# Is there going to be transport encryption for my e-mail

mailbox.org checks security standard of e-mail recipients before sending

How would you know if your e-mail will be delivered via a **secure connection**?
When composing your message with mailbox.org, just by typing the recipient address, you will find out in an instant – **before actually sending** anything! A simple symbol next to the recipient address will show you what kind of transport encryption is supported by the e-mail provider of the recipient. As a result, your private and business communication will become transparent and more secure.

All customers of mailbox.org can now easily check if the message they want to send will be transmitted to the recipient via an SSL-encrypted connection. mailbox.org uses a straightforward way to classify the e-mail providers at the receiving end of the communication. Basically, there are four symbols indicating the supported transport security level:

- 1: If the system supports the **highest SSL standard as well as DANE and DNSSEC security**, users will be presented with a **completely colored green symbol showing a tumbs-up**:
  "Even though surveillance scandals are in the news on an almost daily basis, only 85 percent of e-mail providers offer basic SSL encryption.", says Peer Heinlein, founder and operator of mailbox.org. "For this reason, users have no real certainty about the secure transmission of their e-mail messages around the world."
- 2: **Standard SSL encryption** support will yield a **green framed thumbs-up symbol**.
- 3: **A grey question mark** will show if there hasn't been any e-mail handling between the mail provider of the recipient and mailbox.org (so **we don't know yet**, which set of security measures this provider supports).
- 4: If the provider offers **no encryption** whatsoever, users will see a **red prohibition sign** next to the recipient's address.
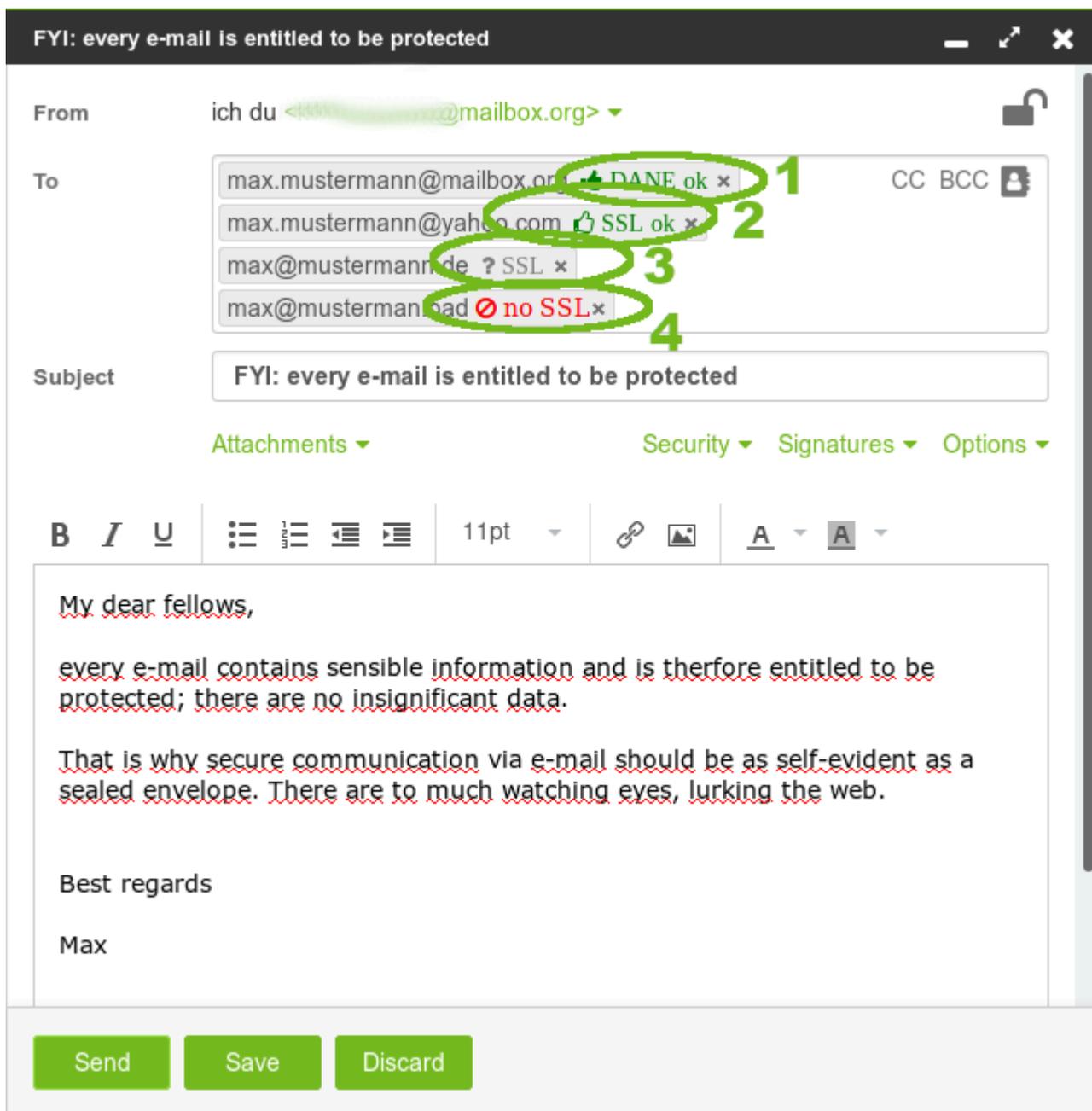
Offering secure transmission to… everywhere

E-mail providers are not obliged to facilitate secure communication to other providers. If there is no encryption, a malicious actor could interfere as a "man in the middle" and manipulate the SMTP connection process in order to force an unencrypted delivery of the message.

At mailbox.org, such attacks **will be detected** automatically and if an external mail server suddenly falls below its previously known security standard. We will stop the delivery of e-mails to this server **until our administrative team will investigate the case** and determine, when it will be safe to deliver messages to this server again.

Through these measures, mailbox.org creates a new level of security for the sending of e-mails. The new service works with all mail servers on the web, which stands in contrast to the project "E-Mail made in Germany", where the secure transmission of messages is limited to a few selected providers. mailbox.org can guarantuee the secure sending of e-mails to all providers which support **secure encrypted connections**.

Verwandte Artikel

- An introduction to mailbox.org Guard
- Is there going to be transport encryption for my e-mail
- Fingerprints of our SSL Certificates
- HowTo: YubiKey NEO as PGP smartcard
- Activate your mailbox.org Guard