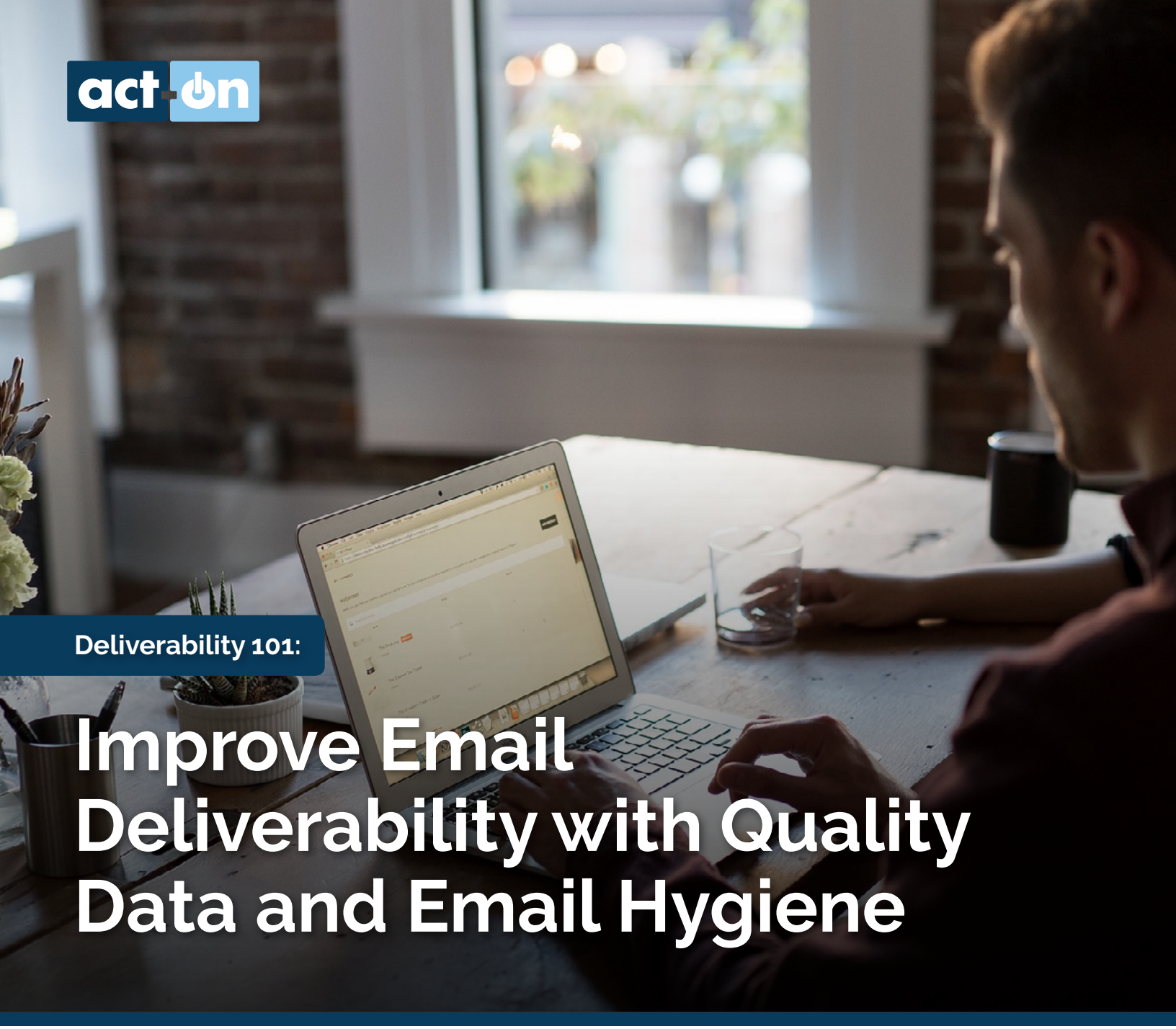


Deliverability 101:

Improve Email Deliverability with Quality Data and Email Hygiene

In this section of our deliverability series, we will discuss how quality data and email hygiene can improve your deliverability. Checking the validity of your emails and understanding where and how to collect your data are important to consider when ensuring proper inbox placement.

Data Quality

Before discussing where and how to get data, there are a few items that are needed to have an effective email strategy. First, depending on your location and whom you are sending to, you need a legal strategy. GDPR, CASL, and similar laws require the data sources to be kept along with the date of the opt-in.

Additionally, there are specific bits of information that any system needs to function properly. Below is a list of essential information, followed by information you should have to improve the efficacy of your emails. Note: Information tagged [PII] is important to think about when storing information in different systems, per GDPR.

Essential Information

- Email [PII] (and yes, some senders don't have this in their email data)
- Name (first and last) [PII]
- Specific source of opt-in [Possible PII]
- Date/time of opt-in
- Double opt-in confirmation [PII]
- Location [PII]
- Company
- Title [PII]

Data affecting performance

- Time zone
- Time in role [PII]
- Decision maker [PII]
- Relevant triggers for business use [PII(?)]
- Behavioral data

Sources of Data (All Emails Are NOT Equal)

Not all data is the same, and not all leads are equal. In marketing and sales, leads can be qualified at different levels and as more or less valuable. The same rule applies with deliverability. Some are "qualified" (good engagers who will help reputation) and others are less qualified (cold emails that haven't been emailed in a while but were engaged with previously).

Below is a list of how emails can be collected and put into a list. These methods can be used by a variety of sources. That said, it is nearly always possible to get data of the best quality (by a sender's second email).

1. **Organic Double Opt-In Email with reCAPTCHA**

This is the preeminent email data for deliverability, marketing, and sales. Hand-raisers have visited your site or completed online forms (with the reCAPTCHA "Are you human?" check) and then confirmed their identity via email.

2. **Organic Double Opt-In Email**

Like the emails you collect through the double opt-in process, these are high-quality emails as the person who submitted their information has confirmed their identity. That said, without reCAPTCHA, the email will likely eventually gain several (depending on the industry, sometimes up to tens of thousands) bots. These bots inflate stats in an disruptive way and can distort testing.

3. **Organic Opt-In Email**

This is good data but has a much greater chance of typos, fake data, and spam traps. In the EU, after GDPR, this type of data is likely not allowed (the law is not clear as of this writing, but accepted best practice is that double opt-in is required). If this is the data a sender is working with, list hygiene is a must for making sure that fewer traps get into the list. (More on list hygiene below.)

4. **Double Opt-In Email**

This data primarily consists of in-person and paper/badge sign-ups at tradeshows and events. A proper double-opt in with the first email fulfills two important purposes: 1) It checks to make sure the right address was listed (hygiene also helps with that); and 2) If the individual has forgotten who the sender is, it reminds the receiver of the purpose of the emails.

5. **Opt-In Email**

Single opt-in emails are the easiest way to put bad data into a system other than the types of data outlined below, which are not allowed in Act-On. Treat this data carefully, and always incorporate list hygiene best practices. Additionally, limit the number of times these emails can be sent-to without a response.

6. **Third-Party Opted-In Data**

There are two types of third-party opted-in data: The "okay" and the "bad." The former occurs when someone opts into an email stream they either know or are told explicitly in email that the person emailing them is different from the sign-up location. Here are two examples:

- **Lendingtree.com:** This site doesn't provide loans, but they do source individuals who do and pass off the information gathered to these third parties. The person signing up is told explicitly what is happening, and they expect and want the emails from the third parties.
- **Marketing coming from an outside source:** At times, companies outsource certain areas — such as marketing content and curation. If a consumer will be getting an email from someone else (a different domain sends the email), it is critical to include the who, what, where, when, why, and how they are receiving the email.

Bad Data (Act-On Prohibited Data)

These data sources are a major pain source for deliverability and can ruin the deliverability of a sender quickly. It doesn't take much bad data to make inboxing disappear, even with the best possible content.

1. **Scraped Data**

Scraping is a technique in which an email visible on the web is "scraped" into a database. This is illegal in some locations (the EU and Canada, to name a few) and is also the primary source of spam traps. Sending to someone who has not asked for content is the definition of unsolicited commercial email (UCE), one of the major types of spam.

Beyond being a spammy practice, scraping also is the #1 way to get pristine spam traps into a database. These traps can quickly put a sender onto a blacklist, and Act-On, along with most ESPs, takes this very seriously. At Act-On, a blacklisting moves accounts to an isolated zone with others who have caused a blacklisting until we feel the situation is remedied.

2. **Purchased (or Rented) Data**

This is the other half of any data that is third-party "opted-in." Unlike the earlier examples, in the broad sense, purchased data is from a third party that offers bulk emails for marketing purposes. Many of these sources claim to have "opt-ins," but this data is either opted-in through misrepresentation, hidden or obfuscated terms, or simply scraped.

Many platforms offer guarantees on their data and claim to have the point of contact to close deals, but these have been the largest source of pain for senders due to various spam traps and "complainers" contained within the email lists. This may look like an easy win to expand reach, but it is not worth it since the cost of a single send to a purchased list can quickly ruin a good reputation.

These companies lists include Lead 411, Discover.org, InsideView, Uplead, Leadiro, and many more. Many of these companies offer a few legitimate services and help complete info on data already collected, but their lists are toxic to a good sender.

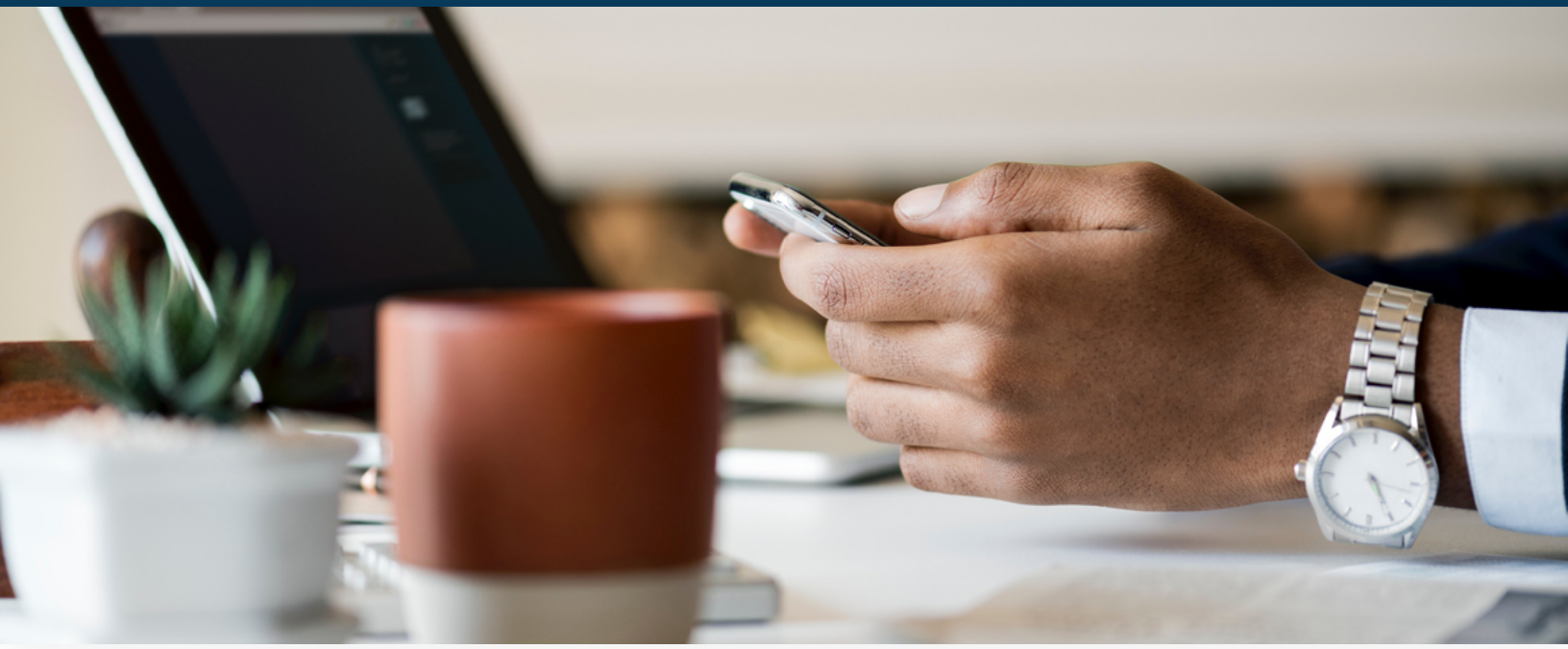
Unknown Data

Marketers, salespeople, and customer service reps are often removed from their data. For instance, senders are frequently handed lists from their predecessor or an executive and told to email to it blindly. That is an easy way to hit a trap and block further sending.

When confronted with an unknown list, there are a few things a sender should do:

- Ask about the lists' origins - gather what information you can
- Look for past sends to the list to see how they have performed and check its age
- Run the list through a hygiene service
- Run a limited test to see if it contains problems and gauge performance

It would be better to not send to an unknown data set at all, but if a sender has gone through the steps outlined above, they can send to the list. However, it is important to keep the sends at less than 20% of that day's total volume to minimize impact and to sunset emails after just a few sends when there is no engagement.



Email Hygiene

Email hygiene is the process of checking the validity of an email list and its likelihood for potential traps. It is a crucial part of any email program and is gaining importance when it comes to deliverability. The email industry used to view hygiene vendors in a negative light because they made it appear senders were getting bad data, but with the rise of internet trolls and the rampant addition of bots flooding sites and forms, hygiene has become a good first line of defense against bad data.

Act-On currently partners with Neverbounce to ensure quality email hygiene. We also continue to work with Webbula, which is an excellent product for catching trap data.

NEVERBOUNCE

Neverbounce is easily integrated with Act-On and allows for segments and lists to be sent to Neverbounce for review. The results are then imported back into your Act-On instance.

The service accomplishes two primary objectives. First, it checks to see if an email is a valid, which is the best way to reduce the number of hard bounces. Second, it checks for proper mail exchange (MX) location, ensuring an email is who it says it is. This is their primary way of catching traps, and, in conjunction with good email sunsetting practices and engagement segmentation (discussed in the next few pages), will nearly eliminate traps from a list.

WEBBULA

Webbula is another hygiene company that also provides validation but with a different approach to addresses that could potentially damage your reputation. Instead of performing a real-time check on the addresses, Webbula keeps a historical database of traps, markers, and other known trackers to remove from a system. This is an aggressive approach to data hygiene that is effective at getting older and unknown-sourced lists ready for sending. Due to the aggressive nature of the cleaning, it does have a large number of trap false positives. However, in the case of an older or unknown list, more is better for a cleanse.

Data Cleanup and Sunsetting Emails

As anyone who works with a CRM knows, data cleanup is necessary to keep a system lean and running well. Email list maintenance is similarly important. Reducing the number of opted out, hard bounces, and unengaged recipients from email lists is important for several reasons:

- **System Speed:** The system runs faster when there are fewer files to check against for every send.
- **Expectations and Actual List Size:** When sending a list, the number of recipients selected may not be the number of emails sent. Many of the emails may be suppressed for various reasons, primarily due to opt-outs and hard bounces. If these are removed from the list, a more accurate list size will be selected.
- **Reputation in the Case of Unengaged Recipients:** Unengaged recipients are those that drag down your stats and lower reputation with every email without an action. They are also sources of possible recycled spam traps.

SUNSETTING EMAILS

It's important to sunset (remove) unengaged recipients from your system at some point. When you choose to sunset these emails should be determined by your sending cadence and level of contact. For example, a prospect who is unengaged should be treated differently than a hand-raiser — and also differently from a current customer. Setting engagement limits based on business process helps ensure the right amount of opportunity for conversion and engagement depending on your industry. Segmentation strategy around sunsetting is covered in our section on engagement segmentation.

Conclusion

Maintaining good list and email hygiene is key to ensuring your emails get seen and that you are targeting individuals who want to engage with your content. Companies like Act-On have maintenance programs to make this ongoing process easier.