

Identifying Fraudulent Messages incl. Phishing

1. Rule: Check the sender and the contents of every message for plausibility.

- ✓ The sender info@**secuso.org** for a SECUSO email
- ✗ The sender info@**sy.e.jp** for a SECUSO email

2. Rule: Familiarize yourself with the location of the actual web address behind a link (e.g. for PCs or laptops in the tooltip or the status bar).

3. Rule: Identify the who-area of the web address (bold and coloured).

[https://nophish.**secuso.org**/login](https://nophish.secuso.org/login)

4. Rule: Check, if the who-area matches the supposed legit message...and is written correctly.

- ✓ [https://www.**my-parcelservice.de**/](https://www.my-parcelservice.de/)
- ✗ [https://**s-o-k.de**/secure](https://s-o-k.de/secure)
- ✗ [https://www.my-parcelservice.de.**online-shopping.de**/](https://www.my-parcelservice.de.online-shopping.de/)
- ✗ [https://**online-shopping.de**/my-parcelservice.de/](https://online-shopping.de/my-parcelservice.de/)
- ✗ [https://**129.13.152.9**/my-parcelservice.de/](https://129.13.152.9/my-parcelservice.de/)
- ✓ [https://www.**farmers-market-total.de**/](https://www.farmers-market-total.de/)
- ✗ [https://www.**farners-market-total.de**/](https://www.farners-market-total.de/)
- ✗ [https://www.**farmres-market-total.de**/](https://www.farmres-market-total.de/)
- ✗ [https://www.**farmers-rmarket-total.de**/](https://www.farmers-rmarket-total.de/)

5. Rule: If you cannot assess the who-area, collect further information, e.g. by searching for the address using a search machine.

- ✓ [https://www.**secuso.org**/](https://www.secuso.org/)
- ✗ [https://www.**secuso-research.org**/](https://www.secuso-research.org/)

6. Rule: Check the file format of the attachment.

- ✗ Executable formats, e.g. .exe, .bat, .cmd
- ✗ Files including macros, e.g. Office files like .doc, .docx, .docm.

7. Rule: If you cannot clearly validate the attachment or if you are uncertain about receiving precisely this format from the sender, collect further information, e.g. by contacting the sender. Never use the contact details given in the message.