Criminals use various strategies to harm you. Popular attack strategies are:

- The dissemination of malware to e.g. gain access to your devices and in the next step to the IT infrastructure of KIT.
- Deception of the end users to obtain sensitive information (e.g. access data).

A widely used attack method is to send fraudulent messages to you that pretend to have a legitimate reason. Fraudulent messages may be received via different channels, e.g. as emails, SMS, via Messenger or social networks. For employees of KIT the risk is greatest in the context of emails, because often names are given on the website and so the mail address can easily be determined.

The contents of these messages may be dangerous in different ways:

- **Sensitive data:** The messages ask you to return sensitive data, such as access data or documents worth protecting.

**Money transfers/calls:** The messages ask you to transfer money or to call e.g. cooperation partners, supposed friends or business partners. In this way, criminals will get the money by direct transfer or debiting them on the telephone invoice.

**Links:** The messages may contain one or several dangerous links (this kind of message is also called phishing message). The fraud is aimed at making you open the attachment. By opening or executing files (e.g. an attachment of an email) the criminals want to make you open the attachment. By opening or executing the file, malware is installed on your device.

**Advertisements:** The messages may contain ads or other worthless contents (these messages are frequently called spams). The attack is aimed at making you buy something. In reality, the primary damage done is lost working time, because often names are given on the website and so the mail address can easily be determined.

In this flyer you will find general information about fraudulent messages as well as seven rules to detect fraudulent messages.

In everyday life, your focus is not always on checking messages for fraudulent content. However, with the help of these rules you will be able to discover most of the fraudulent messages. In case you fall for a fraudulent message and then notice it, please contact immediately your IT appointee of the business unit or send an email to cert@kit.edu. Please do not be afraid. By fast reporting incidents you help to inform the KIT of attacks and/or to minimize damage.

In case you identify a fraudulent message in future, delete it directly. You may also register for the procedure to report fraudulent mails and shift these mails to the corresponding folder in your mailbox. Doing this, you help protect KIT’s IT infrastructure. For more information on the procedure to report fraudulent messages, click: [https://s.kit.edu/it-security.reporting-procedure](https://s.kit.edu/it-security.reporting-procedure)

If you receive a message and you hesitate whether it’s a fraudulent message, please also contact your IT appointee of the business unit or send an email to beratung-itsec@scc.kit.edu with the request for help.

**Identifying Fraudulent Messages**

How to Detect Fraudulent and Phishing Messages

**Protected by:**

Karlsruhe Institute of Technology (KIT)
President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe, Germany
www.kit.edu
Karlsruhe © August 2020

**Contact**

Steinbuch Centre for Computing (SCC)
Division IT Security and Service Management (ISM)
Andreas Lorenz
Phone: +49 721 608 24500
E-mail: beratung-itsec@scc.kit.edu
www.scc.kit.edu

Digital Office
Information Security Officer
Milan Burgdorf
Phone: +49 721 608 41035
E-mail: informationsecuirtyofficer@kit.edu
www.digitaloffice.kit.edu

Institute of Applied Informatics and Formal Description Methods (AIFB)
Research Group Security • Usability • Society (SECUSO)
Prof. Dr. Melanie Volkamer
Phone: +49 721 608 45045
E-mail: secuso@aifb.kit.edu
secure.aifb.kit.edu
twitter.com/secusoresearch

**Issued by**

Karlsruhe Institute of Technology (KIT)
President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe, Germany
www.kit.edu
Karlsruhe © August 2020
The following seven rules will help you detect fraudulent messages:

1. **Rule:** Check the sender and contents of every message for plausibility.
   - Does the sender not fit to the message?
   - The sender info@secuso.org for a SECUSO e-mail
   - The sender info@secuso.org for a SECUSO e-mail
   - Are you asked to provide sensitive data?
   - Are you asked to transfer money or to call somebody, with the information required for this purpose being given in the message?
   - Do you have no user account at the sender's address?
   - Do you not expect the message?
   - Is the form of the address incorrect or does it not match the sender?
   - Is the message digitally signed by the respective person?

   The more questions can be answered in the affirmative, the higher is the probability of a fraudulent message. Special care is required, if you are asked for sensitive data, passwords included.

2. **Rule:** If the sender and the content of a message appear plausible and the message contains one or several links, check the links carefully before you click on one of them. To make sure that it is not a fraudulent message, e.g. somebody pretending to be the supposed sender, therefore you check the link.

   On mobile devices (smartphones and tablets), the process of identifying the web address of a link depends strongly on the device and the respective app. In most cases, the web address is displayed in the dialog window by touching the link with your finger and holding it for at least two seconds. Take care not to click the link accidentally. If you are uncertain, wait until you are back at your PC or laptop.

3. **Rule:** As soon as you have found the web address behind the link, look up the so-called who-area of the web address.

4. **Rule:** Having identified the who-area of the web address, check whether the who area domain is related to the (apparent) sender and the contents of the message. If the sender or the subject does not match the content, do not click the link.

   For example, in case you expect the link to lead you the website for a SECUSO e-mail address to deceive you, e.g. by searching for the address in a search machine. If you are still unsure afterwards, please contact your IT appointee to assess the message together.

5. **Rule:** If the file format is potentially (very) dangerous, open the attachment only if you expected precisely this attachment.

   If you have opened Office programs and you are asked whether so-called macros are may be executed, think again about whether the message containing the respective file is fraudulent. If you are still unsure afterwards, please contact your IT appointee or contact via e-mail beratung-itsec@kcc.kit.edu to assess the message together.

Further Information

How to recognize fraudulent messages is explained in two videos:

To the videos: s.kit.de/ssitsecurity/fraudulent-messa-ges.video

To the NoPhish online training: s.kit.de/IIT-security/fraudulent-messa-ges.training

If you want to deepen your information on fraudulent messages from this flyer, you are invited to join the NoPhish online training.