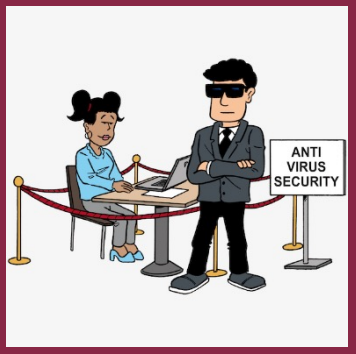
DIE ZEHN GOLDENEN REGELN DER IT-SICHERHEIT



→ **MEDIEN- UND INFORMATIONSZENTRUM (MIZ)**

LEUPHANA
UNIVERSITÄT LÜNEBURG

DIE 4. GOLDENE REGEL DER IT-SICHERHEIT:

SEI SORGSAM IM UMGANG MIT E-MAILS!

„ICH FALLE NICHT AUF PHISHING-MAILS REIN!“ **ODER DOCH…?**

- Im Sommer führte das MIZ zur Sensibilisierung für IT-Sicherheit eine **Phishing-Simulation** durch
- Bis 08.09. hatten **14,2 %** der Empfänger*innen auf mindestens einen der versandten Phishing-Links geklickt
- Eine der E-Mails hatte sogar eine Klickrate von **25,4 %**!

Wie gut erkennen wir Phishing-Versuche also wirklich?

GÄNGIGE FEHLER
WAS MAN NICHT TUN SOLLTE…

- Darauf vertrauen, dass der **angezeigte Absender** auch immer die tatsächliche Person ist, mit der man kommuniziert
- Den **Inhalt** jeder Mail für bare Münze nehmen, auch, wenn man den Vorgang, der angesprochen wird, eigentlich gar nicht zuordnen kann
- **Links und Anhänge** ungeprüft anklicken und öffnen
- **Grafiken** in E-Mails standardmäßig anzeigen lassen, weil die Mails dann besser aussehen
- Dienstliche E-Mails mit einem **privaten Gerät** (PC, Smartphone, Tablet etc.) abrufen
- Dienstliche E-Mails an das **private Postfach** weiterleiten oder durch den privaten E-Mail-Anbieter (z. B. Gmail) abrufen lassen
- **Sensible Daten** wie Passwörter oder Personendaten **unverschlüsselt** versenden

DIE CHECKLISTE
PHISHING-MAIL – JA ODER NEIN?

- ✓ Kommt die Mail wirklich von dem*der vermeintlichen **Absender*in**?
- ✓ Wurde die E-Mail **digital signiert**?
- ✓ Ist es **nachvollziehbar/wahrscheinlich**, dass die angegebene Person Ihnen schreibt?
- ✓ Ist Ihnen die **Angelegenheit**, zu der geschrieben wird, bekannt?
- ✓ Wird ein **Schreckensszenario** angekündigt und sollen Sie zu einer schnellen Handlung, z. B. der Eingabe Ihrer Zugangsdaten oder einer PIN, gedrängt werden? Oder sollen Sie etwas für jemanden **kaufen**?
- ✓ Gibt es **Auffälligkeiten** wie kuriose Rechtschreib- und Grammatikfehler oder ist der **Stil** der Mail seltsam?
- ✓ Werden Sie **namentlich** angesprochen oder nur sehr generisch?

NICHT NUR FÜR DIE WORK-LIFE-BALANCE GUT **DIENSTLICHES UND PRIVATES NICHT MISCHEN!**

- Rufen Sie Ihre dienstlichen E-Mails nicht **mit privaten Geräten** ab!
- **Leiten** Sie dienstliche Mails nicht automatisiert **an Ihr privates Postfach weiter** und rufen Sie sie auch nie über einen **Sammeldienst** o. ä. Ihres privaten E-Mail-Anbieters (z. B. Gmail) ab!

Ansonsten gefährdet eine Kompromittierung privater Geräte auch das Uni-Netz (oder umgekehrt)!

(NICHT) NUR FÜR SENSIBLE DATEN UNVERZICHTBAR **E-MAIL-VERSCHLÜSSELUNG**

- Versenden Sie so viele Ihrer E-Mails wie möglich **verschlüsselt**!
- Das MIZ bietet allen Mitarbeitenden **kostenlose digitale Zertifikate** für das Signieren und Verschlüsseln von E-Mails an. Wie Sie ein solches Zertifikat bekommen, und, wie Sie damit verschlüsselte Mails versenden und empfangen, erfahren Sie hier: https://go.leuphana.de/verschluesselung

LEIDER NICHT DER STANDARD
E-MAIL-VERSCHLÜSSELUNG

- Signierter und verschlüsselter Mailverkehr ist leider immer noch die **Ausnahme** und längst nicht die Regel!
- Zudem existieren **zwei** konkurrierende, miteinander nicht kompatible, Verschlüsselungsverfahren: **S/MIME** und **PGP**
    - Die Leuphana verwendet S/MIME
- An der Leuphana ist verschlüsselte Kommunikation möglich, aber **nur wenige Privatpersonen und andere Institutionen** verwenden überhaupt E-Mail-Verschlüsselung.

Seien Sie in der Kommunikation mit Externen besonders vorsichtig und verschicken sie sensible Daten nie unverschlüsselt per Mail!

KONTAKT

WENDEN SIE SICH BEI ALLEN FRAGEN RUND UM DAS THEMA IT-SICHERHEIT AN DEN IT-SERVICE!

IT-SERVICE
Hotline 04131.677-1212
it-service@leuphana.de
Service-Counter: C7.004

Öffnungszeiten: www.leuphana.de/services/miz/service-support/it-support.html

NOCH MEHR GOLDENE REGELN DER IT-SICHERHEIT?

www.leuphana.de/it-sicherheit