General Information

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 e-mails, 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: 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: messages may contain one or several dangerous links (this kind of message is also called phishing message). The fraud is aimed at making you click one of these links. These links will then lead you to e.g. a deceptively real-looking, but fraudulent website (also called phishing site) where you are supposed to log in. Alternatively, you are guided to a website that installs malware on your device.

Attachments: messages contain one or several dangerous files (e.g. an attachment of an e-mail). The criminals want to make you open the attachment. By opening or executing the file, malware is installed on your device.

Advertisements: 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 you look at the message, assess it, and delete it.

Protecting the IT infrastructure of KIT together

The SCC uses various technical measures to prevent fraudulent messages from entering the KIT network. Unfortunately, with the existing tools it isn't possible to detect fraudulent messages at all, because fraudulent messages are increasingly difficult to detect as the methods of attack are getting better, and too strict filtering would have the consequence that even messages would not be delivered which aren't fraudulent but, as it happens, showing similar characteristics like fraudulent messages.

Therefore, it is important that you check your messages carefully. Your assistance is an integral part of the IT security concept of KIT.

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 e-mail 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 will 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

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 e-mail to beratung-itsec@scc.kit.edu with the request for help.

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: informationsecurityofficer@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
secuso.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 Institute of Technology

Identifying Fraudulent Messages

How to Detect Fraudulent and Phishing Messages

A Cooperation of SCC, Information Security Officer, Research Group SECUSO at AIFB and KASTEL

SCC Steinbuch Centre for Computing · Information-Security-Officer · aifb · KASTEL · SECUSO SECURITY · USABILITY · SOCIETY

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@**sye.jp** 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?
- Did 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. Parts of KIT including SCC and the IT appointees would not ask you to send them your password.

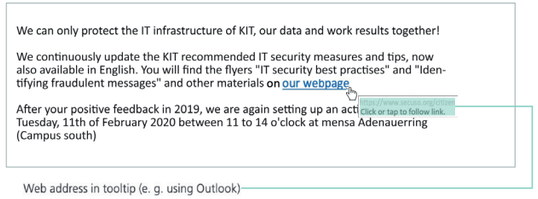
By the way: most of these questions may be useful in other situations, for example when receiving a fax, a call or letters.

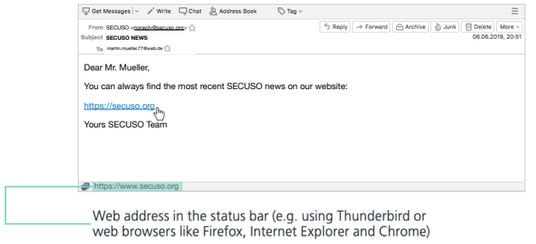
2. Rule: If the sender and the content of a message appear plausible and the message contains one or several links, check the links carefully before you click on one of them. To make sure that it is not a fraudulent message, e.g. somebody pretending to be the supposed sender. Therefore you check the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

In most cases links are underlined and colored blue. However, links may also be integrated in the form of buttons or pictures.

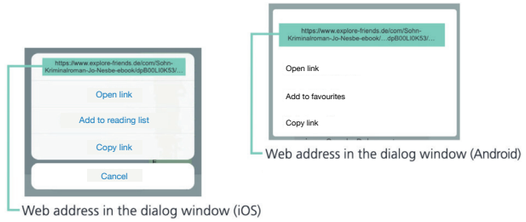
To check the link, find out which web address (also called URL) is hidden behind it. This information can be found in different locations, depending on device, software and service (e.g. Amazon, Dropbox, Skype, WhatsApp, Facebook, Xing). Before using a device, software, or service, check where to find the actual web address of the link.

On PCs and laptops, web addresses can be usually displayed by hovering over the link with the mouse, without clicking it. The link will display either in the status bar at the bottom of the window or in an information field, called a tooltip.





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.

https://nophish.secuso.org/login
who-area

The who-area always consists of the last two terms of a web address that precede the first single "/" separated by a dot (in the above case, secuso.org). The whois is most important part of a web address and can be used to detect dangerous web addresses or messages with fraudulent links. It is called a domain. If the domain consists of numbers, it is a so-called IP address and most probably dangerous.

✗ https://129.13.152.9/secuso.org.secure-login.de/

By the way: nowadays criminals also use https.

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 of the KIT:

✓ https://www.s.kit.edu/it-security
✗ https://www.s-o-k.de/secure

Criminals replace the expected who-area domain in the web address to deceive you, e.g.

✓ https://www.my-parcelservice.de/
✗ https://www.my-parcelservice.de.online-shopping.de/
✗ https://www.online-shopping.de/my-parcelservice.de

Criminals register who-area domains that are very similar to the correct who-area domain with only a few characters difference:

✓ https://www.farmers-market-total.de/
✗ https://www.farmers-rnarket-total.de/
✗ https://www.farrners-market-total.de/
✗ https://www.farmrers-market-total.de/

5. Rule: Having identified the who-area in the web address, but you find you still cannot validate it, collect further information, e.g. by searching for the address in a search machine. If you are still unsure afterwards, please contact your IT appointee or contact via e-mail beratung-itsec@scc.kit.edu to assess the message together.

✓ https://www.secuso.org/
✗ https://www.secuso-research.org/

6. Rule: If the sender and contents of a message appear plausible and the message has an attachment, check whether this attachment has a potentially (very) dangerous file format. Potentially dangerous file formats are:

- File formats that can be executed directly (very dangerous):
  e.g. .exe, .bat, .com, .cmd, .scr, .pif
- Formats that may contain macros:
  e. g. Microsoft Office files, such as .doc, .docx, .ppt, .pptx, .xls, .xlsx
- File formats you do not know

7. Rule: If the file format is potentially (very) dangerous, open the attachment only if you expected precisely this attachment from the sender. If you are uncertain, collect further information. In no case use the contact details given in the message. For example, call the sender. Terminate the process for the time being.

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@scc.kit.edu to assess the message together.

Further Information

How to recognize fraudulent messages is explained in two videos:

To the videos:
s.kit.edu/it-security.fraudulent-messages.video

If you want to deepen your informationen on fraudulent messages from thes flyer, you are invited to join the NoPhish online training at ILIAS:

To the NoPhish online training:
s.kit.edu/it-security.fraudulent-messages.training

By the way: If you receive a lot of feedback that someone has received a message from you but you didn't send anyone, please contact your IT appointee of the business unit to analyse the situation and to discuss how to troubleshoot.