Don't give phishing mails a chance

THINK BEFORE YOU Click.Post.Type

Fraudsters use phishing to get your confidential data. These phishing e-mails resemble messages from your work colleagues, suppliers or customers and can look legitimate at first glance. In most cases, however, you will find evidence of fraudulent intent.

If you discover one of these indicators or are unsure, report the mail with the phishing button. If you have opened an attachment or clicked on a link, please contact your IT team immediately.

Date

- Was the e-mail sent at an unusual time (night / weekend)?

Recipient

- Was the e-mail sent to other recipients as well?
- Do you know the recipients?

Enclosure

- Do you expect a corresponding file?
- Does the file name seem trustworthy?
- Which file type is attached?
- Does the document contain macros? (Attention: Do not activate macros!)

External mail banner

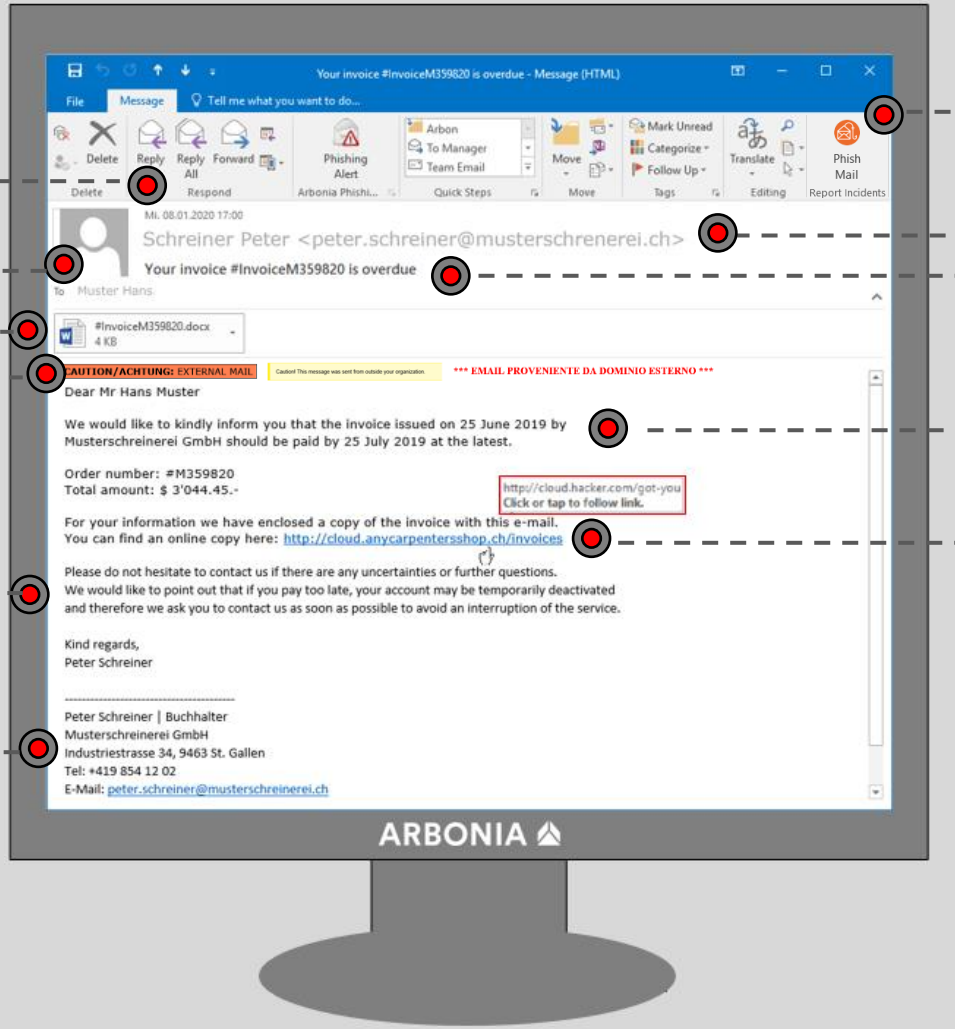
- Is the sender internal or external?
- If you see this text, the e-mail does not originate from our organization and you should exercise appropriate caution when clicking links, opening attachments, etc.

Contents

- Are you being urged to act quickly?
- Are you being threatened with consequences?
- Are you being asked for personal data?

Contents

- Does the signature look trustworthy?
- Is the phone number correct?
- Is the postcode correct?



Phishing Button

- The “phishing button” allows you to call attention to a possible threat with just a few clicks and provide your IT department with all necessary information.

Sender

- Do you know the sender?
- Is the content unusual?
- Is the e-mail address correct? **@musterschrenerei.ch**

Subject

- Does the subject match the content?
- Is it an answer to your inquiry?

Contents

- Does the text have spelling mistakes or incorrect grammar?

Hyperlinks

- Does the same hyperlink appear when you move the mouse over it? (Attention: Never click on it!) **http://cloud.hacker.com/got-you**
- Is the target address of the hyperlink correct?