General Information on Fraudulent Messages

Internet scammers use different strategies to harm you and/or your company. These strategies include, for example, the distribution of malware, or the deception of end users in order to access sensitive information (e. g., login details). A popular and widespread method is to send you fraudulent messages that will fool you into believing that there are legitimate reasons for sending you such messages. Fraudulent messages aimed at picking up sensitive information are called phishing messages. Fraudulent messages can be received via different channels e. g., as email, SMS, message via messenger or social networks. The contents of these messages can be dangerous in different ways:

Sensitive data: Messages will prompt you to send back sensitive data such as login details, confidential documents, or credit card details. These messages often involve a threat or a promise of a benefit to convince you to quickly and imprudently send sensitive data.

Bank Transfers/Calls: Messages will prompt you to make money transfers or phone calls e. g., to supposed friends or business partners. The scammer aims to make you pay him/her a certain amount of money. In this way, he or she will receive from you a direct bank transfer, or the amount in question will be charged to your next phone bill.

Links: Messages can contain one or more dangerous links. The aim of the fraud is to make you click on one of the links. These links then lead you, for example, to a real-looking but fraudulent website (also referred to as phishing site) to log in. Alternatively, you will be redirected to a website that will install malware on your device.

Attachments: Messages contain one or more dangerous files (such as an attachment in an email). The aim of the scammers is for you to open the attachment. By opening or executing the file, malware is installed on your device.

Contact

Karlsruhe Institute of Technology (KIT)

Institute for Applied Informatics and
Formal Description Methods (AIFB)

Research Group Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Bldg. 05.20
76133 Karlsruhe, Germany

Phone: +49 721 608 450 45
Email: kontakt@secuso.org

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

Issued by

Karlsruhe Institute of Technology (KIT)

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

The content of this flyer is based on findings from the project „KMU AWARE – Awareness im Mittelstand“ (awareness in small and medium-sized businesses), which was carried out by the SECUSO research group at TU Darmstadt and was funded by the Federal Ministry for Economic Affairs and Energy within the framework of the „Initiative IT-Sicherheit in der Wirtschaft“ (Initiative on IT security in business) until March 31, 2018.

Karlsruhe Institute of Technology

aifb

Fraudulent Messages

How to Recognize Fraudulent Messages, and Especially Phishing Messages

INSTITUTE OF APPLIED INFORMATICS AND FORMAL DESCRIPTION METHODS (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

The Following Rules will help you Recognize Fraudulent Messages

1st rule: Check the sender and content of each received message for plausibility: Does the sender match the message? Are sensitive data queried? Do you have a corresponding account at all? If the message is implausible, it most likely is a fraudulent message: Please delete it!

✗ In an email pretending to be from Amazon, the sender shop@sye.jp is not plausible.

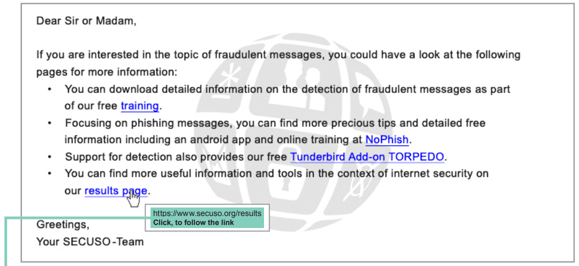
✓ In an Amazon email, the sender bill@amazon.com is plausible.

2nd rule: If the sender and content of a message are plausible and the message contains one or more links, please do not prematurely click on one of these links but find out whether the message could be a well-made scam where someone pretends to be the (supposed) sender.

A link can usually be identified by its text being blue and underlined. However, links can have various manifestations and may appear, for example, as buttons, words in diverse colors, or images.

Finding details on which address is actually behind a link depends on the respective device, software, and service (e. g., Amazon, Dropbox, Skype, WhatsApp, Facebook, Google+, Xing, LinkedIn). Before using a device, software, or service, you should therefore familiarize yourself with where to find the actual web address of a link.

In the case of laptops and PCs, the web addresses usually appear if you hover your mouse over the link without clicking on it. The link is displayed either in the status bar at the bottom of the window or in the info field, which is also referred to as tooltip.



Dear Sir or Madam,

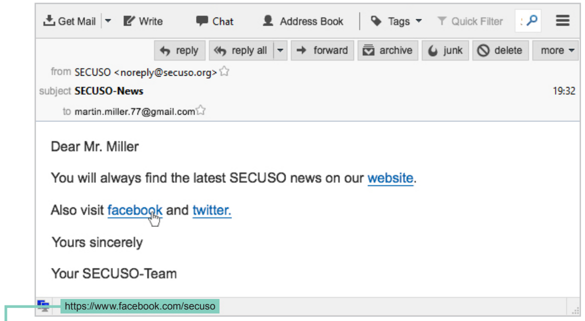
If you are interested in the topic of fraudulent messages, you could have a look at the following pages for more information:

- You can download detailed information on the detection of fraudulent messages as part of our free training.
- Focusing on phishing messages, you can find more precious tips and detailed free information including an android app and online training at NoPhish.
- Support for detection also provides our free Tunderbird Add-on TORPEDO.
- You can find more useful information and tools in the context of internet security on our results page.

https://www.secuso.org/results
Click, to follow the link

Greetings,
Your SECUSO-Team

Web address in the tooltip (e. g., in the case of Outlook)



from SECUSO <noreply@secuso.org>
subject **SECUSO-News** 19:32
to martin.miller.77@gmail.com

Dear Mr. Miller

You will always find the latest SECUSO news on our website.

Also visit facebook and twitter.

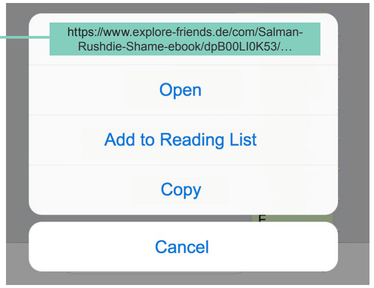
Yours sincerely

Your SECUSO-Team

https://www.facebook.com/secuso

Web address in the status bar (e. g., in the case of Thunderbird or web browsers such as Firefox, Internet Explorer, and Chrome)

In the case of mobile devices (smartphones and tablets), the procedure of identifying the web address of a link strongly depends on the device and the respective app. Usually, it suffices to hold your finger on the link for at least two seconds to make the web address appear in the dialog box. Please take care not to click on the link accidentally.



https://www.explore-friends.de/com/Salman-Rushdie-Shame-ebook/dpB00LI0K53/...

Web address in the dialog box (iOS operating system)

3rd rule: As soon as you have found the web address behind the link, please identify the so-called who area.

http://nophish.**secuso.org**/login

who area

The who area of a web address always consists of the last two terms separated by the dots before the first single "/" (in this case, secuso.org). It is the most important area for the identification of dangerous web addresses and, thus, of messages that contain dangerous links, and is also referred to as "domain". If the domain is made up of numbers, it is a so-called IP address, which is most likely a dangerous web address.

4th rule: As soon as you have identified the who area in the web address, please check whether it is related to the (alleged) sender and the content of the message and whether it is spelled correctly. If the sender or subject does not match the content, please do not click on the link.

✗ https://www.my-delivery-service.com.secure-shop.com/

✗ https://secure-shop.com/my-delivery-service.com/

✓ https://www.my-delivery-service.com/

✗ https://www.129.13.152.9/secure-shop.com/

✗ https://www.my-delivery-srevice.com/

✗ https://www.my-delivry-service.com/

✓ https://www.my-delivery-service.com/

5th rule: If you have identified the who area in the web address but cannot clearly judge it, you should gather further information e. g., by searching the address in a search engine. If you cannot classify the who area as trustworthy, delete the message!

✗ https://www.secuso-research.org/

✓ https://www.secuso.org/

6th rule: If the sender and content of a message are plausible and the message contains an attachment, make sure to check whether this attachment contains a potentially (very) dangerous file format. Potentially dangerous file formats are:

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

7th rule: If the file format is potentially (very) dangerous, make sure to open the attachment only if it is exactly the attachment you expected from the sender. If you are unsure whether you can simply delete the message, you should gather more information. Under no circumstances use the contact options provided in the message. Call the sender, for example.