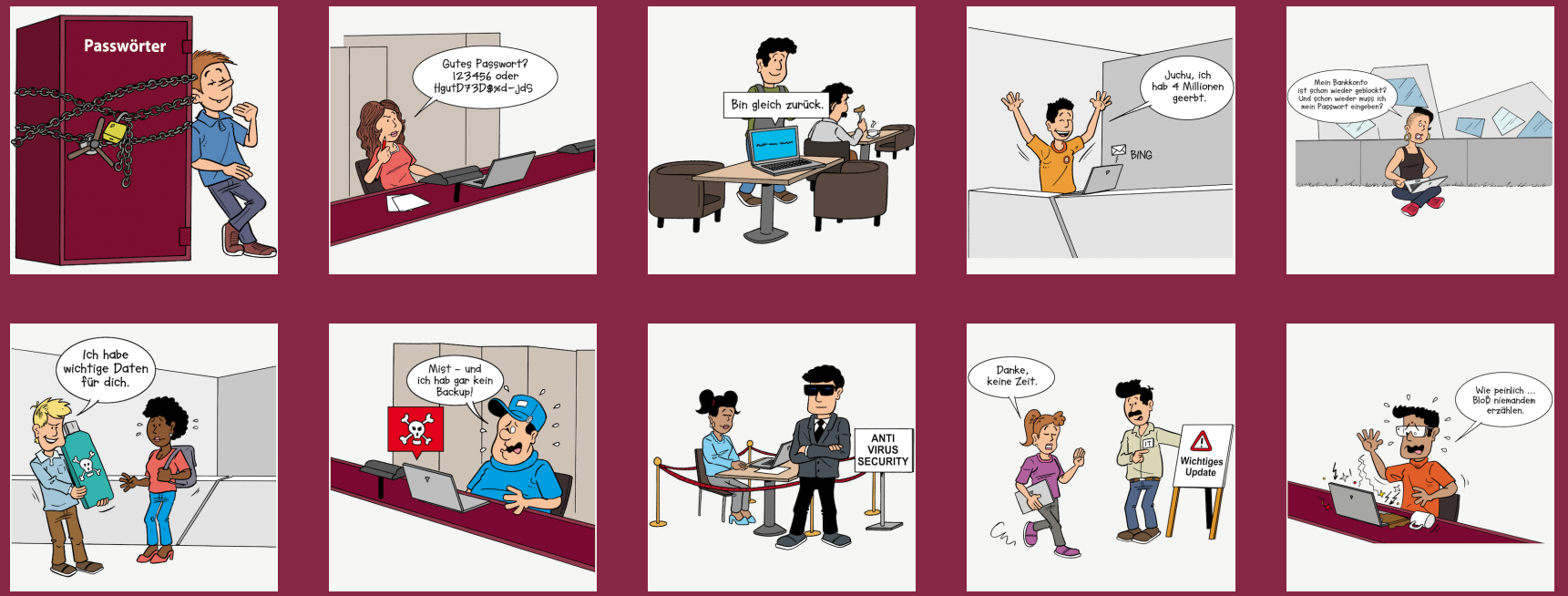
DIE ZEHN GOLDENEN REGELN DER IT-SICHERHEIT



MEDIEN- UND INFORMATIONSZENTRUM (MIZ)

LEUPHANA
UNIVERSITÄT LÜNEBURG

DIE ACHTE GOLDENE REGEL DER IT-SICHERHEIT:

SCHÜTZE DICH VOR VIREN UND WÜRMERN!

GÄNGIGE FEHLER
WAS MAN NICHT TUN SOLLTE

- Einen Computer **ohne Virenschutzsoftware** betreiben
- Bedenkenlos auf Links und Anhänge in **E-Mails** klicken
- Unbedacht beliebige **Internetseiten** aufrufen und von dort **Software** herunterladen
- Sorglos mit **Wechselmedien** wie USB-Sticks, externen Festplatten oder CDs Dateien zwischen Computern hin- und herschieben
- Den Befall eines Dienstrechners mit Schadsoftware **selbst zu lösen** versuchen und nicht dem IT-Service melden

VON HAUS AUS SICHER
DIE ENDPOINT-SECURITY-LÖSUNG SENTINELONE

Betreiben Sie Ihren Computer grundsätzlich mit einer seriösen und aktuellen Virenschutzsoftware!

- Wenn Ihr Dienstrechner vom IT-Service betreut wird (Regelfall), ist darauf automatisch die Schutzsoftware **SentinelOne** installiert
  - Logo in der Taskleiste/Menüleiste: 

SENTINELONE IST BEI IHNEN NOCH NICHT INSTALLIERT? **DANN ABER GANZ SCHNELL!**

SentinelOne hat im Sommer 2023 die vorher genutzte Software Sophos Endpoint Protection abgelöst. Bei allen vom IT-Service administrierten Computern erfolgte die Umstellung zentral.

- Sie sehen kein SentinelOne-Logo in Ihrer Taskleiste/Menüleiste? 
- Oder Sie sehen noch das Sophos-Logo? 

⚠ Wenden Sie sich bitte baldmöglichst an den IT-Service!

HAND IN HAND GELINGT'S AM BESTEN
SCHUTZSOFTWARE + IT-SICHERHEITS-BEWUSSTSEIN = 😎

Erinnern Sie sich an die vorherigen goldenen Regeln der IT-Sicherheit!

- 4. Regel: Sei sorgsam im Umgang mit E-Mails!
- 5. Regel: Surfe mit Umsicht und Verstand!
- 6. Regel: Vorsicht vor USB-Stick, CD & Co.!

UND, WENN ES DOCH EINMAL PASSIERT…?

„MEIN COMPUTER VERHÄLT SICH KOMISCH“
ANZEICHEN FÜR EINEN SCHADSOFTWARE-BEFALL

- Meldungen durch **Schutzprogramme** wie SentinelOne
- Unerklärliche **Fehlermeldungen**
- Unvermuteter Start oder plötzlicher Absturz von **Programmen**
- Unbekannte Dienste oder Funktionen fordern **Administratorzugriff** an
- Versand von **E-Mails** in Ihrem Namen ohne eine Aktion Ihrerseits
- Verschwinden von oder unerklärliche Veränderungen an **Dateien** (Name, Inhalt, Größe, Icon)
- Kein Zugriff auf einzelne **Laufwerke**
- Probleme beim **Abspeichern** von Dateien oder Daten von Fachanwendungen
- Ungewöhnlich hoher **Ressourcenverbrauch** (z. B.: der Computer ist auffallend langsam)

NICHT WARTEN – SICHERHEITSVORFALL MELDEN!

SCHON IM VERDACHTSFALL
SICHERHEITSVORFALL MELDEN

Bewahren Sie Ruhe!

Melden Sie **jeden** Verdacht auf einen Schadsoftware-Befall **sofort** **telefonisch oder persönlich** an den **IT-Service**: 📞 -1212 | 👨‍💼 C7.004 | Details und Servicezeiten: www.leuphana.de/it-service

Bitte halten Sie folgende Informationen bereit:

- Welches Betriebssystem nutzen Sie?
- Mit welchem Account sind Sie auf dem Rechner eingeloggt!
- Gibt es noch andere Personen, die diesen Rechner benutzen?
- Welchen Virenscanner nutzen Sie (i. d. R. SentinelOne)?

WEITERE SCHRITTE
SCHADENSBEGRENZUNG

Befolgen Sie zudem folgende Schritte:

- **Mit dem betroffenen Endgerät oder der Anwendung darf nicht weitergearbeitet werden!**
- Ziehen Sie das **Netzwerkkabel** bzw. deaktivieren Sie das **WLAN**.
- Haben Sie den Verdacht, dass die Schadsoftware ein IT-System befallen hat, auf dem eine von Ihnen genutzte **Fachanwendung** bereitgestellt wird, darf diese nicht weiter genutzt werden! Melden Sie sich bitte sofort von der Fachanwendung ab.
- Können Sie die Schadsoftware auf einen **Datenträger** im Ihren Besitz zurückführen, darf dieser nicht weiter verwendet werden oder an andere Anwender*innen weitergegeben werden. Geben Sie den Datenträger bitte sofort beim IT-Service bzw. den IT-Tutor*innen ab.
- Wenn noch **andere Anwender*innen** auf Ihr Endgerät zugreifen, warnen Sie diese, dass ein Verdacht auf einen Schadsoftware-Befall besteht.
- Setzen Sie Ihre Arbeit mit dem mutmaßlich befallenen Endgerät oder der Fachanwendung erst fort, wenn Ihnen das MIZ bestätigt hat, dass die **Bereinigung des IT-Systems abgeschlossen** ist und ändern Sie dann sofort Ihr Anmeldekennwort (bei Dienstrechnern bzw. Fachanwendungen).

LEIDER OFT INKLUSIVE **DATENSCHUTZVORFALL MELDEN**

Besteht bei dem Befall die **Gefahr**/der **Verdacht**, dass dienstliche Daten unberechtigterweise mit Dritten geteilt werden? Dann kann es sich zusätzlich um einen **Datenschutzvorfall** handeln!

Bitte nehmen Sie **zusätzlich** zu der Meldung an den IT-Service mit dem **Datenschutzmanagement** auf!

Details: www.leuphana.de/intranet/datenschutz

Beispiele für mögliche Datenschutzvorfälle:

- Nicht autorisierte **Nutzung** eines Computers durch einen Dritten – ob vor Ort oder übers Netz
- Verlust von oder nicht autorisierter Zugriff Dritter auf **Datenträger**, **Akten** oder andere **Unterlagen** mit personenbezogenen Daten
- **Verlust** oder unbeabsichtigter bzw. unberechtigter **Versand** oder **Upload** von Dateien, Präsentationen, Fotos etc.

DON'T PANIC

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/it-service

NOCH MEHR GOLDENE REGELN DER IT-SICHERHEIT?

www.leuphana.de/it-sicherheit