Recognize the scammail

The shortest

Security Awareness Training

RADIX MKB ICT

Don’t be naive about Cybersecurity

7 red flags

1. **Is the email WEIRD in any way?**
2. **Is it about money or about something of value?**
3. **Does it leverage fear, habit or greed?**
4. **Is it from a bank, authority or large company?**
5. **Does it have a (dangerous) link?**
6. **Does it have a (dangerous) attachment?**
7. **Why do I get this email?**

- **Authority** (the CEO, the police, bailiff, collection agency)
- **Large company** (Amazon, Telco, Microsoft, Office365)
- **Money / value** (Euro, bitcoin, giftcard, phonecard)
- **Fear** (Invoice, invoice reminder, fine)

NEVER use the login link and never just open the attachment

If in doubt, DO NOT click and just DELETE

Is the address of the sender 100% correct:

- Is there nothing added or changed with the emailaddress (letter or word) (1-> l or m -> rn)

Recognize the scamlink in the e-mail:

- **Hover** (place your mouse over the link without clicking). Then you will see the actual web address of the link appear.
- **Take a good look at the sender address**. Especially at the address between <>. If you don't see it, forward the mail (don’t send) and look at the **From** line in the text.

Distrust EVERY bank account number change request:

- Any email request for change of the bank account of an invoice or for salary payment is suspicious. Different fonts on an email invoice and stickers on a paper invoice is also suspect.

1. **Always call the company or person if you get a change request.**
   Do not change until you have spoken to the right person.

Even more

Security tips

5 password tips that reduce the chance of a hack by 99%:

- **Never log in via a link in an email.**
- Use multifactor authentication where possible.
- Always use a strong password
- Use a different password everywhere.
- Use a password manager to manage all passwords.

5 PC security tips for your home situation to think about:

- Always use a good anti-virus / anti-malware program.
- Update the PC and your applications regularly.
- Never download & install cracked software or freeware from an unknown site.
- Backup all files regularly. Disconnect backup afterwards from the PC.
- Never leave a laptop in your car, not even if on standby or powered off. Thieves can still detect them.

Also consider this:

- Be careful with free wifi. You never know who's watching. Never log into your email or bank account there. At least use a private VPN.
- Make regular backups of the photos on your phone. Those memories are irreplaceable.

Security wisdom:

- **If it is too good to be true, it probably is.**
- **Never believe a pityful or unlikely story. Do a check.**
- **Banks do not ask your login, to send them your bankcard or to transfer your money to a vault account because of fraud.**
- **Your customer does not suddenly have a new bank account number because they have problems with their old bank account.**
- **Your children / partner / friends do not have a new mobile number and just then ask you via Whatsapp to pay some bills.**

If in doubt, delete or check

Better safe than sorry