

Information on phishing emails

What is phishing?

Phishing is a criminal method on the Internet. Using this method attackers try to get hold of personal data especially passwords. Frequent targets of phishing are the access data for email accounts as a kind of “door openers” to the online life of the affected persons (social media accounts, accounts for online-shopping, banking access etc.).

How do I recognize a phishing email?

If one or more of the following characteristics apply to an email that you have received, this email is most likely a phishing email (German examples in quotation marks):

- unknown email address of the sending person
- impersonal form of address without calling your name: “Hallo ...@hmt-rostock.de”
- pretending of an increased urgency: “Wenn Ihr E-Mail-Konto innerhalb der nächsten 24 Stunden nicht überprüft wird, ...”
- threats: „Andernfalls wird Ihr Konto aus dem System entfernt.“
- one or more links that do not belong to the hmt Rostock
*Links belonging to the hmt Rostock always end with hmt-rostock.de:
„https://service.hmt-rostock.de“*
- a request to reveal personal data and passwords
Neither the hmt Rostock nor the company Gecko as an IT service provider will ever ask for a password to be revealed.
- linguistic errors
- wrong display or no display of vowel mutations („ä“, „ö“, „ü“)

How do I react if I received a phishing email?

- Ignore the email and delete it.
- Do not click on any links.
- If you have accidentally clicked a link, close your internet browser immediately.
- Never reveal your password.
Technical support is possible without this information.
- Do not open any attachments that you are not expecting or that you cannot assign.
Files of the following formats can be particularly dangerous: *.zip, *.doc, *.docx, *.xls, *.xlsx

If you are uncertain whether your email is a phishing email

(e. g. if the sending person's email address appears to be from the hmt)

- Check whether the sender or the content of the email is already listed in the collection of phishing emails.
- Get in touch with the contact person at the hmt and ignore the email for the moment.

How do I react if I have accidentally revealed personal data?

If you have revealed personal data such as the password of your email account:

- Change your password immediately. Use only the usual web interface at <https://exchange2013.hmt-rostock.de/> for this.
- In addition, inform the contact person at the hmt.