

CURRENT EMAIL ANTI-SPAM TECHNICAL SOLUTIONS

Introduction

Email SPAM is the most common type of SPAM and is currently combated through a variety of solutions on the technical side of combating SPAM. The key anti-SPAM solutions for email SPAM that are adapted by existing industrial products and practices are introduced in this article.

Mail Filters

The current mail filters can be classified as Non-Machine Learning (Non-ML) mail filters and Machine Learning (ML) mail filters. The Non-ML mail filters are designed to act based on manual settings to combat SPAM. They are not capable of self learning from different patterns of SPAM emails and also not capable of adapting to emerging SPAM characteristics. On the other hand, the ML mail filters are intelligent filters that learn from different patterns of SPAM emails and combat them accordingly. Hence, they are designed to adapt to emerging SPAM characteristics. Following are the major types of existing mail filters:

➤ **Black Listing/White Listing Mail Filters**

The black listing/white listing mail filters are classified as Non-ML filters. The black listing filters are based on a list (black list) of email addresses that are considered as sources for SPAM emails. Hence, emails sent from those addresses are filtered by the filtering system. White listing mail filters are based on a list (white list) of email addresses that are considered as sources for legitimate emails. Hence, only emails from those addresses are allowed to pass through and the rest are filtered by the filtering system. Both white lists and black lists can be manually configured or set for automatic configurations. In the manual configuration, the white-listed or black-listed senders are added manually by adding their email address to the list. In the automatic configurations setup, the senders are added to the white list/black list automatically if their addresses meet certain characteristics.

Benefits: The black listing/white listing mail filters are considered simple, fast and easy to implement.

Limitations: A main limitation of the black listing/white listing mail filters is that they can be easily fooled by spoofing the sender's email address.

➤ **Heuristics Mail Filters**

The heuristic mail filters are classified as Non-ML filters. They work based on predefined rules. The rules may be applied to the header of email messages as well as to the body of the messages. The rules that are applied to the email header identify certain predefined characteristics of SPAM email in the header fields such as, patterns of what may be invalid email addresses, dates, and subjects. Additionally, these rules may also be customized to include other header fields. The rules that are applied to the email body identify phrases of SPAM emails using "regular expressions". The regular expressions may be customized to include new expressions of evolving SPAM wordings. Emails are given scores based on the number of rules they match. If an email scores higher than a predefined threshold, the email will be classified as a SPAM email and filtered by the filtering system.

Benefits: The Heuristic mail filters are considered simple, highly accurate against the regular expression rules, and optimum in their speed of execution.

Limitations: The Heuristic mail filters do not have intelligent learning capabilities (they do not adapt to emerging SPAM characteristics), they require administrator interference to

update the rule sets or rule sets need to be downloaded on regular basis, and they may also generate high rates of false positives as the sensitivity is increased.

➤ **Embedded HTML Mail Filters**

The embedded HTML mail filters are classified as Non-ML filters. They are based on the Heuristic mail filters. They scan through emails to identify if the email contains any embedded HTML code. Many email clients support composing and displaying messages in HTML format. HTML content may contain links to retrieve content that is located on the web, such as images or websites that contain SPAMming content, scripts to indicate to SPAMmers that an email has been read and that the email account is active, and scripts to download malicious codes and/or scripts to execute malicious codes. As many of the email filters filter emails based on their content, SPAMmers tend to use such techniques to escape from them. The embedded HTML mail filter will block receiving/displaying emails that contain malicious HTML code. As such, Embedded HTML Mail Filters safeguard user machines from the malicious content that could be embedded in SPAM and legitimate messages. It could also protect the users' computers from becoming Zombie machines.

Benefits: The embedded HTML mail filters are considered very effective to block receiving or block displaying emails that contain embedded HTML code or web-scripts such as JavaScripts. As such, they protect the recipient's machine from SPAMming contents as well as from contents that may be considered malicious. Many email clients also provide an option to disable the display of email messages in HTML format.

Limitations: The embedded HTML mail filters may block receiving or block displaying legitimate emails such as emails from newsletters because the majority of newsletter emails are set to be displayed in HTML format or may contain links to retrieve images from the web.

➤ **Signatures Mail Filters**

The signature mail filters are classified as Non-ML filters. The filters are developed based on the mathematical concepts of "hash functions". Hash functions are designed to be highly resistant to collision by producing distinct outputs for their inputs. Signature mail filters maintain a list (database) of hash values for known SPAM emails. A signature mail filtering system operates as follows. It generates a hash for an incoming mail and compares it with existing hashes of known SPAM emails. Upon a successful match, the mail is classified as SPAM email and filtered. However, the filtering system does not have the capability to identify hashes for new SPAM emails. The hash list for SPAM emails need to be fed to the filtering system. The filtering system receives hash updates for new SPAM emails from a signature distribution server. The communications with the signature distribution server as well as storing of the hash list of SPAM emails requires high security measures.

Benefits: Based on high resistance of hash functions to collision, signature mail filters generates low rates of false positives.

Limitations: The signature mail filters do not have intelligent learning capabilities (they cannot identify hashes for new SPAM emails), they require administrator's interference to update the hash list of SPAM emails or the list needs to be fetched from a signature distribution server on a regular basis, and the filtering mechanism fails to detect pre-known SPAM emails if they are amended. Amendments to pre-known SPAM emails generate a different hash than the known one to the filtering system. Hence, the amended SPAM email will pass through the filtering system.

➤ **Bayesian Mail Filters**

The Bayesian mail filters are classified as ML filters. They are the only ML filters that are implemented at present. The Bayesian mail filters are based on calculating probabilities for a set of tokens. The tokens are defined as words of the natural language that are found in email content. The tokens are given probability scores based on their previous records of appearing in earlier detected SPAM emails. Email users can customize the filters to classify (filter) the

received mails based on their preferences. Therefore, Bayesian mail filters can be customized differently for different users. They can also adapt their rules based on feedback from users. Incoming emails are tokenized on arrival and each token is matched with its known record to calculate its probability. The probabilities of all tokens are combined based on the mathematical Bayes' rule. High probability indicates a higher possibility of an email to be a SPAM. Based on the combined probability value, SPAM emails are filtered. Bayesian mail filtering systems better suit client side setup than the server side due to the filter's customization advantage. Setting up Bayesian filtering systems only on the server side confines email users from benefiting from the filter's customization feature unless the feature is also facilitated on the server side.

Benefits: The Bayesian mail filters have intelligent learning capabilities (ML filters) as well as enhanced filtering capacities based on content analysis. They allow email users to customize the filters based on the type of SPAM the users may receive. Additionally, the Bayesian mail filters are considered highly accurate.

Limitations: The tokens in the Bayesian filters are formed of single words. Hence, combined words may pass from detection. Additionally, the filters lack the capability of analyzing consecutive words that form common SPAMming phrases in email contents, such as the phrase "special offer". Instead, each word is analyzed separately. Certain consecutive words and combined words are frequently noticed in SPAM emails. Failing to recognize such words limits the filtering mechanism from detecting these types of SPAM emails. However, there are some algorithms that exist currently which help in analyzing permutations of single words, consecutive words, and words appearing within a distance of one another.

➤ **Traffic Analysis Mail Filters**

The traffic analysis mail filters are classified as Non-ML filters. They use the log files of the SMTP mail server to detect anomalies in the email traffic. Email traffic of SPAM nature is characterized by email arrival process (if the email is relayed), email size, number of recipients per email (if the email was flooded), and popularity and temporal locality among recipients. Based on anomalies in the email traffic analysis, SPAM emails are detected and filtered.

Benefits: The traffic Analysis mail filters are considered relatively complex. However, their mechanism proposes enhanced and fast mail filtering comparatively with actual analysis of email contents because they only analyze the SMTP logs.

Limitations: The traffic Analysis mail filters do not have intelligent learning capabilities (they do not adapt to emerging SPAM characteristics). As of now, it is not possible for the filters to decide which of the characterizing attributes of email traffic are the most appropriate for a particular stream of email traffic.

Source Authentication

Authenticating the source of an email/the email sender increases the trustworthiness of received emails and puts unknown emails under suspicion of being SPAM. A common practice of SPAMmers is to falsify their identity to harden tracking the source of their SPAM emails. Apart from using mail relays, open proxies and zombie computers, SPAMmers may also use advanced techniques to forge the email headers. As such, different schemes have been introduced for email source authentication. The following are the major schemes that are implemented in existing industrial products and practices.

➤ **Sender Policy Framework / Sender ID Framework**

The Sender Policy Framework (SPF)/Sender ID is an extension to the Simple Mail Transfer Protocol (SMTP) to enable email source authentication. SPF/Sender ID allows mail servers to identify fake addresses in the "from/sender" field of the mail header by protecting the

“Return-path”. Faking the “from/sender” field of the mail header is commonly practiced by SPAMmers to avoid revealing their real identity and perhaps to send their SPAM emails by the names of known senders. This is done by exploiting a shortcoming in the normal implementation of the SMTP specification. The SMTP specification allows the mail servers to send emails without strongly stipulating their identities. SPF/Sender ID addressed this shortcoming by allowing owners of internet domains to use their DNS records (TXT record) to specify the mail servers of their domain that are authorized to transmit emails. Specifically, the records contain the IP addresses of the legitimate mail servers and their corresponding domain names that will be specified in the “Return-path”.

SPAMmers may fake the “from/sender” field but cannot fake the “Return-path” field as it is secured by the SPF protocol. As such, recipient mail servers can query the DNS server of the source mail server’s domain and compare the “Return-path” and the specified IP address of the source mail server with the ones registered in the DNS record. A PASS will result from a valid match and a FAIL will result from mismatches. Email servers that fail the SPF/Sender ID validation can be considered SPAMming sources and blocked. Another form of scam can be practiced by SPAMmers if the SPF/Sender ID protocol is not in use. They may forge the “Return-path” field and place addresses of other people so that they may annoy them with bounced emails, unsolicited replies and error messages. However, using the SPF/Sender ID will not allow such problems to occur in the first place.

The naming of the SPF is based on its operational mechanism as it sets policies for outgoing mail in an internet domain. Although the Sender ID operates similarly to the SPF, it is considered as a different protocol as both differ in the implementation aspects. Sender ID and SPF differ in how they validate and what layer of the email system they are concerned with. The sender ID is slightly incompatible with existing specifications.

Benefits: The SPF/Sender ID lay out an effective authentication scheme for validating source mail servers by introducing enhancements to the SMTP protocol. As such, zombie machines, open relays and open proxies can be blocked. The blocking of emails is a feature of the mail servers (MTAs) that implement SPF/Sender ID. Thus, they do not require the setup of additional hardware or software. The SPF/Sender ID also provides a secure approach of combating SPAM emails by not receiving (blocking) emails from SPAMming mail servers in the first place. The SPF/Sender ID can be used as a premail filtering technique.

Limitations: Although the SPF/Sender ID has been implemented and used among various email exchangers, it still remains as an internet draft with regards to RFC standardization. As such, the SPF/Sender ID protocol is not mandatory to be implemented and followed by email servers. Some email users may want to specify a different return address for their emails. As of now, this is not possible with the SPF/Sender ID because it strictly binds the sender’s entity in the “Return-path” field.

Sender ID might consider forwarded email as SPAM if the forwarded IP address does not match the originator’s domain name. Since the Sender ID slightly contradicts the existing specifications, recommendations have been made to discontinue it as an internet draft until the inconsistency is resolved. However, until now it still remains under consideration for RFC standardization and it is also implemented in various products.

➤ **Domain Key Identified Internet Mail**

The DomainKey Identified Internet Mail (DKIM) enables email source authentication independently from the SMTP mail protocol. It allows for tracking forged email sources by verifying the domain of a mail sender and verifying the email message integrity. This is achieved by “digital signatures” which is a well known function of “public key cryptography”. Each domain will have a pair of private and public keys for signing. The signing operation is done by the sender’s mail server (MTA) using the sending domain’s private key and the verification is done by the receiver’s mail server (MTA) using the sending domain’s public key. Both, the sender’s mail server and the receiver’s mail server, need to

implement the DKIM. The DKIM requires that for each domain, the domain's DNS record should publish the domain's public key beside other attributes, and that the mail servers of a domain will confidentially house the domain's private key. The mechanism works as follows. The sender's mail server will digitally sign the content of the outgoing email message using SHA-1 as a hash function and RSA as the cryptographic algorithm and attach the signature (DomainKey Signature) to the mail header. The sender's mail server will then send out the mail. Upon receiving the mail, the receiver's mail server will extract the domain name from the "from/sender" header field and inquire the DNS server of the sender's domain to retrieve its public key. If the public key was not found then the receiver's mail server can judge that the source of the email was forged, that the mail may be a SPAM, and that the email should be discarded. However, on successful retrieval of the public key, the receiver's mail server will use the key to verify the digital signature. Upon passing the verification, the receiver's mail server will trust the email source as a legitimate mail server. Upon failing the verification, the receiver's mail server may consider the source of the mail as a SPAMming source and discard the email. Further, passing the verification process will ensure that the content of the email message was not tampered with.

Benefits: The DKIM layouts an effective authentication scheme for validating the legitimacy of an email's source and ensuring the email message's integrity. Using DKIM, discarding emails is a feature of the mail servers. Thus, email servers do not require the setup of additional anti-SPAM hardware or software. The DKIM also provides a secure approach of combating SPAM emails by discarding SPAM emails at first place. As such, it can be used as a premail filtering technique. The DKIM specification is based on optional RFC 2822 headers and DNS records. Therefore, it is backwards compatible with the existing email protocols.

Limitations: The DKIM does not include the email header in the DomainKey Signature. Therefore, forging the "Return-path" is not detected. As such, SPAMmers may forge the "Return-path" field and place addresses of other people so that they may annoy them with bounced emails, unsolicited replies and error messages. Additionally, PKI is an expensive technology and thus adopting this technique may not be cost effective.

Challenges and Responses

The challenge-response systems are based on human interactions with the system to decide on SPAM emails. They validate that the sender of an email is a human entity and not an automated SPAMming system (SPAMbot). The systems run on the mail server to intercept incoming emails that are suspected of being SPAM. They then send a challenge to the sender for him to respond back. The underlying concept is that SPAMmers will not respond back given that they send bulk emails. Further, SPAMmers will never receive a challenge if they falsify their email address. Based on this concept, emails are recognized as SPAM and discarded/filtered if a response is not received for a challenge. The challenges and responses are exchanged in the form of emails.

Benefits: The challenge-response systems are very effective to combat SPAM emails if the SPAM emails are sent by SPAM bots or sent with a false identity.

Limitations: The challenge-response systems do not have intelligent learning capabilities (they do not adapt to emerging SPAM characteristics). Additionally, they are found inconvenient for email users as the users are required to respond to challenges for some of the emails sent.

Reverse DNS Lookups

The reverse Domain Name System (DNS) lookups may help identify SPAM emails and block incoming mails from SPAMming mail servers. The reverse Domain Name System (rDNS) performs the reverse function of the DNS. The DNS primarily determine the IP address(es) associated to a given host name which is known as “forward DNS lookup”. The rDNS records determine the hostname(s) associated to a given IP address which is known as “reverse DNS lookup”¹. The DNS records also list mail servers for each domain. The Mail Transfer Agents (MTAs) of mail servers use this information to deliver emails correctly between mail servers. Based on these fundamental concepts, MTAs perform reverse DNS lookups to detect SPAM emails by checking:

1. If the results of forward DNS lookups matches the reverse DNS lookups at some domain name and IP address entry for a source mail server. This technique is known as Forward Confirmed Reverse DNS (FCrDNS). The FCrDNS validates that there is a level of legitimate relationship between the owner of a domain and the owner of the IP address. This binding is only sufficient to know that source email servers are not zombie computers or the source domains are not forged which are popular techniques used by the SPAMmers.
2. The domain names for source email servers in the rDNS records to verify if they are likely from dialup users, dynamically assigned addresses, or home-based broadband internet users. It is assumed that a bulk amount of SPAM emails are originated from mail servers set within the mentioned categories.

Conducting reverse DNS lookup is almost a standard feature of mail servers. MTAs are usually designed to perform the two types of checks and block incoming emails accordingly from source mail servers.

Benefits: Detecting SPAM emails using reverse DNS lookups is considerably fast and optimized. The blocking of emails is a feature of the mail servers (MTAs). Thus, it does not require the setup of additional hardware or software. It also provides a secure approach of combating SPAM emails by not receiving (blocking) emails from SPAMming mail servers in the first place. The FCrDNS technique has proven to be effective in blocking static zombie machines that are used as SPAMming mail servers. The technique can be used as a premail filtering technique. The OECD recommended the use of it to combat SPAM in the OECD workshop on SPAM.

Limitations: The checks performed by the MTA are limited as explained in the above methods. Therefore, advanced SPAMming techniques and SPAM emails are not blocked. A major hindrance to the success of this technique is IP spoofing. Although IP spoofing is complex and not cost effective for SPAMmers, it is possible that SPAMmers may use IP spoofing to fake their sent IP address. Additionally, the given methods are not standard implementations of the email protocols (RFCs) although conducting reverse DNS lookups is almost a standard feature of mail servers at present. As a result, they may not necessarily be implemented by all MTAs. Further, the reverse DNS lookups are not specifically purposed to address the email SPAM problem. They are utilized as an application to combat email SPAM. Also, DNS lookups may generate a high level of false positives since some inexperienced system administrators may not setup reverse DNS records. Some system administrators assign multiple domains to the same IP address which is legitimate and widely adopted.

¹ It is possible to have a single IP address mapped to multiple host names for virtual hosting purposes, and it is also possible to have multiple IP addresses mapped to a single host name for fault tolerance and load balancing purposes.

DNSBLs

DNSBLs (DNS Black Lists) are records that primarily contain entries of IP addresses and corresponding domain names of mail servers that are considered to be source of SPAM emails on the internet. DNSBLs are published on a DNS server and their format is based on the DNS record format. When receiving emails from a mail server, the recipient mail server (MTA) queries a DNS server that hosts a DNSBL to resolve the source mail server's IP address. The DNS server searches through the DNSBL for a domain name that maps to the queried IP address. If a domain name is found, the DNS server responds back with it and the source mail server is considered to be a well-known source of SPAM emails. If a domain name is not found, the DNS server responds back with "NXDOMAIN" value which means that "no domain was found". Accordingly, the recipient mail server decides on SPAM emails and blocks emails from the source mail server. DNSBLs are proven effective to block SPAM emails from open mail relays, open proxies, known SPAMmers, etc. There are well known DNSBLs available specific to list open mail relays and open proxies which can be used by mail servers before accepting mails from unknown email servers.

Benefits: Detecting SPAM emails using DNSBL is considerably fast and optimized. The blocking of emails is a feature of the mail servers (MTAs). Thus, it does not require the setup of additional hardware or software. It also provides a secure approach of combating SPAM emails by not receiving (blocking) emails from SPAMming mail servers in the first place. The technique has proven to be effective in blocking zombie machines that are used as SPAMming mail servers. The technique can be used as a premail filtering technique.

Limitations: The type of check covered by the DNSBL technique is considered primitive if compared to advanced SPAMming techniques. SPAMmers may find a work around to spread their SPAM emails by setting up intermediate zombie machines (mail servers) between the blacklisted SPAMming mail server and the recipient mail server. Besides, dynamic IP addresses are hard to list every time and SPAMmers can always set up new SPAMming mail servers. A major hindrance to the success of this technique is IP spoofing. Although IP spoofing is complex and costly for SPAMmers, it is possible that SPAMmers may use IP spoofing to fake their sent IP address. The DNSBLs are not self learners. Their records need to be manually updated with new entries by an authorized body. Choosing a trusted DNSBL may be challenging in some cases as many DNSBLs are available in public and claim to be trustworthy. SPAMmers may publish fake DNSBLs to mislead the mail servers. Validating the DNSBL's publisher may require complex authentication mechanisms. Additionally, the DNS server and the DNSBL require high levels of security measures to avoid DoS attacks, manipulations, and falsifications.

URL Lookups

The URL lookups may help identify SPAM emails containing links to websites that are used by SPAMmers to place unsolicited contents. In an effort to bypass email filters, SPAMmers tend to host a website on which they place their unsolicited content. They then circulate the URL through SPAM emails. Typically, a service provider will publish a list of domain names for the websites that contain SPAM contents. Upon receiving an email with a URL, the anti-SPAM solution will extract the URL and perform a query to an online copy of the list or check with a local copy to identify if the URL is referring to a website of SPAM nature. The SPAM email will be blocked upon matching the URL's domain with a listed domain in the list.

Benefits: The URL lookups technique is considered effective to block emails that may contain links to websites of SPAM nature. At present, it is the only mechanism to validate the legitimacy of links within emails.

Limitations: The URL lookups technique is limited to identify emails that contain links to websites of SPAM nature. Other types of SPAM emails are beyond the focus of this technique. The lists containing the websites of SPAM nature are not self learners. They need to be manually updated with new entries by an authorized body. Unless detected by a human and published in the list, a link to a website of SPAM nature will never be detected. Choosing a trusted service provider that publishes the list may be challenging in some cases. SPAMmers may publish fake lists to mislead URL lookups. Additionally, validating the publisher may require complex authentication mechanisms. Needless to say that this approach might generate some false positives by blocking emails that advise against visiting a dangerous website.

Grey Listing Mail Rejection

Grey listing mail rejection refers to a mechanism that returns back emails which are received from unrecognized mail servers. The underlying assumption is based on the RFC specification that a legitimate mail server will attempt to connect later on to deliver rejected emails. It is anticipated that SPAMming mail servers will not follow the specification and resend their emails since they transmit bulk emails. However, most SPAMming mail servers that attempt to retransmit returned emails are listed in popular DNSBLs. Typically, the recipient mail server (MTA) records the IP address of the source mail server, the sender's email address and the recipient's email address. The MTA checks the record with its internal database. If the record is not found, the recipient mail server rejects the email. The recipient mail server then waits for a period of time for the source mail server to resend the rejected email. Upon expiration of the period and not receiving the rejected email, the recipient email may add the source mail server as SPAMming source. However, in all cases unrecognized emails are rejected in the first place. The SPAMming mail servers/SPAM bots will generally not attempt to resend the rejected emails. Hence, the method is found effective in blocking SPAMming mail servers.

Benefits: Detecting SPAM emails using grey listing mail rejection is fast, simple and optimized. It utilizes the standard specification of the mail protocols. The blocking of emails is a feature of the mail servers (MTAs). Thus, it does not require the setup of additional hardware or software. It also provides a secure approach of combating SPAM emails by not receiving (rejecting) emails from SPAMming mail servers in the first place. The technique has proven to be effective in rejecting zombie machines that are used as SPAMming mail servers. The technique can be used as a premail filtering technique.

Limitations: The grey listing mail rejection cannot be considered as a comprehensive anti-SPAM solution. Despite its effectiveness, it can cause major inconveniences for emails that require a prompt response. An example can be of websites that require user responses through email to complete their web registrations. The technique may hinder the users from completing their registration for some time. Another major inconvenience may occur if the period of waiting time given to the returned emails is not followed/not recognized by the source mail server. In such case, the mail will be sent after the expiration of the period. Thus, the mail will not reach the recipient. Consequently, the recipient mail server may consider the source mail server a SPAMmer and block it.

Disposable Email Addresses

Disposable Email Addresses (DEAs) are mainly a service provided by DEA service providers. DEAs are very effective in controlling SPAM. The underlying concept is as follows. The user can have many temporary email addresses (DEAs) that are linked to one or more original email addresses. Typically, the user can have a DEA for a group of contacts, or a DEA for each contact (ex. SingleContactName@User.DEAServiceProviderName.Com). The user publicizes the DEAs while keeping the original email addresses confidential. The DEAs forward the incoming emails to the user's original email address(es). In case a DEA is attacked by SPAM emails, or the user is no longer interested in receiving emails from the DEA, the user can cancel it out. If the DEA is set on single contact basis, the user can further detect the source of SPAM and report a SPAM abuse. Additionally, if the user wants to change a DEA for a legitimate contact, he/she only needs to update the contact with its new DEA.

Benefits: The DEA mechanism for combating SPAM emails is simple and effective. As explained, DEAs that are attacked by SPAMmers can be cancelled out, forwarded to a "junk email" folder or to the "trash". Further, a report for abuse can be submitted for single contact basis DEAs. The DEA mechanism for receiving email ensures high levels of security and protects the user's original email from compromise. The DEA enables better management of user's contacts. If the DEA is changed for a single contact, the user only needs to update the contact with the new DEA. Furthermore, if the user's original address is changed, the user only needs to update the DEA service provider with the user's new email address without bothering about informing all of his/her contacts.

Limitations: When using DEAs for contacts, the user may need to maintain a list of the contacts and their respective DEAs. Managing the list for large number of contacts may be a little troublesome. As the trusted DEA service providers do not offer their services for free, some users may find it irrational to pay for a service that mainly enhances a free service (email service). In many cases, users may want to use DEAs to register and subscribe to various online/offline services. Some of such services require users to provide them with real (official) emails to accept their registration. In such cases DEAs are not helpful as the service providers want to have the real emails of their subscribers for a better level of identity validation.