Erwin Hoffmann, FB 2
Frankfurt University of Applied Sciences

Task 1: Personal 'hacks' and threats

Most of us have already experiences in 'hacks': Spam mails, viruses and other malware is daily business in the Internet.

Let's consider these common cases:

a) Ransom Ware:
Is a program, which actually encrypts your PC's disk thus data become not accessible any more; except if some money is transfered to the source subject and a decryption key is send:

- `https://en.wikipedia.org/wiki/Ransomware`
- `https://www.theregister.co.uk/2018/01/16/us_hospital_ransomware_bitcoin/`
- `https://en.wikipedia.org/wiki/Emotet`

Which IT Security principal is violated here?

b) Identity Theft:
Somebody has access to your login accounts by guessing or extracting your personal keyword (*passphrase*).

- `https://twitter.com/hashtag/identitytheft`
- `https://www.heise.de/newsticker/meldung/Politiker-und-Promi-Hack-Ehemaliges-Twi`
  `html`

Is this issue part of the magical CIA triangle in IT Security?

c) Phishing:
In case somebody tries to contact you and are urged respond with immediate trust. Probably because the person contacting you seems to be familiar or originating from a trustful source. Rather, your identity becomes abused or your PC/Smartphone becomes infected, while either doing espionage or abusing your resources.

How is Phishing related to Identity theft?

d) Black Mailing:
Someone contacts you and pretends to have compromised material of you to be disclosed if you do not pay, for instance some amount in BitCoins ₿.

Check out the material for lecture 1 on Moodle. You will find:

- Some Blackmails as visible by the email client.
- The Blackmaisl in raw Internet mail format.
- In comparison: A raw email called 'Beacon.txt'.

i) How to tell, that the compromised material is never existing, thus you can certainly trash this email?
ii) How you you advice your mail client on the PC/Smartphone to display more information about the mail received?
iii) Check the 'Beacon.text' raw email. Is this phishing? How does the sender know, you've read the email?
iv) Since I have server high efficient Anti-Spam means in place, how does the Blackmail sender was able to overcome those systems?

Given these examples, compare now the standard 'magical IT security triangle' with my extension: the CAR principals.