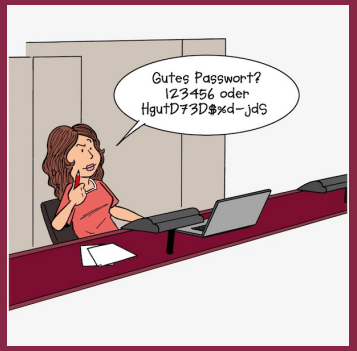
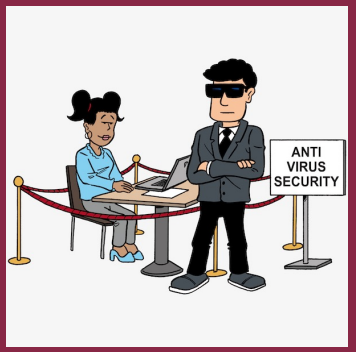
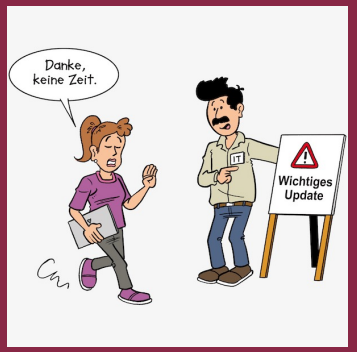
DIE ZEHN GOLDENEN REGELN DER IT-SICHERHEIT







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

LEUPHANA
UNIVERSITÄT LÜNEBURG

DIE 1. GOLDENE REGEL DER IT-SICHERHEIT:

DEIN PASSWORT GEHT NUR DICH ETWAS AN!

GÄNGIGE FEHLER
WAS MAN NICHT TUN SOLLTE…

- Passwörter auf einen **Zettel** schreiben, der dann am Bildschirm, unter der Tastatur oder in der Schreibtischschublade landet
- **Identische** Passwörter für verschiedene Dienste nutzen
- Passwörter **unverschlüsselt weitergeben** – z. B. per E-Mail oder Messenger, über ein geteiltes Laufwerk oder die Cloud
- Passwörter **unverschlüsselt** (z. B. in einer Word-Datei oder Excel-Liste) **speichern**
- Dienstliche Passwörter auf **privaten Geräten** (z. B. im Browser auf dem Privat-Laptop) speichern oder umgekehrt
- Passwörter **leichtfertig** auf x-beliebigen Websites eingeben
- Passwörter für **persönliche Accounts** an Kolleg*innen oder studentische Hilfskräfte **weitergeben**
- Passwörter **an den IT-Service weitergeben** – wir brauchen Ihre Zugangsdaten nicht und werden Sie niemals danach fragen

UNSERE EMPFEHLUNGEN

Teilen Sie **niemals** die Zugangsdaten Ihrer persönlichen Accounts (insbesondere des Leuphana-Accounts) mit anderen Personen – auch dann nicht, wenn Sie in einem direkten dienstlichen Verhältnis zueinander stehen (z. B. Lehrende und Sekretariate oder SHKs)!

Wenn das MIZ eine nicht autorisierte Weitergabe von Zugangsdaten feststellt, sind wir verpflichtet, den Account als **kompromittiert** zu betrachten, zu sperren und ggf. weitere Schritte einzuleiten!

UNSERE EMPFEHLUNGEN
PASSWÖRTER SICHER TEILEN

Wenn Sie Passwörter, bspw. für Funktions-Accounts oder Forschungsprojekte, mit Kolleg*innen teilen müssen, verwenden Sie **sichere Wege**!

Zum Beispiel:

- einen gemeinsam genutzten **Passwort-Manager**
- eine gemeinsam genutzte, selbst passwortgeschützte, **Datei**, deren Passwort Sie nur persönlich weitergeben
- eine **verschlüsselte** E-Mail (nicht optimal, aber besser als nichts)

UNSERE EMPFEHLUNGEN
PASSWORT-MANAGER

Passwort-Manager können helfen, die wachsende Zahl von Passwörtern zu meistern – Sie müssen sich nur noch das Passwort des Passwort-Managers merken!

Vom MIZ empfohlen:

- KeePass (für Windows)
- KeePassXC (für macOS (und Windows, Linux))

💡 **Anleitungen im Wiki unter „IT-Sicherheit“ > „KeePass Kennwort-Datenbank“**

UNSERE EMPFEHLUNGEN
PASSWORT-MANAGER

Auch die Passwort-Speicher-Funktion von **Webbrowsern** ist ein (sehr einfacher) Passwortmanager, aber in der Regel:

- fehlender eigener Passwortschutz
- keine Synchronisation → Verlust der Passwörter bei Defekt, Verlust, Gerätewechsel

→Besser als nichts, aber ein vollwertiger Passwort-Manager ist empfehlenswerter!

UNSERE EMPFEHLUNGEN
MFA UND 2FA

Nutzen Sie **Multi-Faktor-Authentifizierung (MFA)** bzw.
Zwei-Faktor-Authentifizierung (2FA)!

Zusätzlich zum Passwort wird dann ein weiterer Faktor für den Login benötigt, z. B.:

- Einmal-**Zahlencode** (OTP)
- Bestätigung einer **Push-Benachrichtigung** auf dem Mobilgerät
- **Biometrisches** Merkmal (Fingerabdruck, Face ID)

Bekannt z. B. aus dem Online-Banking oder beim Online-Shoppen mit Kreditkarte.

⏳ **Einführung von MFA für die meisten Leuphana-Dienste erfolgt bald!**

UNSERE EMPFEHLUNGEN
WENN ES WIRKLICH MAL PAPIER SEIN MUSS…

Möchten/müssen Sie Ihre Passwörter auch auf Papier dokumentieren, legen Sie sie ausschließlich an einem **abschließbaren** Ort ab, auf den **nur Sie** Zugriff haben!

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