmail.com** as the sending email domain which uses all three authentication protocols SPF, DKIM and DMARC. We selected **prashant@gmail.com** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Fail	via shown
Outlook	Spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Fail	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown

iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	warning
Mail.com	Inbox	Pass	Pass	Fail	-
Yandex Mail	Spam	Pass	Pass	Fail	-

Table2: Experiment results for prashant@gmail.com with single sender email id

From the above table we found that DMARC was failed in all the cases due to identified alignment issue while both SPF and DKIM were passed by all the email servers used in experiment for the spoofed email. Gmail and Zoho Mail shows "via" message along with the sender email id. Proton Mail and Rediffmail displays a warning message to the user along with the email and in most cases the email is successfully delivered to inbox without any kind of warning to the user. To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the result of which is as follows:

Receiving Server Name	**Delivery Location**	**SPF**	**DKIM**	**DMARC**	**Remarks**
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	warning
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	Fail	-

Table3: Experiment results for prashant@gmail.com with multiple sender email id

From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail and Proton Mail which was not possible with single sender id. Even no "via" message was shown in case of Gmail for the spoofed email with multiple sender email ids which was displayed in case of spoofed email with single sender email id. Also, in case of mail.com the email was completely rejected and not delivered to the recipient user when multiple sender email ids were used.

C. Scenario – 2.2: Spoofing with SPF, DKIM & DMARC

In this case, we selected **outlook.com** as the sending email domain which uses all authentication protocols SPF, DKIM and DMARC. We selected **prashant@outlook.com** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	**Delivery Location**	**SPF**	**DKIM**	**DMARC**	**Remarks**
Gmail	Inbox	Pass	Pass	Fail	via shown
Outlook	spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Fail	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	-
Mail.com	Inbox	Pass	Pass	Fail	-
Yandex Mail	Spam	Pass	Pass	Fail	-

Table4: Experiment results for prashant@outlook.com with single sender email id

From the above table, we can see that DMARC was failed in all the cases due to identified alignment issue while both SPF and DKIM were passed by all the email servers used in experiment for the spoofed email. Gmail and Zoho Mail shows "via" message along with the sender email id and Proton Mail displays a warning message to the user along with the email and in majority of the cases the email is successfully delivered to inbox without any kind of warning to the user.

To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the result of which is as follows:

Receiving Server Name	**Delivery Location**	**SPF**	**DKIM**	**DMARC**	**Remarks**
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Pass	Fail	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	Fail	-

Table5: Experiment results for prashant@outlook.com with multiple sender email id

From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail and Proton Mail which was not possible with single sender id. Unlike the case with single sender email id, even no "via" message was shown in case of Gmail for the spoofed email with multiple sender email ids. Also, in case of Mail.com the email was completely rejected and not delivered to the recipient user when multiple sender email ids were used.

D. Scenario – 3: Spoofing with only DKIM

In this case, we selected **msubaroda.ac.in** as the sending email domain which uses only DKIM protocol. We selected **prashant@msubaroda.ac.in** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	**Delivery Location**	**SPF**	**DKIM**	**DMARC**	**Remarks**
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Fail	none	-
Mail.com	Inbox	Pass	Pass	none	-
Yandex Mail	Spam	Pass	Pass	none	-

Table6: Experiment results for prashant@msubaroda.ac.in with single sender email id having only DKIM record

From the above table, we can see that result of DMARC is shown as "none" as the selected domain has not published DMARC record. It is to be noted that in all the cases SFP was passed even though the selected domain has not published any SPF record. Also, Gmail and Zoho Mail shows “via” message along with the sender email id.

To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the result of which is shown in Table7. From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail and Proton Mail which was not possible with single sender id. Also “via” message was shown in case of Zoho Mail and warning was shown only in Proton Mail.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Inbox	Pass	Pass	none	-

Table7: Experiment results for prashant@msubaroda.ac.in with multiple sender email id having only DKIM record

E. Scenario – 4: Spoofing with only SPF

In this case, we selected **orthocarehospital.in** as the sending email domain and we published only SPF records for this domain for the purpose of our experiment. We selected **prashant@orthocarehospital.in** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Inbox	Pass	Pass	Pass	-
Yandex Mail	Spam	Pass	Pass	none	-

Table8: Experiment results for prashant@orthocarehospital.in with single sender email id having only SPF record

From the above table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has only published its own SPF record and all the email were delivered to the inbox except Yandex Mail which delivered the spoofed email in spam folder. Also, Gmail and Zoho Mail shows “via” message along with the sender email id except which warning was shown in none of the selected email servers. The results for multiple sender ids in spoofed email are shown in table 9. From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail and iCloud Mail which was not possible with single sender id. The “via” message was shown only in case of Zoho Mail and email was delivered to spam folder for AOL Mail, Yahoo Mail, iCloud Mail and Yandex Mail. For the rest, all the email were successfully delivered to the inbox of the recipient user.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Spam	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table9: Experiment results for prashant@orthocarehospital.in with multiple sender email id with only SPF record

F. Scenario – 5: Spoofing with SPF and DKIM

In this case, we selected **orthocarehospital.in** as the sending email domain and published both SPF and DKIM records in the DNS for this domain. Then, we selected **prashant@orthocarehospital.in** as the spoofed sending email id for this case. The result of our experiment for this case is as follows:

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	-
iCloud Mail	Inbox	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Inbox	Pass	Pass	Pass	-
Yandex Mail	Spam	Pass	Pass	none	-

Table10: Experiment results for prashant@orthocarehospital.in with single sender email id having SPF and DKIM records

From the above table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has published its own SPF and DKIM records and all the email were delivered to the inbox except for Yandex Mail where the email was delivered in the spam folder. Also, only Gmail shows “via” message along with the sender email id rest all others just delivers the spoofed email without any kind of warning to the end user. Then we performed the same experiment by sending multiple sender ids in spoofed email whose results can be seen in Table 11. From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail, Proton Mail and iCloud Mail which was not possible with single sender id. Also “via” message was shown only in case of Zoho Mail and email was delivered to spam folder only for AOL mail and Yandex mail, for rest all the email was successfully delivered to the inbox of the recipient user.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	Pass	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table11: Experiment results for prashant@orthocarehospital.in with multiple sender email id having only SPF and DKIM records

G. *Scenario – 6: Spoofing with no authentication*

In this case, we selected **gujarattourism.com** as the sending email domain which uses none of the authentication protocols. We selected **prashant@gujarattourism.com** as the spoofed sending email id in this case. The result of our experiment in this case is as follows:

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Fail	none	-
Mail.com	Inbox	Pass	Pass	none	-
Yandex Mail	Spam	Pass	Pass	none	

Table12: Experiment results for prashant@gujarattourism.com with single sender email id

From the above table, we can see that result of DMARC is shown as "none" as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has not published its own SPF and DKIM records and all the emails were delivered to the inbox except for Yandex Mail and Outlook. Also, only Gmail and Zoho Mail shows "via" message along with the sender email id.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	Pass	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table13: Experiment results for prashant@orthocarehospital.in with multiple sender email id

Then, we performed the same experiment by sending multiple sender ids in spoofed email whose results are displayed in Table 13. From this table, we can see that by using multiple sender ids we were able to pass all three protocols in case of Gmail, Proton Mail and iCloud Mail which was not possible with single sender id. Also "via" message was shown only in case of Zoho Mail and email was delivered to spam folder only for AOL Mail and Yandex Mail, for rest all, the email was successfully delivered to the inbox of the recipient user. Also, the email was completely rejected by Mail.com server, when multiple sender email ids were used in the spoofed email.

III. The Conclusion

With our experiment we conclude that in present scenario the only options for preventing spoofing of email are authentication protocols namely SPF, DKIM and DMARC which are not sufficient enough to prevent email spoofing completely. Also, with experiment we found that there are some ways like sending spoofed email with multiple sender email ids, by which we may bypass all the three authentication protocols SPF, DKIM & DMARC and make way for the spoofed email to the inbox of the recipient user instead of marking the email as spam or rejecting the email all together.

Identifier alignment used in DMARC is helpful in marking the email as DMARC fail but, the liberal DMARC policy of allowing the email even in case of failure of DMARC many times leads the email to the inbox of the user which might be dangerous for the recipient. Some of the email service providers like Gmail and Zoho Mail shows a "via" message along with the sender email id which is quite helpful in detecting the source of the email and warn the user for possibility of spoofing. Also, in few cases, only Proton Mail and Rediffmail displayed a warning message to the user so as to warn him of possibility of spoofing of email, while rest others displayed no warning to the user regarding possibility of spoofing. We suggest need of some additional security measures to ensure prevention of email spoofing which is still possible by some tweaks by the attackers.

Research Data Policy

All relevant raw data, will be freely available to any researcher wishing to use them for non-commercial purposes

Data Availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] "Email Trouble: Secrets of Spoofing, the Dangers of Social Engineering, and How We Can Help", Bridget Opazo, Don Whitteker, Chen-Chi Shing, 13th International Conference on Natural

[2] "Identifying Email Threats Using Predictive Analysis", Yuanyuan Grace Zeng, International Conference on Cyber Security And Protection of Digital Services, IEEE, 2017

[3] "Towards the Adoption of Anti-spoofing Protocols", Hang Hu, Peng Peng, Gang Wang, arXiv:1711.06654v3, 2018

[4] "Securing Email", Jeremy Clark, P.C. van Oorschot, Scott Ruoti, Kent Seamons, Daniel Zappala, arXiv:1804.07706v, 2018

[5] "A Comprehensive Secure Email Transfer Model", Geethapriya Liyanage, Shantha Fernando, 12th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2017

[6] "Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks", Proceedings of the 30th USENIX Security Symposium. August 2021

[7] "Improvement of Legitimate Mail Server Detection Method using Sender Authentication" IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications (SERA), 2021

[8] "Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis" IEEE Transactions on Network and Service Management (Volume: 18, Issue: 3, September 2021)