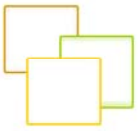
eMill

PROFESSIONAL EMAILING SOLUTION



WHITE PAPER

HOW TO OPTIMIZE EMAIL DELIVERABILITY?

Deliverability is the biggest challenge marketers are facing with the email channel. Whatever is the solution you choose (in-house or ESP), you will have to follow specific guidelines to avoid your email being flagged as a Spam by filtering tools or by your own subscribers.

You will find below a detailed list of the different issues you should be aware of. Note that the requirements are not the same if you send a monthly newsletter to 100 subscribers or if you are managing large scale email marketing campaigns.

I. Avoid that subscribers complain about your emails

Follow the rules

- **Advice 1**: Follow the anti-spam and local privacy laws
- **Advice 2**: Ask permission before subscribing someone

4 subscribe processes are usually implemented:

Opt-out: When someone fills a form, he is automatically subscribed. This process is illegal in most countries.

Opt-in: When someone fills a form, he has to check a button ("I want to receive newsletters") to subscribe. By using this process, you take the risk to have invalid email addresses or to have people subscribed by error.

Notice

eMill includes all the tools to manage automatically subscribe requests using the double opt-in process. Read the "*Managing a subscribers list with eMill*" tutorial to learn more about it.

Confirmed Opt-in: When someone fills a form, he has to check a button ("I want to receive newsletters") to subscribe and he receives an email confirming his subscription. This process allows you to remove invalid addresses but people can still be subscribed by error.

Double Opt-in: When someone fills a form, he has to check a button ("I want to receive newsletters") to subscribe and he receives an email asking him to click a link or to reply to the email in order to confirm his subscription. This process allows you to have a 100% clean list but the number of subscribers will be lower than other processes.

Use clean and updated list

- **Advice 1**: Check what your data sources are or who your data partners are

Your emails are more likely to be reported as spam if you rent a list than if you build a list by yourself through a subscription form or by using traditional marketing techniques (games, contests or draws).

- **Advice 2**: Check the age of your list records

If user records & email addresses are quite old, you should check address validity (features available with eMill) and send a first campaign asking receivers to confirm that they really want to receive your emails.

- **Advice 3**: Manage bounces

Most ISPs filtering systems block campaigns if the bounce rate (number of invalid emails/number of emails sent) is too high. This is the reason why you must automate the update of your lists when a message bounces.

Notice

eMill includes all the tools to manage bounces automatically. Read the "*Managing DSNs or bounces*" tutorial available on the eMill help file knowledge base.

Process unsubscribe requests

- **Advice 1**: Do not forget to include an unsubscribe link to your emails

- **Advice 2**: Check that your unsubscribe process is fully functional

Notice

eMill includes all the tools to manage automatically unsubscribe requests. Read the "*Managing a subscribers list with eMill*" tutorial to learn more about it.

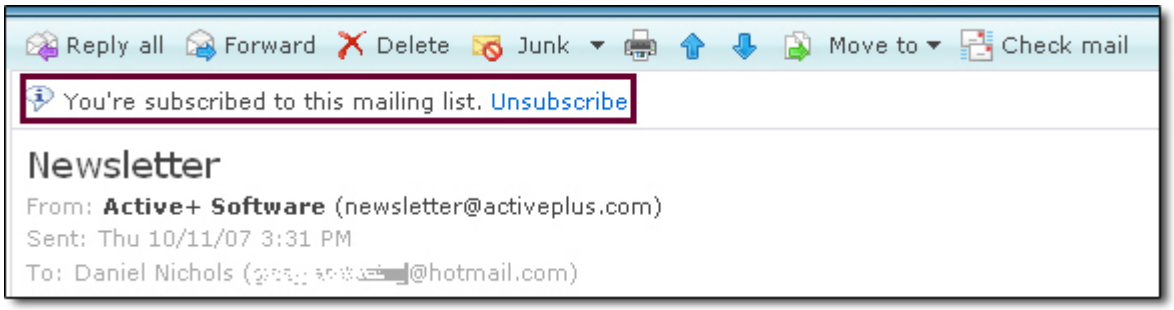
- **Advice 3**: Put your unsubscribe link at the top of the message

- **Advice 4**: Use the new list-unsubscribe standard.

This new standard consists in adding a header in your email using one of the 2 following formats:

- List-Unsubscribe: <mailto:unsubscribe@domain.com>
- List-Unsubscribe: <http://domain.com/unsubscribe.asp?tech@domain.com>

ISPs that support this standard will display an “Unsubscribe” button within the mail client interface. For example, Windows Live Mail displays it this way:



Note: On Windows Live Mail, the “Unsubscribe” link is only displayed when the sender is in the receiver’s safe sender list

Analyse your email program

- **Advice 1**: Remember to your subscribers where they opted in
- **Advice 2**: Include content & disclosure agreements
- **Advice 3**: Follow recipient expectations on content
- **Advice 4**: Follow recipient expectations on delivery frequency
- **Advice 5**: Offer the possibility to your subscribers to define their preferences

You could let them choose which email they prefer (HTML or Text), what kind of content they want to receive…

II. Avoid being blocked by filtering tools

Keep your message content clean

- **Advice 1**: Use standard HTML

You should create your message with high quality HTML editors (eMill HTML Editor, latest version of FrontPage, Dreamwaver…). Tools like MS Word or Publisher generate horrendous HTML with empty or non-standard tags. These are generally found in Spam.

Notice

When creating a campaign with the eMill wizard, emails are in a Multipart format. The *HTMLBody* content is the HTML version and the *TextBody* content is the text version.

- **Advice 2**: Use Multipart MIME

This means that the email includes an HTML and a text version.

.

- **Advice 3**: Make sure that the From and Reply-to addresses are valid.

- **Advice 4**: Do not use some words or letters

All filtering systems are browsing message contents to detect characters used in Spam (Rolex, sex, drugs, Viagra…). In order to have a detailed list of these characters, visit the Microsoft for Outlook or Wilson Web websites.

- **Advice 5**: Minimize graphics.

Most ISPs advise email senders not to exceed 50% of graphics in a message.

- **Advice 6**: Verify web addresses look normal & point to valid domains & don't use web addresses with the following format: http://192.168.102.12

- **Advice 7**: Analyse your content using Spam Assassin.

Notice

The eMill preview mode lets you analyse your email content with Spam Assassin. Just click the *Anti-spam Analysis* button when previewing a message.

Manage anti-spam filters

- **Advice 1**: Ask your subscribers to add you in their address book or safe sender list.

This ensures you that all your future emails will be delivered to the inbox.

- **Advice 2**: Manage Challenge Response requests

This represents anti-spam systems sending an email to the sender asking to confirm the delivery before it is delivered to the receiver's inbox. The main anti-spam systems using this technique are SpamArrest & EarthLink.

- **Advice 3**: Monitor blacklists

Most anti-spam systems are using blacklists to filter emails. You must regularly check if your IP is not listed on blacklists. If it is the case, most of them give the possibility to be removed from their blacklist.

MX Toolbox (free) and Blacklist Monitor allow you to check your IP on the main blacklists. The most used blacklists are Spam Cop & SpamHaus. Note that SpamCop also offers a reporting program.

ISPs are often using commercial blacklists such as Brightmail or proprietary blacklists. If you think you are listed on these blacklists, you must contact them directly.

- **Advice 4**: Monitor delivery

You must monitor general and per domain delivery statistics to react quickly if you detect a problem.

You may also use test lists or 3rd part services to know if your email is delivered to the inbox or to the Junk folder.

The main companies offering this service are:

- Delivery Watch (from US$ 55.00 per month)
- Pivotal Veracity (eDelivery Tracker)
- Return Path (SenderScore Monitor)

- **Advice 5**: Monitor complaint rate and deal with Spam complaints

In order to be informed when a receiver complains about you, you must first create an 'abuse@domain.com' email address where you will receive complaints that are 'manually' sent.

But, as most ISPs include a "Report as a spam" button in their interface, you will not be informed of complaints. This is the reason why some ISP and 3rd part services let you subscribe to 'feedback loops' which allow you to be informed when a receiver uses this button to complain.

- Windows Live Mail

  The Windows Live Mail feedback loop is called 'Junk Mail Reporting Program'.

  You can subscribe for free to this service by answering few questions on your company and your email activity but the subscription and the delay are not guaranteed.

- AOL

  Subscription to the AOL feedback loop is free of charge. You just need to fill in a short form and the delay before your account is enabled is usually short.

- Abuse.net

  Abuse.net is an Internet abusive activity reporting network. If you subscribe to their free service, you will be informed when someone complains about your email activity.

Advice 6: Subscribe to whitelisting programs

Most ISPs use accreditation service providers as a whitelisting program. However, some are still managing whitelists by themselves:

- Yahoo!

  You can subscribe to the Yahoo! Mail Whitelist program for free by answering a detailed questionnaire on your email activity.

- AOL

  You can subscribe to the AOL Whitelist by following strict guidelines and answering a detailed questionnaire.

- United Online

  You can subscribe to the United Union Trusted List by answering a detailed questionnaire on your email activity.

Note that all ISPs let their users create their own whitelist. If you want to be added to a personal whitelist, you must ask the subscriber in your first emails to add you in their address book or safe list.

III. Authentication, accreditation & reputation

- **Advice 1**: Implement Authentication Methods[1]

It represents the practice by ISPs and other mail gateway administrators to establish the true identity of the sender.

The most used authentication methods are the following (click on it to have more information):

- Sender Policy Framework
- DomainKeys
- SenderID

Notice

eMill offers you a free white paper on authentication methods. It explains you where they come from, what they do and how you can implement them.

- **Advice 2**: Contract with an accreditation service provider[2]

These are third-party white list programs that certify your emails as “safe for delivery” after you have followed a rigorous review process.

Here are the 4 main accreditation service providers:

- GoodMail Systems

  Emails certified by Goodmail are directly delivered to inbox to ISPs partners. They bypass all filters except user preferences and links/images are enabled.

  To be certified by Goodmail, you must follow strict guidelines and pay:

  - A non-refundable accreditation fee of US$ 399.00.
  - A per message fee.

- SenderScoreCertified (ReturnPath)

  Emails certified by SenderScore are delivered with preferential treatment to ISPs partners but the delivery to the Inbox is not guaranteed.

  To be certified by SenderScore, you must follow strict guidelines and pay (depend on the number of messages per month):

  - A non-refundable application fee from US$ 400.00 to US$ 1,500.00.
  - An annual license fee from US$ 1,000.00 to US$ 20,000.00 (free for non-profit)

[1] Read the Appendix section to learn which ISPs support which authentication methods.
[2] Read the Appendix section to learn which ISPs support which accreditation service provider

- TRUSTe

  Emails certified by TRUSTe are delivered without any preferential treatments.

  To be certified by TRUSTe, you must follow strict guidelines and pay:

  - A non-refundable application fee based on volume
  - An annual license based on revenue (from US$ 1,000.00 per brand)

- Habeas SafeList

  Emails certified by Habeas are directly delivered to inbox to ISPs partners

  To be certified by Habeas, you must follow strict guidelines. Payment fees are not public.

Advice 3: Monitor your reputation

Reputation services continuously monitor sender activity and determine a reputation score based on a fixed set of criteria. The reputation score changes in real-time with sender activity. Partner ISPs/receivers use the reputation score to filter mail for delivery but a good score never guarantees delivery to inbox.

Here are the 3 main reputation services:

- Lashback

  The reputation score is based on the quality of the unsubscribe processes (unsubscribe reputation, unsubscribe process, list abuse, unsubscribe mechanism). All senders can check live their reputation score for free via the the UnsubSafe lookup tool.

  To have Lashback monitor your email activity, you must pay a set up fee and monthly maintenance fees based on the number of IPs or unsubscribe links monitored.

- SenderBase

  SenderBase is offered by IronPort, one of the leading email appliances vendors. Based on the IronPort machine network, the reputation service allows senders to monitor their score for free.

- SenderScore

  The reputation score is based on the number of complaints, the filtering test, the email volume, the network integrity, the ID stability, the unsubscribe reputation, the sending stability, the reputation on 3rd party services and the authentication methods implemented.

  All senders can check live their reputation score for free at https://www.senderscore.org/.

  It is possible to have access to complementary reputation information by paying a yearly subscription fee.

IV. Get appropriate and clean sending techniques

- **Advice 1**: Choose the appropriate sending method

In order to send messages, you need a SMTP server that handles email transport on the Internet. Here are the different possibilities offered by eMill:

- Use your ISP SMTP Server: Most ISPs allow you to use their own SMTP server to send emailing campaigns. However, it is recommended to consult their policy before choosing this solution. Moreover, it is possible that some ISPs block sending when you reach a fixed limit of messages sent per hour. If you are facing this problem, the eMill « throttle » feature allows you to determine the overall maximum quantity of messages sent per minute (Project > Properties, Mailer Properties tab).
- Use your our company SMTP Server: This solution is the most efficient because you control your sending. Moreover, the IP address usually corresponds to the 'From' and the 'Reply-to' domain names which is a positive point for most anti-spam filters. The only limitation of this solution is that the sending of a high volume campaign could overload your SMTP server. If you are facing this problem, you can either schedule the sending of your campaign during the night or use the eMill « throttle » feature. This allows you to determine the overall maximum quantity of messages sent per minute (Project > Properties, Mailer Properties tab).
- Use the built-in SMTP Server: If you cannot use the above solutions, eMill includes a built-in SMTP server to deliver directly your messages. If you choose this solution, it is important to have a fixed IP address to minimize the risk of being flagged as a Spam. Indeed, the receiving mail server could check if your IP address corresponds to a domain name.

- **Advice 2**: Separate mail streams

In case email is widely used in your company, you could separate mail streams between:

- Corporate Email
- Customer Acquisition
- Customer Retention
- Transactional Emails

- **Advice 3**: Sending Permanence

Sending large campaigns regularly from the same machine is ideal. Spammers usually send a large mailing from one machine and disappear. Therefore, infrequent senders who send large scale mailings could be detected as a spammer or a compromised server.

- **Advice 4**: Configure properly your server

Here are the main settings you must check:

- Get a static IP address
- Control your server security. If a spammer can use your server to send emails, it will be rapidly blacklisted.
- Don't use proxies
- Configure your reverse DNS
- Configure your MX record

You have the possibility to check if your server is properly configured at http://www.dnsreport.com/

If you are facing problems, contact your system administrator or the eMill technical support.

- **Advice 5**: Control the sending volume

Most ISPs set a volume cap to avoid that server gets overloaded. These limits are based on the number of connections or messages per connection but they can vary according to:

- The newness of the IP address
- The domain reputation
- The number of complaints

Appendix

1. Windows Live Mail

If you want to learn more about Microsoft email deliverability policies, we suggest you to download and read the Microsoft white paper 'Improving E-mail Deliverability into Windows Live Hotmail'.

Microsoft has also created 2 free programs to monitor your campaigns:

- The Smart Network Data Services (SNDS) that allows you to monitor the email activity coming from your server.
- The Junk Mail Reporting Program that allows you to receive a notification when a Live Mail user complains about you.

If you are facing delivery problems with Windows Live Mail, you will find complementary information at http://postmaster.msn.com.

Here is a list of the different techniques used by Windows Live Mail to filter emails:

- Sender ID authentication method.
- SmartScreen
    - Content filtering (machine learning approach)
    - Use the feedback of Live Mail users who opted in to the Feedback Loop program
- Phishing heuristics-based check. See http://www.microsoft.com/safety/antiphishing for more details.
- Brightmail anti-spam content filter: Leveraging the "Probe Network", a collection of more than two hundred thousand (200,000) e-mail addresses designed to attract junk e-mail.
- SenderScore Certified accreditation program
- Individual filter (Allow/block list)
- Individual address book
- Server configuration :
    - Up to 500 concurrent connections from a single IP address
    - Each message limited to 100 recipient
    - Follow RFC http://www.faqs.org/rfcs/rfc821.html.
    - The number of messages that can be sent from a single IP address varies according to the sending reputation (new IP address limited to 1000 emails per day, established IP address limited to 3-4 millions messages per day)
    - Check server security and reverse DNS

2. AOL (22,8 millions subscribers)

AOL offers a lot of information to help you deliver correctly your email to AOL users at http://postmaster.aol.com.

AOL has also created 2 free programs to monitor your campaigns and improve your deliverability:

- The AOL Whitelist to improve your chance that your email gets correctly delivered
- The AOL Feedback Loop to receive a notification when an AOL user complains about you.

Here is a list of the different techniques used by AOL to filter emails:

- SPF/Sender ID authentication method.
- Goodmail accreditation program
- Check server security and reverse DNS
- Fingerprinting
- Commercial blacklists
- Content filtering
- Individual filter
- Bounce rate
- Volume cap

Name	Nb of subscribers (million)	Authentication Method	Whitelist	Feedback loop	Accreditation program	Filtering Technology	Contact
ATT.net	NA	No	No	No	Goodmail	Brightmail, volume cap, proprietary blacklist	
BellSouth	NA	SPF	No	No	NA	Proprietary filter, proprietary blacklist	
British Telecom	NA	DK	No	No	NA	NA	
Charter	NA	SPF	No	No	NA	NA	
Comcast	7	SPF	No	No	Habeas, Goodmail	Brightmail, external blacklists	abuse@comcast.net
CompuServer	NA	SPF/Sender-ID	Yes	Yes	NA	DNS check, volume cap, user feedback, reputation	
Cox Communications	2.4	NA	NA	NA	Goodmail	Brightmail (BrightSigTM technology), individual spam filter (McAfee SPAMKiller), machine-learning solution (Corvigo)	abuse@cox.net
Earthlink (mindspring, peoplepc, earthlink)	5.2	DK	No	Yes	NA	SPAMBlocker (brightmail), proprietary blacklists, challenge-response	abuse@earthlink.net
Excite	NA	No	No	Yes	NA	Proprietary blacklist	
Google	NA	SPF/DK	No	No	NA	Image blocking	
Netscape	NA	SPF/Sender-ID	Yes	Yes	NA	DNS check, volume cap, user feedback, reputation	

Name	Nb of subscribers (million)	Authentication Method	Whitelist	Feedback loop	Accreditation program	Filtering Technology	Contact
OptOnline	NA	No	No	No	NA	SpamHaus blacklist, Spamcrub proprietary filter, brightmail	
Outblaze	30	No	No	No	Habeas	Public blacklists (ORDB, RSL, SBL, CBL, Blitzed OPM, Sorbs DUHL), proprietary blacklist (OBSL)	abuse@outblaze.com
Rediff	NA	No	No	No	NA	SpamHaus blacklist	
RoadRunner	3.9	SPF	Yes	Yes	SenderScore, Habeas, Goodmail	3rd part blacklists, static IP	abuse@roadrunner.com
Rocket Mail	NA	DK	Yes	No	NA	NA	
Rogers Cable	NA	DK	Yes	No	NA	NA	
UnitedOnline (Juno/NetZero/BlueLight)	6,6	SPF/Sender-ID	Yes	Yes	Habeas	Content filtering, volume cap, DNS configuration	
USA.net	NA	No	No	No	Habeas	Brightmail	
Verizon	NA	SPF	Yes	No	Goodmail	Proprietary blacklist, brightmail	
Yahoo/SBCGlobal	5.1 (SBCGlobal only)	DK	Yes	No	Goodmail	SpamGuardTechnology, individual feedback, individual filter, volume cap	

eMill

PROFESSIONAL EMAILING SOLUTION

Active+ Software
51, Avenue Général de Gaulle - 66320 – Vinça – France
Phone: +33 4 6805 4774 – Fax: +33 4 6805 5701
E-mail : info@activeplus.com