What to do when information security is threatened?

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec TU Darmstadt

You should always report incidents and anomalies. You can find out the best way to do this here.

If you are unsure - better to ask once too much than too little.
We help you to classify and solve the threat!

TUDa-CERT

☏ **Emergency number:** +49 6151 16 27777
✉ **E-Mail:** cert@tu-darmstadt.de

⚠ Security problem

Detected vulnerability or threat without damage

- You have detected a phishing mail or you are unsure, but you have neither opened attachments nor clicked on links
- You receive a suspicious or a blackmail email

→ Forward with short comment to **phishing@tu-darmstadt.de**

- You send or receive a lot of spam
- You receive dubious calls and/or requests
- Something seems strange to you in general
- You have other questions

→ Message to **cert@tu-darmstadt.de**

Need for action
What you should do in such cases:

- Report
- Further actions are not required

⚠ IT security incident

Event with concrete damage effects

- You have clicked on a link or opened an attachment that is suspicious
- You have shared sensitive information
- You discover devices/objects that are unexpectedly in your premises (other computers, USB devices, cables, boxes, ...)
- Loss or theft of devices (e.g. laptops), data carriers (e.g. USB sticks) and documents

→ Message to **cert@tu-darmstadt.de**

Need for action
What you should do in such cases:

- Report
- Perform virus scan if necessary
- Change passwords (TU-ID password via IDM https://www.idm.tu-darmstadt.de)
- Inform any affected parties

⚠ IT security emergency

Security incident with serious, longer-term damage effects

- Finding malware on your device, unusual behavior of your device or your device stops working
- Files on your end device are or suddenly become encrypted
- You are acutely threatened or blackmailed, your data has suddenly disappeared
- Loss or theft of devices (e.g. laptops), data carriers (e.g. USB sticks) and documents containing confidential information
- Your IT behaves in a way that makes you fear for your data
- You suspect an acute danger for the IT of the TU-Darmstadt

→ Notification to **TUDa-CERT**
  - +49 6151 16 27777
  - cert@tu-darmstadt.de
→ Message to **responsible admin**

My personal admin contact:

Need for action
What you should do in such cases:

- Disconnect the affected device from the network
- Inform responsible admin and TUDa- CERT
- Do not continue working and wait for instructions

ATTENTION!
In case of imminent danger:
Contact us by phone or in person!