

Credibility Brief: Goodmail CertifiedEmail

Shaun Kane for the Credibility Commons
June 6, 2006

Overview

Goodmail CertifiedEmail [1] is a commercial email verification service. Its purpose is to allow large organizations to send authenticated bulk email messages to consenting recipients. Goodmail messages are digitally signed so that the recipient can verify that the sender's identity. Goodmail believes that this approach may help protect users against email fraud and so-called "phishing" attacks.

AOL and Yahoo! have recently agreed to provide Goodmail service for their customers. This has created some controversy among some Internet users and organizations. Goodmail has been described by some as an "email tax" that could have a negative effect on how email is used on the Internet.

In this document we briefly describe the Goodmail system, list the proposed benefits of Goodmail, and outline the concerns raised by Internet users and consumer protection organizations. We also describe several alternative systems intended to reduce phishing attacks.

How Goodmail works

The Goodmail service acts as a trusted intermediary between email senders and receivers. Goodmail is targeted primarily at companies that wish to send commercial email to consumers who have agreed to receive such email. Companies that wish to send verified email must first register themselves with Goodmail Systems. Goodmail verifies the reputability of the sender based upon their business and email history. Senders then pay approximately one quarter of one cent to send each verified message. Users pay nothing for the service.

The Goodmail architecture provides end-to-end verifiability for email messages. Messages are sent through the Goodmail service by the following process:

1. The sender requests a digital signature key from the Goodmail servers.
2. Goodmail's servers verify that the sender is registered with Goodmail and provide a signature key.
3. The message is signed using the Goodmail key and is sent through normal email channels.

4. The message is delivered to the recipient. If the recipient's ISP supports Goodmail, the ISP will verify the message key with Goodmail's servers.

Verified message may bypass the user's junk email filters and may be marked with a special "verified" icon. Email sent through Goodmail to non-partnered ISPs will be sent as regular email. Email that is not sent through Goodmail will be handled normally, so it is still possible to send unverified and free email to Goodmail users. Currently, AOL and Yahoo! are the only major ISPs that support the Goodmail service.

Benefits for end users

Goodmail Systems states that their system helps protect users from e-mail fraud and phishing attacks. The service provides the following benefits to end users [1]:

1. Goodmail verifies the credibility of registered senders. As part of the certification process, Goodmail examines the sender's business address, business history, and email history. Senders with unverifiable contact information or a history of sending unsolicited email will not be certified and cannot send messages through Goodmail. Goodmail currently certifies businesses in the US and Canada only.
2. Goodmail provides a secure audit trail between email senders and recipients. Senders digitally sign their messages to prove their identity. The Goodmail server verifies this signature at the receiving ISP. Theoretically, it should be difficult to spoof messages from the Goodmail service.
3. Goodmail makes it easier for users to identify fraudulent messages. Email programs may display a special "verified" icon to indicate that a message has been verified by Goodmail. As a result, users may learn not to trust important messages that have not been sent through Goodmail. Users do not need to significantly change their behaviors to use Goodmail.

Community response to Goodmail

Since its announcement, the Goodmail service has received criticism from a number of organizations including the Electronic Frontier Foundation (EFF), the AFL-CIO and the Democratic National Committee [2, 3]. Critics of Goodmail have made a number of claims regarding the effectiveness and fairness of the system:

1. Goodmail creates an "email tax". Although it is still possible to send unverified email to users of Goodmail-partnered ISPs, many are concerned that Goodmail's introduction will start a transition from free to pay-only email service. Critics are also concerned that pay-based email systems favor commercial organizations over non-profit organizations. Goodmail currently provides reduced rates for non-profit organizations.

2. Goodmail and its partner ISPs may filter messages inappropriately. AOL was recently charged with blocking email messages that included links to DearAOL.com, a Goodmail protest site [4]. AOL has stated that these messages were blocked due to a technical error, although the event generated negative publicity for both AOL and Goodmail.
3. Goodmail may create more, rather than less, junk email. The Goodmail system does not prevent unverified junk email. In addition, Goodmail provides a method to send additional commercial email that is guaranteed to bypass junk email filters. The CEO of Goodmail has stated that the Goodmail system is not designed to reduce junk email [5].
4. Goodmail is a proprietary system and depends upon the cooperation of several proprietary services to function. In order for messages to be securely verified, users must use Goodmail-compatible email clients and ISPs, and must interact with businesses that use Goodmail. Without an open standard, the development of competing systems may cause incompatibility issues for users.

Alternatives to Goodmail

Although Goodmail has received a large amount of attention, it is not the only service that attempts to address the issue of email credibility. A number of alternative systems have been developed to provide verification of email senders and message content.

- *Commercial email accreditation services.* A number of private companies have developed third-party email verification services that are similar to Goodmail, such as Habeas [6] and Return Path [7]. These organizations verify the credibility of subscribing organizations and publish lists of credible senders.
- *Public-key digital signatures.* Many of the systems described here use public-key encryption and authentication to transmit information. Public-key encryption technologies allow users to send encrypted and digitally signed email after users exchange encryption keys. However, users are usually required to set up their own email software and to first exchange keys with whomever they wish to contact. Companies such as PGP [8] provide desktop applications that support public key encryption and digital signatures for email.
- *Open authentication standards.* A number of open standards have been proposed that would allow ISPs to securely authenticate email messages. These standards allow email servers at the receiver's ISP to verify the authenticity of email themselves, rather than relying on a third party. Microsoft's Sender ID Framework enables ISPs to verify the source of a message using public domain name servers [9]. A similar system developed by Yahoo!, DomainKeys, uses digital signatures to verify that messages have not been forged or altered during transmission [10].

- *Whitelists.* Email whitelists are lists of trusted senders and domains. ISPs may maintain whitelists and may allow email from these senders to pass through email filters. ISP whitelists are usually invisible to the end user. AOL maintains a large email whitelist [11]. Bulk email senders may apply to be added to the AOL whitelist, and may be promoted to an enhanced whitelist after a period of good behavior. Some ISPs also maintain *blacklists* of confirmed email abusers.
- *Email applications.* Applications on the user's computer can also be used to help manage fraudulent email. For example, email software can highlight features commonly found in fraudulent email and alert the user to their presence. Yahoo! Mail currently provides a suite of tools to help users identify and protect themselves from fraudulent and junk email [12].

What good is Goodmail?

Goodmail's primary purpose is to allow organizations to send verified email to consumers. Goodmail Systems has stated publicly that their service is not intended not reduce junk email. Given the commercial and proprietary nature of the service, it is unlikely that the system will provide a general solution to email credibility. At the same time, it is unlikely that the pay-to-send model used by Goodmail will become standard in the near future, as some have feared.

The creation of a widely supported email verification service is generally beneficial to Internet users, and may be helpful in protecting users of Goodmail-partnered ISPs from some types of fraudulent email. However, the costs associated with using Goodmail may also limit adoption of the Goodmail service by organizations and ISPs. The proprietary and commercial nature of Goodmail has also caused some users and organizations to be distrustful of the system. More open systems such as Yahoo's DomainKeys and Microsoft's Sender ID Framework manage to address these concerns, and may be more successful in the future.

Finally, it is important to note that no single system can completely solve the problems of email credibility. Goodmail and other systems like it will be helpful for some users and organizations, and may protect against certain types of email fraud. However, it is unlikely that a single system can protect users from all types of fraud. The best defense against email fraud will come from a combination of different types of tools and through raising users' awareness of Internet credibility issues.

References

- [1] Goodmail Systems. Web site: <http://www.goodmailsystems.com/certifiedmail/>
- [2] Stop AOL's Email Tax! Web site: <http://www2.dearaol.com/letter/>
- [3] Cohn, C. (2006, February 8). *AOL, Yahoo and Goodmail: Taxing your email for fun and profit*. Retrieved June 6, 2006 from EFF:DeepLinks. Web site: <http://www.eff.org/deeplinks/archives/004398.php>
- [4] Olsen, S. (2006, April 13). *AOL charged with blocking opponents' email*. Retrieved June 6, 2006 from ZDNet. Web site: http://news.zdnet.com/2100-9595_22-6061089.html
- [5] Spam Daily News (2006, April 11). *Goodmail: CertifiedEmail will not reduce spam*. Retrieved June 6, 2006 from Spam Daily News. Web site: http://www.spamdailynews.com/publish/Goodmail_CertifiedEmail_will_not_reduce_spam.asp
- [6] Habeas: The Email Trust Authority. Web site: <http://www.habeas.com/>
- [7] Return Path. Web site: <http://www.returnpath.biz/>
- [8] PGP Corporation. Web site: <http://pgp.com/>
- [9] Microsoft Corporation. (2005, February 17). *Sender ID Framework overview: Verification system aims to reduce spam and increase safety online*. Retrieved June 6, 2006 from Microsoft Safety. Web site: <http://www.microsoft.com/mscorp/safety/technologies/senderid/overview.mspx>
- [10] Yahoo! Inc. (n.d.). *DomainKeys: Proving and protecting email sender identity*. Retrieved June 6, 2006 from Yahoo! Anti-Spam Resource Center. Web site: <http://antispam.yahoo.com/domainkeys/>
- [11] America Online, Inc. (2004). *Whitelist information*. Retrieved June 6, 2006 from AOL Postmaster. Web site: <http://postmaster.aol.com/whitelist/>
- [12] Yahoo! Inc. (n.d.). *Yahoo! Mail anti-spam features*. Retrieved June 6, 2006 from Yahoo! Anti-Spam Resource Center. Web site: <http://antispam.yahoo.com/tools/>