HORNETSECURITY

HOW TO SPOT PHISHING
EMAILS AND BOGUS LINKS

HORNETSECURITY

HOW TO SPOT PHISHING
EMAILS AND BOGUS LINKS

Phishing emails can appear in our inboxes under the guise of a trustworthy sender or a plausible request, cleverly concealing their true intentions, namely to install malware on our computers or to get us to disclose access data through fake login pages.

How can we prevent this?

How can you spot phishing emails?

Outlined below are what you should look out for and the questions you must ask yourself if an email doesn't seem quite right.

- Verify the sender
  Has the email really been sent by your colleague in the neighboring department? Has the sender's address been written correctly? The smallest of discrepancies make a huge difference here.

  John.Doe@it-seal.de—correct
  Jane.Doe@it-sea1.de—incorrect

- Check the target domains before clicking any links
  Do you always display the link details? You often see "Click here" in emails. But where is "here" exactly? Where should the link take you? And even if the link details are shown in full, it's always worth a closer look.
  - Hover the cursor over the link—but do not click it. The (actual) target of the link is then displayed to you, e.g., next to the cursor or in the status bar of the email window. This also works for mobile devices. Tap the link, keeping it pressed for about two seconds.

- Check the "Who" part
  Do you recognize the link? Great! But does it really take you to the site of a well-known online retailer or electronics store? The "Who" part of the link tells you this.

This can be found surrounding the dot before the third "/" in the link address.

https://en.wikipedia.org/wiki/Main_Page

- Check the "Who" part of the link carefully.
  Cyber criminals exploit our lack of attention here and try to mislead us by making small additions, switching letters around or using similar letters and characters:

  https://en.wikipedia.org/ vs.

  https://en.wikipedia-en.org/

  https://bestbuy.com/ vs.

  https://beztbuy.com

  https://fedex.com vs.

  https://fedeks.com

Can you spot the difference?

If you're not sure whether the link will take you to the proper site, copy it into a search engine or test it using a specialist analysis site (e.g., virustotal.com). If you have any doubts, ask the sender of the email whether they sent it to check that the email and link are genuine.

- Be careful with attachments
  The following applies when handling email attachments:
  - Be careful and don't open anything without thinking first! Malware can get into your computer and the network through email attachments.
  - Only open attachments you are expecting.
  - Check with the sender if you are unsure.
- Caution: The contact details given for the sender in the email could also be fake! They might connect you to the criminal, who will, of course, assure you that everything is genuine. So, it's better to reach for the phone and call the purported sender on the number given in your address book.

Stay vigilant!