



BIMI, Explained

Getting your logo beside your mail —
what it takes, and what it is worth

A plain-English guide for people who run businesses, not mail servers. The seventh in a series, and the only one that is not about security. It is the one that costs money, so this guide spends as much time on whether to bother as on how.

01

What BIMI actually does

Shown at roughly the size it appears.

BIMI puts your logo in the little circle beside your messages in someone's inbox. That is the whole of it. Nothing about delivery changes, nothing about security changes, and the message was arriving perfectly well before.

This is the whole of it. A small square, in a list.



Figure 1 — The entire benefit.

Drawn honestly, it is a small thing. Whether a small thing is worth an annual fee and a week of setup is a real question, and Section 10 comes back to it rather than assuming the answer.

What it is not

Worth settling before anyone spends money.

BIMI is regularly described as a security or trust feature. It is neither, and the distinction matters because believing otherwise leads people to buy a certificate when the money would be better spent elsewhere.

- **It does not stop impersonation.** DMARC does that, and BIMI requires you to have already done it. Someone forging your domain is being stopped by the DMARC policy, not by the logo.
- **It does not improve deliverability.** Publishing it will not move your mail from spam to inbox.
- **It does not prove anything to your reader.** A logo appearing is a weak signal at best, and most people do not know what its absence would mean.

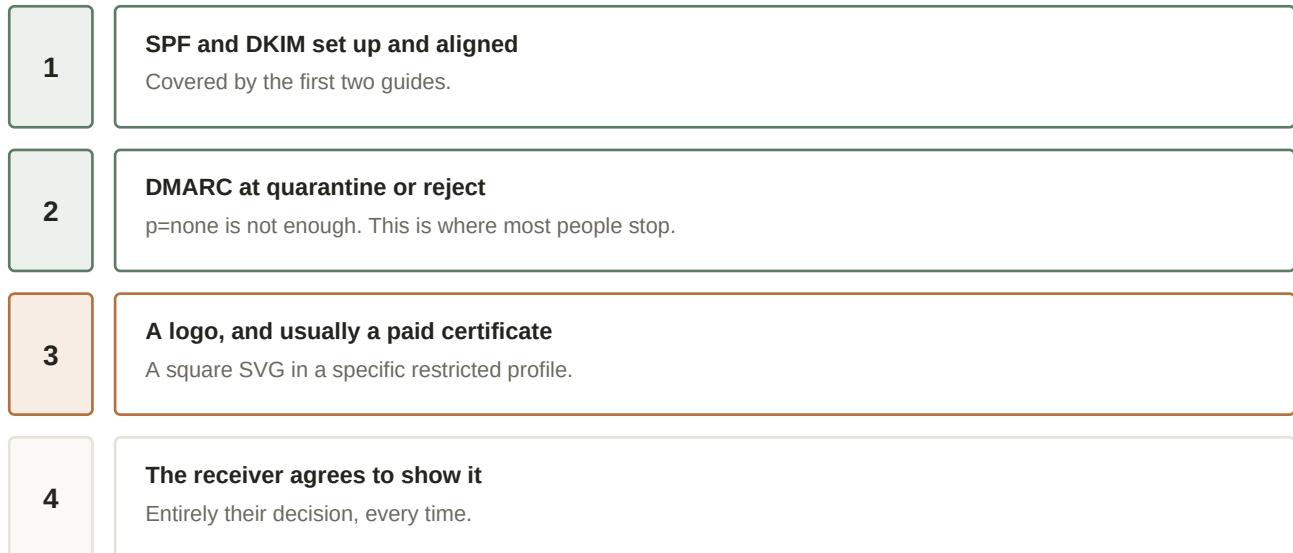
It is also not a standard, quite

SPF, DKIM, DMARC and the rest in this series are published standards. BIMI is a long-running draft maintained by an industry working group, and what actually happens is whatever the mailbox providers choose to implement. That is not a reason to avoid it, but it does mean the rules can move.

What you need before you start

Most readers are not eligible yet.

Four gates. You control the first three.



If you are not already at step 2, that is the work worth doing regardless of whether you ever want a logo — it is the part that actually stops people impersonating you.

Figure 2 — Four gates, and you control three.

The second gate is where nearly everyone stops. A DMARC policy of p=none does not qualify, however long it has been published, because it asks receivers to do nothing. You need quarantine or reject, which is the subject of the DMARC guide in this series.

A wrinkle worth knowing about

Much BIMI guidance still says your DMARC record needs pct=100. That tag was retired from DMARC in May 2026 and receivers now ignore it. If you meet this advice, it is out of date rather than wrong about the intent — what is being asked is that your policy applies to all of your mail, which is now simply the default.

04

The record you publish

The easiest part of the whole exercise.

```
default._bimi.yourdomain.com  
v=BIMI1; l=https://...; a=https://...
```

v=BIMI1

The version. Always this.

l=https://...

Where your logo file is. Must be HTTPS, and must be served as an SVG.

a=https://...

Where your certificate is. Optional in the standard; required in practice by the providers most people care about.

apv=brand

Whether to prefer your logo or a personal avatar. Provider support varies.

Publish it at your main domain and subdomains inherit it. "default" is the selector; others are possible.

Figure 3 — A BIMI record, pulled apart.

Published at your main domain, it is inherited by your subdomains. If you want a different logo for a particular mail stream you can publish under another selector and point messages at it with a header, though support for that varies by provider.

The logo file

Not any SVG. A specific, restricted kind.

The logo has to be an SVG in a profile called SVG Tiny P/S, which exists to make the file safe to render inside a mail client. Exporting from ordinary design software will not produce it.

A restricted profile called SVG Tiny P/S — not any SVG file.

yes	A square viewBox	the same width and height
yes	A title inside the file	your organisation name
yes	A solid background colour	so it survives both light and dark inboxes
no	No scripts	nothing executable, at all
no	No external references	no fonts, images or styles fetched from elsewhere
no	No embedded photographs	shapes only, not pictures

Exporting from ordinary design software will not produce this. There are free converters that will, and your certificate provider will usually check the file before issuing.

Figure 4 — What the file must and must not contain.

The file then has to be reachable over HTTPS and served with the correct content type. A surprising number of BIMI setups fail here rather than anywhere clever — the file is behind a rule that blocks unfamiliar visitors, or the server hands it back as a download rather than as an image.

Design advice that actually matters

It will be shown at about the size of a fingernail. Bold simple shapes, strong contrast, no thin lines and as little text as you can manage. A mark that reads beautifully on a letterhead often turns to mud at twenty pixels.

The certificate, and what it costs

The part that decides whether this is affordable.

Publishing a logo does not prove it is yours, and BIMl never checks. That job belongs to a certificate issued by an independent authority after they have verified your organisation and your rights to the mark.

	VMC	CMC
What it proves	You own a registered trademark	You have used this logo for a year
What you need	A trademark registration	Evidence of prior use
Rough cost	Around a thousand a year	Less, but not free

Both last about a year and then need renewing. The certificate is what an independent authority checks — BIMl itself never verifies that the logo is yours.

Figure 5 — Two kinds of certificate.

For most of BIMl's life only the first of those existed, which meant a registered trademark was effectively mandatory and most small organisations were excluded. The second type is newer and accepts evidence that you have simply been using the logo, which has opened BIMl up considerably.

Remember the renewal

These expire after about a year. When one lapses the logo quietly stops appearing, with nothing to tell you — put the renewal date somewhere a person will actually see it.

Who actually displays it

Fewer than you might hope, and it changes.

Every provider decides for itself. This is the position as this guide goes out.

Gmail	Certificate required
Apple Mail	Certificate required
Yahoo	Will show a logo without one, for bulk mail with good reputation
Others	Varies, and several show nothing at all

Treat this table as perishable. Provider policies change without notice, and none of them owes you a logo even when you have done everything correctly.

Figure 6 — The position as this guide goes out.

The pattern worth noticing is that the two providers most people care about are also the two that require a certificate. If your reason for doing this is that your logo should appear for your customers on the major consumer services, then the certificate is not optional in practice, whatever the specification says.

Nobody owes you a logo

Even with everything published correctly and a valid certificate, display is discretionary. Providers apply their own reputation thresholds and some will show nothing to a sender they do not recognise yet.

Why you are not seeing your logo

The normal experience, not the exceptional one.

You published everything and see no logo. In order of likelihood:

1	DMARC is not at enforcement	the commonest cause by a distance
2	The message did not align	BIMI follows DMARC, per message
3	No certificate, at a provider that needs one	nothing will show
4	The SVG is not reachable or not the right profile	check it loads over HTTPS as an SVG
5	Reputation is not good enough	providers apply their own bar
6	It is simply cached	wait, and send fresh mail

There is no error message anywhere in this process. Nothing tells you which of these it was, which is why the list is worth working through in order.

Figure 7 — In order of likelihood.

The thing that makes this frustrating is the complete absence of feedback. No system tells you that your certificate failed to load, or that your reputation is below a threshold, or that the message you just sent did not align. You are left checking each possibility in turn, which is why the order above is worth following.

A sensible order to do this in

Cheapest and most useful first.

- **1. Get DMARC to enforcement.** Worth doing whether or not you ever publish a logo, and nothing else here works without it.
- **2. Prepare the logo file.** Free converters exist. Do this before buying anything, because a mark that will not convert cleanly is worth knowing about early.
- **3. Publish the record without a certificate.** Costs nothing. Some providers will already start showing it, which tells you the rest of your setup is right.
- **4. Buy a certificate only if you still want the others.** By this point you know your file works and your authentication is sound, so you are paying for exactly one thing.
- **5. Diarise the renewal.** A year passes quickly and the failure is silent.

Why step 3 before step 4

It is the only cheap test available. Publishing a record with no certificate proves your DNS, your file hosting and your alignment all work, and it does so before you have spent anything.

Is it worth it

The question the rest of this guide has been dancing around.

Worth being straight about, before you spend anything.

WHAT YOU GET

Your mark beside your mail at some providers. Recognition in a crowded list. A reason to finish the DMARC work, which is worth doing on its own account.

WHAT IT COSTS

An annual certificate fee, design time for a conforming file, and a renewal to remember. No effect on deliverability, and no guarantee anyone displays it.

A reasonable position: do the DMARC work first because it protects you, and treat the logo as a marketing decision to be judged on marketing grounds.

Figure 8 — Both columns, honestly.

If you send a lot of consumer mail and your brand is something people recognise, the case is reasonable: you are buying recognition in a crowded list, and the annual fee is small next to what you already spend on presenting yourself well.

If you are a small organisation sending mostly to people who already know you, the honest answer is probably not yet. The DMARC work underneath it is valuable and you should do that regardless. The logo is a marketing purchase, and there is no shame in deciding it is not this year's.

Check your own domain

ReaperCloud's BIMI tool checks your record, fetches the logo the way a provider would, validates it against the required profile, and confirms your DMARC policy is at enforcement — which is the check that catches most failures before you spend anything. reapercloud.com/bimi.php, or reapercloud.com/report.php for everything at once.

BIMI is not an internet standard in the sense the rest of this series is. It is specified in a draft maintained by the AuthIndicators Working Group, and display behaviour is decided by individual mailbox providers. Details given here, particularly about which providers show what, were accurate at publication and change without notice.