Ensuring E-Mails are Sent Securely

As we explained in our article on SSL/TLS-encrypted connections, we use such connections for exchanging e-mails with other providers whenever we can. This is largely subject to the other providers also supporting SSL/TLS connections. With most providers, there is no reliable way of telling whether a connection is secured this way. With us, there is!

Sometimes You'd Rather Not Send Anything if It's Not Encrypted

In this event, mailbox.org offers you not only a regular me@mailbox.org address, but also me@secure.mailbox.org. You can make use of this address whenever you wish to be absolutely certain that a secure connection will be used; some data is so sensitive that it cannot be shared at all without protection. 'True' encryption via GPG, of course, is the best way to achieve this, and it is our recommended method. However, GPG isn't available everywhere, and your e-mail partner may be unfamiliar with it. In these cases, you can take advantage of your special @secure.mailbox.org e-mail address – it's perfect for online portals, booking systems, fleeting acquaintances, recipients like hotels, the tax office, or anyone else who is not switched on to GPG yet.

Secure E-Mail Receiving

We make sure to accept all e-mails directed to an @secure.mailbox.org address via secure connections only. Note: If the other provider is unable to send via a secure connection, we will not be able to accept them. In that case, the e-mail will be bounced back to the sender with a delivery failure notification.

Secure E-Mail Sending

When you select @secure.mailbox.org as the sender address in our webmail client, our mail servers will use secure connections for sending e-mails from this address exclusively. Again, the recipient's provider also needs to support connection encryption; otherwise, the e-mail cannot be sent.

If the recipient does not support secure connections, e-mail transmission will fail. That is how secure connections are designed to work. You (i. e., the sender) will get the sent e-mail back in your inbox after a few seconds, complete with a delivery failure notification. Whoever has sent the e-mail is always clearly informed about the delivery attempt having failed.

In this case, you need to figure out an alternative way of sending your sensitive data – and you can also rest assured that your sensitive data wasn't accidentally delivered without encryption protection. Having a security mechanism like this, then, also poses certain restrictions. Most likely, you won't be using your @secure.mailbox.org alias unless you really need to. But much more important than that is that mailbox.org actually provides the option in the first place.

How to Enable Your Secure Mailbox Alias

Log in to your mailbox.org Office and select 'mailbox.org' from the Settings menu. You can enable your personal secure e-mail alias under 'Encrypted Sending'. Share your secure address with friends and colleagues in order to receive e-mails for this address. When you are composing an e-mail within mailbox.org Office, our webmail client will always offer your personal @secure.mailbox.org alias as an optional sender address. Select this sender whenever you want to be absolutely sure that the e-mail will be sent via a secure connection.

Advanced Settings for Experts

The Expert mode described below is only meant for users who have in-depth knowledge of SSL/TLS. We strongly advise regular users against changing anything in the Expert mode, especially if you are unsure what effect your changes might have. We also need to point out that many other providers do not support the advanced secure connection settings offered here, which will usually lead to delivery failures.

Seasoned mail server experts can use the Settings menu not only to enable the secure address alias but also to specify a TLS policy. If 'simple' SSL/TLS connections aren't secure enough for you, you can select more imposing security levels here:

- **encrypt:** Regular secure e-mail encryption via SSL/TLS, but insecure plaintext is forbidden.
- **dane-only:** E-mails are only sent to providers whose SSL certificate is verified by valid DANE records.
- **verify:** E-mails are only sent to providers whose SSL certificates have been manually added to our database.