

Authenticate with DKIM

Scammers, spoofers, and phishers, beware!

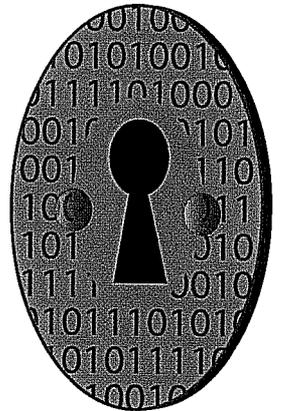
Serious email authentication means scammers' days are numbered.

In a nutshell, DomainKeys Identified Mail (DKIM) is a new and advanced method for verifying the domain of an email sender. Pioneered by Yahoo! and our like-minded partners (industry leaders who also hate scammers), DKIM is a signature/cryptography-based framework. It lets email providers validate that messages do in fact come from you (and not someone pretending to be you).

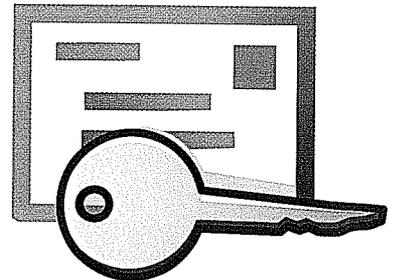
DKIM makes phishing attacks easier to detect, and helps us all identify abusive domains. Because it operates at the domain level, DKIM can be used around the globe. This is just another reason why the Internet Engineering Task Force (IETF) has approved DKIM as a proposed Internet standard (RFC 4871, to be exact).

The next step? Sign and verify your messages using DKIM.

When you authenticate messages, customers will know for certain that your messages are legitimate. This protects them (and you) from forgery and fraud, while letting the world know you're serious about online protection.



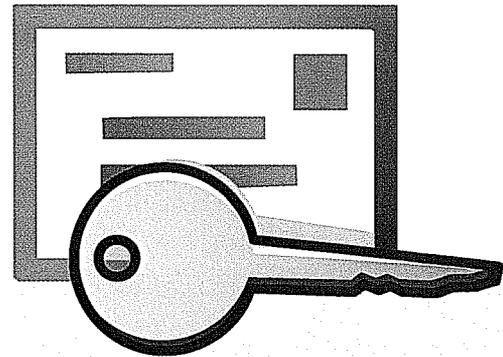
To see how easy and affordable DKIM adoption is, check out the facts on the back.



YAHOO! MAIL

DomainKeys Identified Mail (DKIM) is both easy to adopt and highly effective.

Thanks to DKIM, you can help ensure that your company's legitimate email gets through—and that forgeries are weeded out. The domain level authentication framework validates your email domain on all outgoing messages. This means recipients can tell whether messages that say they're from you, actually *are* from you. All while giving you the benefits of security and simplicity, including:



- Low cost of implementation
- Simple integration with third party mail systems
- No client User Agent upgrades required
- Minimal charges for senders
- Easy scalability
- Easy to implement (regardless of how many domains your company hosts)

Start now. Send a message to phishers (and your customers).

Tell customers that you take their online security seriously—while telling scammers, spoofers, and phishers that their days are numbered. Here's how to begin the process of adopting DomainKeys Identified Mail:

- Compile a list of incoming and outgoing mail systems
- Determine who is legitimately sending messages using your name (including outsourcers, partners, satellite offices, and other sources)
- Identify an implementation partner

To find out more about Yahoo! development of DomainKeys Identified Mail, and how to sign and verify your messages with DKIM, visit:
<http://www.dkim.org>

YAHOO! MAIL