emailHIPPO

EMAIL VERIFY ACTION

Do something great with your email data

A guide to your email verification results

STOP BOUNCES

Emails that bounce hard are bad for business. They never reach a reader. If you keep on sending emails that bounce your sender reputation can fall and this can reduce ALL your email deliveries.

REACH MORE INBOXES

When you have confidence in your email data you'll trust your stats more. So you'll have a clearer picture of your campaigns, sales funnels and customer experience.

REACH LOYAL CUSTOMERS

If your customers use disposable addresses your emails will never reach them. Filter people who don't want to engage with you and spend time connecting with real people.

Don't know your greylist from your catch-all?

Learn what the results mean

Mail server responses were written in the 70's as a standard protocol when email communications began to be a 'thing'. Since then the codes have stayed the same but more people with different levels of IT knowledge need to understand them. Here's a guide that tells you what your email verification results mean. Added bonus? Pointers about how to take action and get inspired by your email data.

Email verification results explained

Catch-All

Catch-all addresses are like central post boxes. All emails for a domain arrive in one place and get checked and forwarded. A catch all result tells you that your email will get as far as the post room, but it can't tell you whether it will be sent to a recipient.

Server does not support international mailboxes

The server we need to check with uses character sets such as Chinese, Arabic or Cyrillic, but it's not set up to cope with international mailboxes. The international language of email is Punycode. We can't speak to international servers that don't translate Punycode. We could try just checking really slowly, shouting at it and pointing but it won't work. Your email address may be OK, but we can't be sure.

At sign not found

@. This little thing is what makes an email address. An email address without an @ isn't an email address. Like a plane without wings. Check where the @ should be and edit the address, or delete it from your list. It'll never fly!

Domain is well known DEA

A DEA is a Disposable Email Address. This email address will last for just a short period of time. People use disposables when they don't want to be reached. You don't want disposables on your mailing list and there's no point sending mail to them. There's a strong link between disposable emails and fraud, so be especially wary of DEAs if you sell online. We scan continually for new disposable email addresses, picking up 99% of them, which is the best detection rate in the business.

No MX servers found

An MX server is a mail exchange server. The thing that takes mail in and sends it out. If an email domain doesn't have an MX server, it isn't possible to send an email to that address. Delete this from your list, or check the domain for errors and try again.

Mailbox does not exist

No mailbox exists - don't try to mail to this email address as you'll get a hard bounce result. There is no chance of getting an email delivered to this address.

Possible spam trap

We think the email address is a spam trap. Don't mail to it. A spam trap is an email address that is monitored but not used. Spam traps can't be opted onto a list, There's a slim chance it might be a really old email address that's been 'recycled' into a spam trap. Mailing to it will probably result in a spam report and may result in your IP address (or your email service provider's IP address) being block listed, which is bad news.

Domain is inexistent

If the email contains a bad domain you can't send an email to it. Check and update the domain, or just delete it from your list.

Greylisting

A greylisting result is recorded as 'unverifiable' because we haven't been able to get hold of the mail server to check the status of the email address. Greylisting happens when we try to shake hands with a server and it tells us to come back later and try again. It's usually due to security protocols; by asking us to come back again, the server is checking that we're not spammers. Our advice is to retry the check later as you might get a different response. You can mail to greylisted addresses.

None

This result is returned when we just don't have any extra information to share. It doesn't happen often, but it's what we say when we are nonplussed. Maybe the server we're trying to reach is on a shut down or there's a system drill going on. Think of it as the mail provider doing things that are ad-hoc and interrupting normal responses.

Too many @ signs

Any email address can only have one of these @ signs. If there are too many, it's an invalid address and you can't mail to it - you'll get a hard bounce. Either check and edit the address or delete it along with your hard bounces. Note: some verification services will have a go at guessing where the right @ should be. Avoid 'guess mail' it's an opt-in nightmare as you can end up mailing the wrong person!

Freemail

We let you know if the email service is a freemail - like Hotmail. That's because freemail services can have different delivery and open rates compared to B2B correspondence. You'll know your customers best, so that's why we flag the email provider and let you understand your results.

Unpredictable system

The email system used by the mail server is unpredictable. This is a result we use to flag malicious spam traps and systems that are acting strangely and not returning intelligible results to our request.

Unknown

This is the secondary code that is the exception to prove the rule. We know the primary result is right, but we can't find out more information to explain why.

Transient network fault

Something went wrong right at the split-split-split second that we got hold of the mail server to check your email address. The result might be different later. It's worth another try, but if you get more than a couple of these transient faults in a row for the same email address don't keep on trying. It might be a long term fault and you'll be wasting time and money trying it over again.

Syntax verification

Lists are checked for syntax errors. If you integrate our API you'll get more detail on over a dozen syntax error types. API users can create unique realtime messaging for users depending on the error; for example; ' whoops, too many domains in your email address.' Syntax checks detect invalid characters and count character strings. Long email addresses are likely to be bot generated, disposable or fraudulent. You can't mail to syntax errors. You might be tempted to guess how to correct syntax errors. We recommend not using 'guess mail' as there's no guarantee of fixing the error and you might end up mailing the wrong people!

Retry later

The domain server wasn't available when the email address was checked. It might be a network fault, or that we were working too fast for the server and we triggered a security flag. If you get this result, try checking it again later.

Mailbox full

There is a mailbox to mail to, which is good news. But it's full. You could try checking again to see if the recipient has cleared up their inbox. In most cases a full mailbox is seldom checked and just crammed full of rubbish. We wouldn't bother trying to send an email to a full inbox.

Mail server fault detected

The fault isn't specified, but we know something is wrong with the mail server at the other end. It might be temporary, so it's worth trying again later. A mail server with a permanent fault won't deliver your email to an inbox.

Role address

We identify role based email addresses (sales@, info@ etc.) with our API so you can filter them in the way that best works for you. Some email service providers won't let you upload role based email addresses. That's because role addresses often have low open rates, and are far less likely to be opted in than email addresses for named individuals. Role based email inboxes often attract spam. Try to connect with the real people behind the role 'bucket' addresses.