

Was tun, wenn die Informationssicherheit bedroht ist?



!InfoSec
TU Darmstadt

Grundsätzlich sollten Sie Vorfälle und Auffälligkeiten immer melden. Wie Sie dabei am besten vorgehen, erfahren Sie hier.

Wenn Sie sich unsicher sind – lieber einmal zu viel gefragt, als zu wenig.
Wir helfen Ihnen, die Bedrohung einzuordnen und zu lösen!

TUDa-CERT

☎ **Notfallnummer:** +49 6151 16 27777
✉ **E-Mail:** cert@tu-darmstadt.de

! Sicherheitsproblem

Erkannte Schwachstelle oder Bedrohung ohne Schaden

- Sie haben eine Phishing Mail erkannt oder Sie sind sich unsicher, haben aber weder Anhänge geöffnet, noch auf Links geklickt
- Sie erhalten eine verdächtige oder eine Erpresser-E-Mail
- Sie versenden oder erhalten viel Spam
- Sie erhalten dubiose Anrufe und/oder Anfragen
- Ihnen kommt generell etwas merkwürdig vor
- Sie haben sonstige Fragen

→ Mit kurzem Kommentar weiterleiten an **phishing@tu-darmstadt.de**

→ Meldung an **cert@tu-darmstadt.de**

Handlungsbedarf

Was Sie in solchen Fällen tun sollten:

- Melden
- Weitere Aktionen sind nicht erforderlich

! IT-Sicherheitsvorfall

Ereignis mit konkreten Schadensauswirkungen

- Sie haben auf einen Link geklickt oder einen Anhang geöffnet, der verdächtig ist
- Sie haben sensible Informationen mitgeteilt
- Sie entdecken Geräte/Gegenstände, die unerwartet in Ihren Räumlichkeiten sind (andere Computer, USB-Geräte, Kabel, Boxen...)
- Verlust oder Diebstahl von Geräten (z.B. Laptops), Datenträgern (z.B. USB-Sticks) und Dokumenten

→ Meldung an **cert@tu-darmstadt.de**

Handlungsbedarf

Was Sie in solchen Fällen tun sollten:

- Melden
- Ggf. Virenscan durchführen
- Passwörter ändern (TU-ID Passwort via IDM <https://www.idm.tu-darmstadt.de>)
- Etwaige Betroffene informieren

! IT-Sicherheitsnotfall

Sicherheitsvorfall mit schwerwiegenden, längerfristigen Schadensauswirkungen

- Fund von Schadprogrammen auf Ihrem Gerät, unübliches Verhalten Ihres Geräts oder ihr Gerät funktioniert nicht mehr
- Dateien auf Ihrem Endgerät sind oder werden plötzlich verschlüsselt
- Sie werden akut bedroht oder erpresst, Ihre Daten sind plötzlich verschwunden
- Verlust oder Diebstahl von Geräten (z.B. Laptops), Datenträgern (z.B. USB-Sticks) und Dokumenten mit vertraulichen Informationen
- Ihre IT verhält sich so, dass Sie Angst um Ihre Daten haben
- Sie vermuten eine akute Gefahr für die IT der TU-Darmstadt

→ Meldung an **TUDa-CERT**

- +49 6151 16 27777
- cert@tu-darmstadt.de

→ Meldung an **zuständige:n Admin**

Mein persönlicher Kontakt:

Handlungsbedarf

Was Sie in solchen Fällen tun sollten:

- Betroffenes Gerät vom Netz trennen
- Zuständige:n Admin und TUDa-CERT informieren
- Nicht weiterarbeiten und auf Instruktionen warten

ACHTUNG!

Bei Gefahr in Verzug: Kontaktaufnahme per Telefon oder persönlich!