

# PHISHING



95% of successful cyberattacks start with **phishing**

Therefore when you receive an email pay close attention to:

## Striking salutation



You are not mentioned by name in the salutation, but the mail does contain an "important" message. Or the mail does have a salutation, but this is different from what you are used to.

## Blurred sender

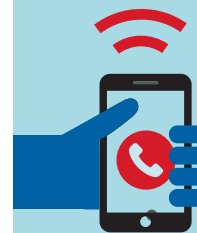
An unknown, vague or unclear email address.



## What to do if you don't trust the email:



Do not open links or files that you do not trust.



Do you know the person who has sent the mail? Call the person or organization and ask if the email actually comes from them.



## Unexpected attachment

An attachment that you're not expecting or that you receive from someone you do not know.



## Strange design and language

Striking use of language and strange design.

## Request for personal data

A request to 'check', 'update' or 'complete' your personal data.



## Prompt action requested

They ask you to respond quickly.



Send the mail with a short explanation to your company IT Security contact.



## Link to unknown website

Are there hyperlinks in the body of the email? View what a link refers to by moving your cursor over it. Make sure you don't click on the link! Do you still not trust it? Check with the sender.



Have you nevertheless clicked on a link or opened a file that you do not trust?

Please contact your local IT Security contact a.s.a.p.