Disposable email address

Disposable email addressing, also known as **DEA** or **dark mail**, refers to an approach where a unique email address is used for every contact, entity, or for limited times or numbers of uses. The benefit is that if anyone compromises the address or utilises it in connection with email abuse, the address owner can easily cancel (or "dispose" of) it without affecting any of their other contacts.

Contents

Uses

Advantages over traditional email

Using "sub-addressing"

Multiple email aliases

Concerns

Restrictions by site administrators

See also

References

Uses

Disposable email addressing sets up a different, unique email address for every sender/recipient combination. It operates most usefully in scenarios where someone may sell or release an email address to spam lists or to other unscrupulous entities. The most common situations of this type involve online registration for sites offering discussion groups, bulletin boards, chat rooms, online shopping, and file hosting services. In a time when email spam has become an everyday nuisance, and when identity theft threatens, DEAs can serve as a convenient tool for protecting Internet users.[1]

Disposable email addresses can be cancelled if someone starts to use the address in a manner that was not intended by the creator. Examples are the accidental release of an email to a spam list, or if the address was procured by spammers. Alternatively, the user may simply decide not to receive further correspondence from the sender. Whatever the cause, DEA allows the address owner to take unilateral action by simply cancelling the address in question. Later, the owner can determine whether to update the recipient or not.

Disposable email addresses typically forward to one or more real email mailboxes where the owner receives and reads messages. The contact with whom a DEA is shared never learns the real email address of the user. If a database manages the DEA, it can also quickly identify the expected sender of each message by retrieving the associated contact name of each unique DEA. Used properly, DEA can also help identify which recipients handle email addresses in a careless or illegitimate manner. Moreover, it can serve as a good tool for spotting fake messages or phishers.

Advantages over traditional email

Ideally, owners share a DEA once with each contact/entity. Thus, if the DEA should ever change, only one entity needs to be updated. By comparison, the traditional practice of giving the same email address to multiple recipients means that if that address subsequently changes, many legitimate recipients will need to receive notification of the change and to update their records — a potentially tedious process.

Additionally, because access has been narrowed down to one contact, that entity then becomes the most likely point of compromise for any spam that account receives (see "filtering" below for exceptions). This allows users to determine firsthand the trustworthiness of the people with whom they share their DEAs. "Safe" DEAs that have not been abused can be forwarded to a real email account, while messages sent to "compromised" DEAs can be routed to a special folder, sent to the trash, held for spam filtering, or returned as undeliverable if the DEA is deleted outright.

Further, because DEAs serve as a layer of indirection between the sender and recipient, if the DEA user's actual email address changes, for instance because of moving from a university address to a local ISP, then the user need only update the DEA service provider about the change, and all outstanding DEAs will continue to function without updating.

Using "sub-addressing"

A number of email systems support "sub-addressing" (also known as "plus" or "tagged" addressing)[2][3][4] where a tag can be appended to the "local part" of an email address — the part to the left of the "@" — but with the modified address being an alias to the unmodified address. For example, the address joeuser+tag@example.com denotes the same delivery address as joeuser@example.com. The text of the tag may be used to apply filtering, or to create single-use addresses.

If available, this feature can allow users to create their own disposable addresses.[5][6]

Multiple email aliases

Another approach is to register one main and many auxiliary email addresses, which will forward all mail to the main address, *i.e.*, the auxiliaries are used as aliases of the main address. The advantage of this approach is that the user can easily detect which auxiliary email is 'leaking' with spam and block or dispose it.

Some services require additional time to set up forwarding, but others allow to create new addresses "on the fly" without registering them with the service in advance. However, this method allows storage and access of all emails from a single main account, although to manage forwarding for some services the user has to remember the password for each alias.

A variation is to use a catch-all address, then forward to the real mailbox using wildcards. Many mail servers allow the use of an asterisk (*), meaning "any number of characters". This makes the whitelist automatic and only requires the administrator to update the blacklist occasionally. In effect, the user has one address, but it contains wild cards, *e.g.*, "me.*@my.domain"', which will match any incoming address that starts with "me." and ends with "@my.domain". This is very similar to the "+" notation, but may be even less obvious, since the address appears to be completely normal.

Concerns

Restrictions by site administrators

Many forum and wiki administrators dislike DEAs because they obfuscate the identity of the members and make maintaining member control difficult. As an example, Internet trolls, vandals and other users that may have been banned may use throwaway email addresses to get around the ban.[7] Using a DEA provider only makes this easier; the same convenience with which a person may create a DEA to filter spam also applies to trolls.[8] Website operators expecting to generate revenue by selling the user email addresses they gather may choose to ban DEAs as well, due to the low market value of such addresses. There are several free lists available to help detect DEA domains, as well as managed services.

Banning DEAs might not be as effective at deterring undesirable users. More effective techniques for controlling undesirables without inconveniences to legitimate DEA users might include: recognizing legitimate DEAs for what they are (they usually have a proper domain and a fixed prefix or suffix), distinguishing them from short-lived, random throwaway address patterns or domains used by undesirables, wildcard banning.

As with any kind of threat and defence measures, no attempts to use or thwart DEAs are foolproof — any filtering method is bound to result in some false positives (legitimate users getting banned), and some false negatives (undesirables getting through, and legitimate users managing to come up with a DEA pattern getting around limitations imposed by site administrators). This is because the email address may be partly or fully defined by the user, made to appear as "permanent"-looking as needed, or made to avoid a particular pattern, defeating any filtering because for all intents and purposes it is not different from a permanent one, despite being limited to one purpose.

Caught in the crossfire between Internet undesirables and administrative and user attempts to deal with them, DEA providers have trouble presenting a total solution. A user may find it necessary to come up with a conventional-looking email address (or create a separate mailbox in the worst case) to a public/commercial entity if required. There is always uncertainty about the trustworthiness and reputation of the site administrators, the availability of options to hide email addresses, the existence/enforcement of an acceptable privacy policy and the chance that the site may one day be compromised or transferred to new owners. Even the largest and otherwise reputable companies have been compromised or resorted to sending spam or giving away emails to third parties. A human correspondent's computer or mailbox may be compromised by malware and his address book can be stolen and sold to spammers.

See also

- Guerrilla Mail
- TrashMail

References

1. "Disposable e-mail addresses foil marketing plans" (http://www.networkworld.com/newsletters/web/2006/1204web1.html). Network World. 2006-12-04. Retrieved 2007-02-02.
2. "Using an address alias" (https://mail.google.com/support/bin/answer.py?hl=en&answer=12096). *google.com*.
3. "Disposable addresses in Yahoo Mail — Yahoo Help — SLN3523" (https://help.yahoo.com/kb/SLN3523.html). help.yahoo.com.
4. "Plus addressing and subdomain addressing" (https://www.fastmail.com/help/receive/addressing.html). *fastmail.fm*.
5. "Yopmail — Disposable Email Account — Temporary Email" (https://www.yopmail.info/). *www.yopmail.info*. Retrieved 2017-05-28.
6. "Disposable E-mail Addresses" (https://www.pcmag.com/article2/0,1759,990137,00.asp). PC Magazine. 2004-03-22. Retrieved 2007-02-06.

7. "Successful Forum Tip #3 — Troll Prevention and Extermination" (http://www.lockergnome.com/nexus/net/2004/08/09/successful-forums-tip-3-troll-prevention-and-extermination/). 2004-08-09. Retrieved 2007-02-02.
8. "Add New Ban" (http://docs.simplemachines.org/index.php?topic=145). *SMF 1.1 Online Manual*. Simple Machines LLC. Retrieved 2007-02-02.
