Verify the credibility

Better safe, than sorry. See guide Spam, Phishing and Malware and Dealing with malware, spam, suspicious content

Be cautious, restrained, distrustful, safety is yours, next is only help.

Five steps to verify the credibility of the message

1. Verify the sender
2. Verify the URL (web link)
3. Verify the signature
4. Verify the content
5. Ask in doubt

Verify the real sender

- Everytime you receive any email, verify the true sender.
- Regardless of detecting email as a suspicious by the spamfilter.

How difficult it is and how to do it exactly depend on the email client. But shortly saying:

1. See the complete address in the form of somebody@somewhere.domain We do not allow outside sender to spoof @cerge-ei.cz domain.
2. In case of any doubt, doublecheck it by call or email ask.
3. Read the next articles as an example how to check real sender. The last article helps you to analyze the complete message path protocol, if you need it.
   Do not worry, it seems difficult, but in fact the quick proof can be simple. Is the header too complex, too long and with server addresses from outside of cerge-ei domain? Then it could not be the true cerge-ei message.

How to see the real email sender in Gmail

How to find the true sender in the message header

Verify the link

- Phishing often uses fake institutional pages, e.g. email login, internal web login, etc. The look could be fine, but the link goes elsewhere. Check link before you use it.
- Sometimes the cerge-ei domain is spoofed in the path to increase credibility. The complete path and the home domain at the end are decisive.
- There are also sophisticated techniques using a similar domain name (like a typo) or fonts where the letter looks correct but the name is actually different.

Verify the signature

- The signature is a significant indication of the trustworthiness of the message. Unknown, unusual or impersonal signature should be grounds for rejection or at least deep distrust.
- Unfortunately on the other hand, the signature could be easily stolen or spoofed. You must not fully rely on the authenticity of the signature.

Verify the content

- Check the style, language and content of the message. Beware of manipulative methods and social engineering.
- **Do not succumb a time pressure** Spam, Phishing and Malware

Ask in doubt

Feel free to ask if you have any doubts and/or to report a suspicious or dangerous email.