General Information

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

- Disseminating malware to, e.g., gain access to your devices or
- Deceiving you to obtain sensitive information (e.g., the access data to your bank account).

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.

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 asking you to transfer money or to call, e.g., fake cooperation/business partners or fake friends/family members. 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 goal of the fraud is to make 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. If you do log in, your access credentials will be stolen by the criminals. 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 goal is to make you open the dangerous file. By opening or executing it, you install malware 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 time, because you look at the message, assess it, and delete it.

Together against Fraudulent Messages

Many e-mail providers use technical measures to automatically detect fraudulent messages. These messages are not even delivered to you or disappear directly in the spam folder.

Unfortunately, with the existing measures it is not possible to discover all the fraudulent messages.

As attack strategies get better and better, many fraudulent messages are becoming harder to detect. Moreover, strict rules would detect fraudulent messages, but also legit ones coincidentally showing similar characteristics as the fraudulent messages.

Therefore, it is important that you check your messages carefully.

Here you will find general information about fraudulent messages as well as seven rules to detect them.

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, try to search the web for help and further actions you may now take, for example by searching for certain federal offices. For example, in Germany you can contact the BSI (Federal Office for Information Security) for advice.

By reacting quickly to fraudulent messages, you can help minimize the extent of the damage to you.

In the future, if you clearly detect a fraudulent message as such, then mark it as spam. This will help the automated measures to recognise similar ones in the future.

Contact

Institute of Applied Informatics and Formal Description Methods (AIFB)

Research Group Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gebäude 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-mail: secuso@aifb.kit.edu

secuso.aifb.kit.edu
twitter.com/secusoresearch

Editor

Karlsruhe Institute of Technology (KIT)

President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

The content of the brochure is based on findings obtained within the project

"KMU AWARE – Awareness im Mittelstand" carried out by the SECUSO research group of TU Darmstadt and promoted by the Federal Ministry for Economic Affairs and Energy under the initiative "IT-Sicherheit in der Wirtschaft" until March 31, 2018. The present brochure is financed within the KASTEL project funded by the Federal Ministry of Education and Research (BMBF).

Karlsruhe Institute of Technology

aifb

Identifying Fraudulent Messages

How to Detect Fraudulent and Phishing Messages

INSTITUTE OF APPLIED INFORMATICS AND FORMAL DESCRIPTION METHODS (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

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 with „yes", the more likely it is a phishing message. Particular care is required if you are asked for sensitive data, including passwords. KIT offices, including the SCC and local IT representatives, would not ask you to send them your password.

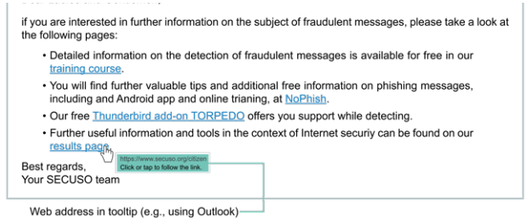
By the way: most of the above questions also work in the telephone, fax or post letter context.

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.

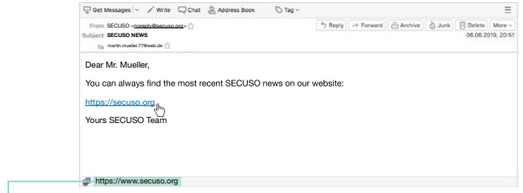
In most cases links are underlined and colored blue. However, links may also be integrated in the form of buttons or pictures.

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.



Web address in tooltip (e.g., using Outlook)



Web address in the status bar (e.g. using Thunderbird or web browser like Firefox, Edge, Chrome and Safari

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. In certain apps on Android devices, this window might be absent altogether and a long press might cause other functions or nothing at all. Take care not to click the link accidentally. If you are uncertain, wait until you are back at your PC or laptop.

Web address in the dialog window (iOS)

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://www.129.13.152.9/secuso.org.secure-login.com/

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.

✓ 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.

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. Terminate the process for the time being.

Further Information

How to recognize fraudulent messages is explained in three videos:

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

You can find further information on fraudulent messages and other cyber security topics here:

Further Info:
https://secuso.aifb.kit.edu/english/642.php

By the way: If you receive feedback that someone has received an email from you that you did not send at all, then you can also ask the BSI for advice.