





















You can use this checklist both at work and at home. It helps you to actively prevent attacks on your data (and that of your colleagues). If you follow these recommendations, you make the most important contribution to IT security possible: **protecting your digital identity**.

**Tip:**

All official mailings sent out by IT-SERVICES are listed on the intranet: [swa.wu.ac.at/it-services-aussendungen](https://short.wu.ac.at/it-services-aussendungen)

Please check the overall impression you get from the message*	YES	NO
Is the sender's <b>email address familiar</b> to you?		
Do you <b>expect</b> to receive an email with this <b>subject line</b> or <b>subject matter</b> from the sender's address?		
Is a <b>generic salutation</b> used instead of a personal salutation? <i>E.g. Dear customer, Dear account holder, Hello, ...</i>		
Does the <b>language used</b> match the nationality of the sender or recipient? <i>E.g. English text or subject sent to/from a German-speaking recipient/sender</i>		
Does the message contain many <b>spelling or grammar mistakes</b> ?		
Does the email emphasize the <b>urgency of the matter</b> ? Does it describe or emphasize <b>unpleasant consequences</b> ?		
Are the facts or consequences described in the message <b>unusual or exaggerated</b> ?		
Are you asked to provide <b>internal university details or access data</b> ?		
Are you requested to <b>open a link</b> or URL?		
Does the email contain one or more <b>attached files</b> ? <b>Attention:</b> even common file formats can carry malicious code		

\* For phone calls, this checklist applies analogously to caller ID, the person calling, and the content of the conversation.

## Symbols

**Everyday communication**

Please be sure to follow our IT security recommendations: <https://short.wu.ac.at/safe-it>  
Thank you!

**Security risk!**

Use appropriate means to check whether the message really comes from the stated person or sender (e.g. website, helpdesk or service center, phone call, or personal inquiry).

**High security risk!**

- Delete the email message from the inbox **and** the trash folder.
- End the phone call immediately and tell the caller that you have to hang up due to reasons of information security.

**Oops! Your data have fallen into the wrong hands?**

- Please report any incidents and shortcomings or deficiencies regarding IT and information security to **hotline@wu.ac.at** as soon as possible.
- Keep all emails and other data after reporting an incident. Do not delete anything! Switch off the affected devices immediately and leave them deactivated.