Characterizing Reverse DNS Deployment for SPF-indicated Sender IP Addresses

Hibiki TOKUNO
Nihon University
Tokyo, Japan
cshb25009@g.nihon-u.ac.jp

Minami YODA
Nihon University
Tokyo, Japan
yoda.minami@nihon-u.ac.jp

Shuji SAKURABA
The University of Electro-Communications
Tokyo, Japan
sakuraba.shuji@ohsuga.lab.uec.ac.jp

Yutaka MATSUNO
Nihon University
Tokyo, Japan
matsuno.yutaka@nihon-u.ac.jp

***Abstract*—In recent years, the configuration of reverse DNS (Pointer records) for outgoing mail servers has become a critical factor in identifying phishing emails. The Council of Anti-Phishing Japan, a leading organization in the field, has reported that a significant majority of observed phishing emails originate from servers lacking PTR records. Furthermore, Google's *Email Sender Guidelines*, published in October 2023, require valid PTR records for all senders. These guidelines stipulate that Forward-Confirmed Reverse DNS (FCrDNS)—where the source IP address and its reverse hostname are mutually resolvable—is a fundamental requirement for successful email delivery. Despite these developments, there remains a lack of comprehensive, large-scale empirical research regarding the actual implementation of PTR records across mail servers. This study clarifies the current state of reverse DNS adoption in real-world operations by conducting large-scale measurements of SPF-indicated candidate sender addresses within the Tranco Top 1M domains. We investigated 20,964,277 potential sender addresses extracted from the Tranco Top 1M list. Our results reveal that 41.1% of all IP addresses were classified as PTR-configured, while FCrDNS was successfully established for only 23.0%. Furthermore, we report that the configuration rates vary significantly depending on the specific SPF mechanisms employed.**

***Index Terms*—email, anti-spam, DNS, PTR, FCrDNS, SPF**

I. Introduction

Phishing and other email-based fraudulent activities continue to represent a severe threat to individuals, organizations, and the overall Internet infrastructure. According to the APWG Phishing Activity Trends Report [1], 989,123 phishing attacks were observed in the fourth quarter of 2024 alone. Furthermore, the FBI's Internet Crime Complaint Center (IC3) reported that phishing/spoofing was the most frequently reported crime category in 2025, accounting for 191,561 complaints, with losses from Business Email Compromise (BEC) exceeding $3 billion [2]. These statistics underscore that email remains a primary attack vector for cybercrime and that enhancing sender authenticity is a critical challenge.

Observations by anti-phishing organizations in Japan have indicated that the PTR configuration rate for source IP addresses of spam emails is notably low. However, the significance of these low configuration rates can only be interpreted accurately when compared against baseline values from legitimate senders. Furthermore, Google's *Email Sender Guidelines* [3] now require valid PTR records for all senders, establishing Forward-Confirmed Reverse DNS (FCrDNS) as a prerequisite for successful delivery. Consequently, understanding the actual deployment status within legitimate infrastructure is essential not only for threat analysis but also for ensuring deliverability and service quality. To address this need, our study conducts a large-scale measurement of potential sender IP addresses. To establish a representative baseline of legitimate infrastructure, we leverage the Sender Policy Framework (SPF) [4] records of popular domains as a reliable source for identifying and extracting these candidate addresses.

This study aims to fill this gap by investigating the adoption status of PTR records for SPF-indicated candidate sender infrastructure of popular domains. The objective of this research is to clarify the extent to which PTR records are configured within legitimately operated email infrastructure, thereby providing an empirical foundation for interpreting PTR-related observations in spam and phishing analysis.

The main contributions of this paper are as follows:

1) Empirical Analysis of PTR and FCrDNS Deployment: We conducted a large-scale measurement of actively used and highly recognized domains (Tranco Top 1M [5]) and reported on the actual status of PTR and FCrDNS configurations.
2) Analysis of Implications for Spam and Phishing Detection: Using the observed PTR and FCrDNS deployment status as a baseline for SPF-indicated sender addresses, we discuss the usefulness and limitations of reverse DNS information as a factor in spam and phishing detection.

II. Background

A. Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an email authentication technology designed to mitigate spoofing of sending domains. A domain administrator publishes, as a DNS `TXT` record, the hosts authorized to send emails from the domain. Upon

receiving an email, the receiving mail server refers to the SPF policy of the domain indicated by the SMTP `MAIL FROM` or `HELO/EHLO` identifier and verifies whether the source IP address is authorized. The SPF authentication result is used by the receiver in handling the email and is also used in DMARC [6] for identifier alignment evaluation with the `RFC5322.From` domain. In an SPF record, mechanisms specify the conditions for authorizing source candidates, qualifiers define the resulting action when a match occurs, and modifiers provide additional evaluation behaviors. Representative mechanisms include `a`, `mx`, and `ip4`, while qualifiers such as `+`, `-`, and `?` are commonly used. Additionally, modifiers like `redirect` can be used to define complex evaluation logic.

III. Related Work

Arouna et al. [7] investigated the deployment of reverse DNS using potential mail-sending IP addresses extracted from the OpenINTEL project dataset. Their research revealed that only 36.7% of the observed potential sender IP addresses maintained PTR records. Among these, 65.1% met the Forward-Confirmed Reverse DNS (FCrDNS) requirements, which corresponds to approximately 24% of all potential sender IP addresses. Furthermore, they reported that hostnames satisfying FCrDNS often do not align with the domains defining the corresponding SPF policies, suggesting that email transmission is frequently delegated to third-party infrastructures. In contrast, frequently utilized sources, such as major Mail Service Providers (MSPs), exhibited a very high compliance rate, with 96.8% meeting FCrDNS requirements and 93.9% maintaining a single PTR record.

While this prior study conducted a large-scale investigation of reverse DNS deployment across the entire internet and reported on FCrDNS requirements among major MSPs, our study focuses specifically on the Tranco Top 1M domains. This allows us to analyze the adoption of reverse DNS among domains that are actively used and highly recognized on the web. In addition to calculating the overall FCrDNS adoption rate, we investigate and report on configuration rates for each mechanism, domain-specific configuration rates excluding MSPs, and the specific status of PTR record configurations. Through this approach, we aim to clarify not only the extent to which reverse DNS is adopted but also how it is operated in practice in real-world environments.

IV. Methodology

A. Sender Estimation Based on SPF Records

SPF records define IP addresses authorized to send mail for a domain. In this study, we extract candidate sender IP addresses from SPF records. We used the Tranco Top 1M list [5] with list ID L76G4, which was first generated on March 16, 2026. From this list, we identified 669,676 domains with MX records, which were considered likely to provide email services. We then collected 736,120 SPF records, including those of domains referenced via the `include` mechanism.

To extract candidate sender IP addresses, we considered SPF mechanisms that can yield a `pass` result, namely `ip4`, `a`, `mx`, and `include`, with an explicit or implicit `+` qualifier. We also followed the `redirect` modifier when applicable. SPF records referenced by `include` and `redirect` were recursively evaluated, and DNS lookups for `a` and `mx` were performed to obtain the corresponding IPv4 addresses.

This study focuses exclusively on IPv4 addresses. Considering the realistic number of mail servers per domain and the CIDR prefix distribution in our dataset, we limited our analysis to prefixes from /20 to /32 and excluded broader prefixes. As a result, we identified 20,964,277 potential sender IPv4 addresses across the analyzed domains.

TABLE I
Classification of PTR configurations and FCrDNS consistency.

Status	Description
`FCrDNS_OK`	Valid PTR with a matching forward lookup.
`CNAME_CHAIN`	Valid FCrDNS established via CNAME.
`NO_PTR`	No PTR record assigned to the IP.
`NO_FORWARD`	PTR exists, but forward lookup fails.
`IP_MISMATCH`	PTR hostname resolves to a different IP.
`MULTI_PTR`	Multiple PTR records detected.
`PTR_ERROR`	Syntactically invalid hostname in PTR.

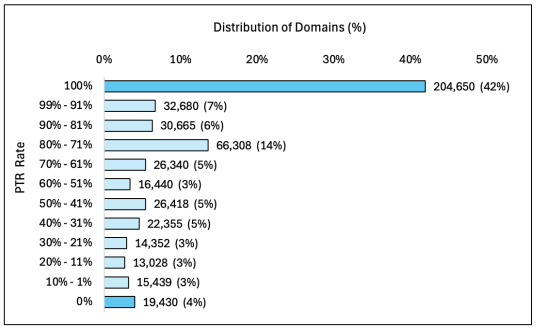
B. DNS Queries and Status Classification

1) Measurement Environment: From March to April 2026, we conducted DNS investigations on the 20,964,277 identified candidate IPv4 addresses. We employed ZDNS [8], a high-speed DNS measurement tool optimized for large-scale network assessments. The measurement was conducted in two phases: the resolution of SPF records and the FCrDNS validation for each IP address.

2) Categorization and Measurement Criteria: Based on the collected DNS responses, we classified the configuration status of each IP address into seven distinct categories, as shown in Table I. In this study, any status other than `NO_PTR` and `PTR_ERROR` is defined as "PTR configured." Among these, only those meeting the `FCrDNS_OK` or `CNAME_CHAIN` criteria are evaluated as "FCrDNS consistent."

C. Analysis of Reverse-DNS Configuration Policies

To analyze reverse-DNS deployment from the perspective of individual domains, we computed PTR and FCrDNS configuration rates for the candidate IPv4 sender addresses authorized by each domain's SPF record. However, a simple domain-level aggregation can be strongly affected by large shared mail infrastructures. Many domains authorize external email service providers, cloud platforms, or ISP-managed mail infrastructures through the SPF `include` mechanism. In such cases, the reverse-DNS configuration of the candidate sender addresses is likely to reflect the operational policy of the shared infrastructure provider rather than the configuration practice of the individual domain administrator. Therefore, to reduce this influence, we identified the top 1,000 domains most frequently referenced by the `include` mechanism in



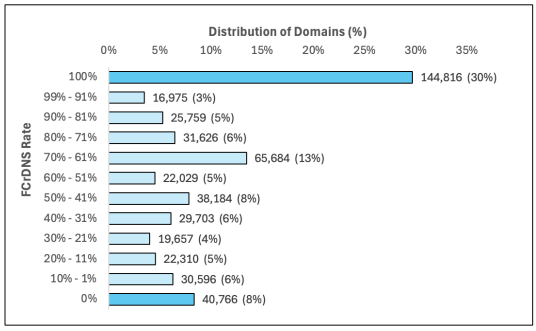


Fig. 1. Distribution of PTR and FCrDNS configuration rates among non-major domains.

TABLE II
PTR AND FCRDNS CONFIGURATION STATUS OF SPF-INDICATED CANDIDATE SENDER ADDRESSES.

Status	Count	Percentage (%)
FCrDNS_OK	4,810,953	22.95%
CNAME_CHAIN	11,256	0.05%
NO_PTR	12,301,165	58.68%
NO_FORWARD	3,070,678	14.65%
IP_MISMATCH	639,863	3.05%
MULTI_PTR	77,188	0.37%
PTR_ERROR	53,174	0.25%
Total	**20,964,277**	**100.00%**

the collected SPF records as major shared mail-infrastructure domains. We then excluded these domains themselves, as well as domains whose candidate sender IP addresses were obtained through them, from the domain-level distribution analysis. As a result, this study focuses on a final dataset of 488,105 domains. We further used MaxMind's GeoLite2 ASN and GeoLite2 Country databases [9] to assess whether PTR and FCrDNS configuration rates vary across ASes and countries.

V. RESULTS

A. Overall Deployment Status

Table II shows the measurement results for 20,964,277 SPF-indicated sender IP addresses. PTR records were found for 8,609,938 addresses (41.1%), while 12,354,339 addresses (58.9%) were classified as not PTR-configured, including NO_PTR and PTR_ERROR cases. FCrDNS was confirmed for 4,822,209 addresses (23.0%), including CNAME-chain cases. Thus, most SPF-indicated addresses did not satisfy FCrDNS consistency requirements. PTR records alone were also insufficient: 3,070,678 addresses (14.7%) had no forward A record, and 639,863 addresses (3.1%) had an IP mismatch.

B. Configuration Differences by SPF Mechanism and Prefix Length

Table III shows that host-level SPF mechanisms had higher configuration rates than broad `ip4` prefixes. The `mx` mechanism had the highest rates, with 80.7% PTR and 69.2% FCrDNS. The `a` mechanism and individual `ip4` addresses also showed relatively high FCrDNS rates of about 59%. In contrast, broader `ip4` prefixes such as /20 and /24 had only about 40% PTR and 22–23% FCrDNS.

TABLE III
PTR AND FCRDNS CONFIGURATION RATES BY SPF MECHANISM AND IPV4 PREFIX LENGTH

Mechanism	Total IPs	PTR	PTR Rate	FCrDNS	FCrDNS Rate
a	373,253	257,093	68.9%	218,612	58.6%
mx	162,886	131,439	80.7%	112,718	69.2%
ip4(with /20 prefix)	5,251,072	2,159,574	41.1%	1,219,148	23.2%
ip4(with /24 prefix)	7,229,184	2,918,847	40.4%	1,608,971	22.3%
ip4(with /32 prefix)	596,695	463,998	77.8%	357,240	59.9%
ip4(without prefix)	550,483	428,209	77.8%	329,367	59.8%

C. Configuration Distribution after Excluding Major Shared Infrastructures

Figure 1 shows the domain-level distribution after excluding major shared infrastructure providers. For PTR, 204,650 domains (42%) had PTR records for all candidate sender IP addresses, while 19,430 domains (4%) had none. For FCrDNS, 144,816 domains (30%) achieved full consistency, while 40,766 domains (8%) had no FCrDNS-consistent addresses. We also examined PTR and FCrDNS configuration rates across ASes and countries, but observed no clear AS- or country-level bias.

VI. DISCUSSION

A. Evidence of Administrator Awareness

The mechanism-level analysis suggests that many administrators recognize, to some extent, the necessity of reverse DNS in email delivery. In particular, the relatively high configuration rates of PTR and FCrDNS in `mx`, `a`, and individual /32 `ip4` entries indicate a tendency where addresses explicitly associated with specific hosts are more likely to have appropriate reverse DNS settings. These mechanisms are typically used to authorize servers that administrators clearly recognize as part of the mail transmission path. On the other hand, the low configuration rates of PTR and FCrDNS in broad `ip4` prefixes indicate that SPF policies often authorize an address range wider than the set of mail servers that are actually used and properly configured. Such over-authorization is considered a suboptimal configuration, as it unnecessarily increases the potential for abuse and administrative complexity. Furthermore,

this study confirmed that address spaces authorized by prefixes that may not correspond to actual sending hosts are a primary factor driving down the overall compliance rates of PTR and FCrDNS.

Overall, these findings suggest that while administrators tend to configure reverse DNS for addresses they clearly recognize as mail-sending hosts, broad SPF authorizations often include address space that is either unrelated to mail delivery or lacks sufficient reverse DNS configuration.

B. Implications for Sender Reputation and Abuse Detection

The findings of this study have direct implications for reputation systems and phishing or spam detection. The absence of PTR records or FCrDNS consistency is commonly treated as a suspicious signal and remains a useful component of sender assessment. However, our measurements demonstrate that a substantial portion of the SPF-indicated address space for likely legitimate domains lacks PTR or FCrDNS consistency. Notably, even for individually specified sender IP addresses, a lack of configuration was observed in over 15% of cases. Consequently, using the absence of reverse DNS as a standalone binary indicator of maliciousness carries a significant risk of misclassifying legitimate senders as malicious (false positives). Therefore, such indicators must be interpreted with caution within reputation frameworks.

C. Distribution Trends of Reverse DNS Configuration Rates in likely Legitimate Domains

Figure 1 illustrates the domain-level PTR and FCrDNS configuration rates after excluding domains that depend on major shared infrastructure providers. The results indicate that domains with 100% configuration rates for both PTR and FCrDNS represent the largest proportion. However, the overall proportion of domains achieving full configuration remains below 50% for both metrics, suggesting that high configuration rates are not yet universal. This lack of full compliance is not necessarily due to a complete absence of PTR or FCrDNS consistency; rather, it often stems from the inclusion of broad network prefixes in SPF records. Such over-authorization lowers the domain-wide configuration rate, resulting in a significant number of domains exhibiting intermediate setup rates.

D. Limitations

This study has several limitations. First, our analysis focused only on IPv4 addresses and did not cover IPv6 sender infrastructure. Second, the addresses extracted from SPF records represent potential sender addresses, not necessarily hosts that actually transmitted emails during the measurement period. Third, SPF policies containing broad network prefixes may include addresses that are operationally unrelated to outbound mail delivery. In future work, we plan to extend the analysis to IPv6, incorporate actual mail traffic observations, and investigate how PTR and FCrDNS deployment correlates with domain reputation, mail service providers, and phishing or spam activity. Such extensions will further clarify the practical role of reverse DNS in modern email security and deliverability.

VII. Conclusion

In this paper, we conducted a large-scale empirical analysis of reverse DNS deployment for SPF-indicated sender IPv4 addresses. Using domains from the Tranco Top 1M list, we extracted 20,964,277 potential sender IP addresses from SPF records and classified their PTR and FCrDNS configuration status through DNS measurements. Our results show that PTR records were configured for 41.1% of the analyzed addresses, while FCrDNS consistency was confirmed for only 23.0%. These findings indicate that a large portion of SPF-indicated sender address space does not satisfy FCrDNS consistency requirements, even among domains that are likely to be legitimately operated.

These results provide an empirical baseline for interpreting PTR and FCrDNS observations in email security analysis. Although the lack of PTR records or FCrDNS consistency can be a useful indicator in sender reputation systems and spam or phishing detection, our research shows that it should not be used as a standalone indicator of malicious behavior. Since many SPF-indicated addresses of likely legitimate domains also lack complete reverse DNS configuration, relying solely on this factor may increase false positives. Therefore, reverse DNS information should be combined with other authentication, reputation, and behavioral indicators.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers JP25K21182 and JP25K15109.

References

[1] APWG, “Phishing activity trends report,” 2025. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

[2] FBI, “Internet crime report,” 2025. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] Google, “Email sender guidelines,,” 2024. [Online]. Available: https://support.google.com/a/answer/81126?hl=en

[4] S. Kitterman, “Sender policy framework (spf) for authorizing use of domains in email, version 1,,” 2014, RFC7208.

[5] V. Pochat, T. Van Goethem, S. Tajalizadehkhoob, C. Huygens, and W. Joosen, “Tranco: A Resilient and Transparent Top-1M List for Web-Oriented Research,” in *Proceedings of the 2019 Network and Distributed System Security Symposium (NDSS)*, 2019.

[6] E. Z. M. Kucherawy, “Domain-based message authentication, reporting, and conformance (dmarc),,” 2015, RFC7489.

[7] A. Arouna, R. Fontein, B. Meijerink, I. Livadariu, and M. Jonker, “On the role of forward-confirmed reverse dns in e-mail authentication,” in *2025 9th Network Traffic Measurement and Analysis Conference (TMA)*, 2025, pp. 1–11.

[8] L. Izhikevich, G. Akiwate, B. Berger, S. Drakontaidis, A. Ascheman, P. Pearce, D. Adrian, and Z. Durumeric, “ZDNS: A fast DNS toolkit for internet measurement,” in *Proceedings of the 2022 ACM Internet Measurement Conference*, ser. IMC ’22, 2022, pp. 33–43.

[9] MaxMind, “Geolite2 free geolocation data,” 2025. [Online]. Available: https://www.maxmind.com/en/geolite-free-ip-geolocation-data