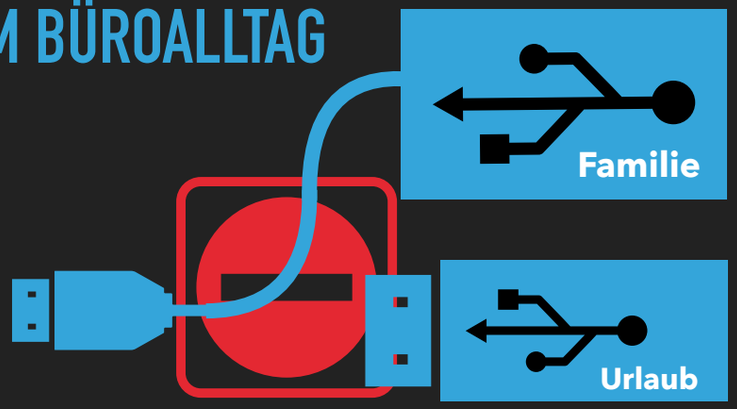
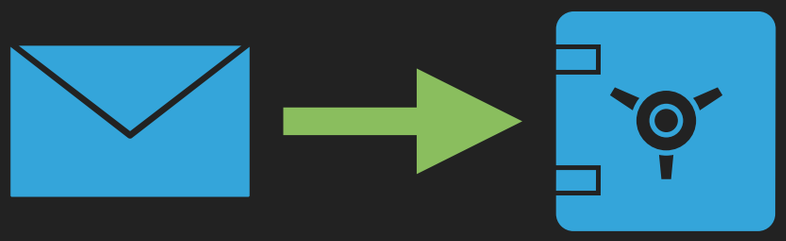
SICHERHEITSREGELN IM BÜROALLTAG



- Keine privaten Speichermedien an dienstlichen Geräten verwenden
- Sorgsamer Umgang mit sensiblen Informationen

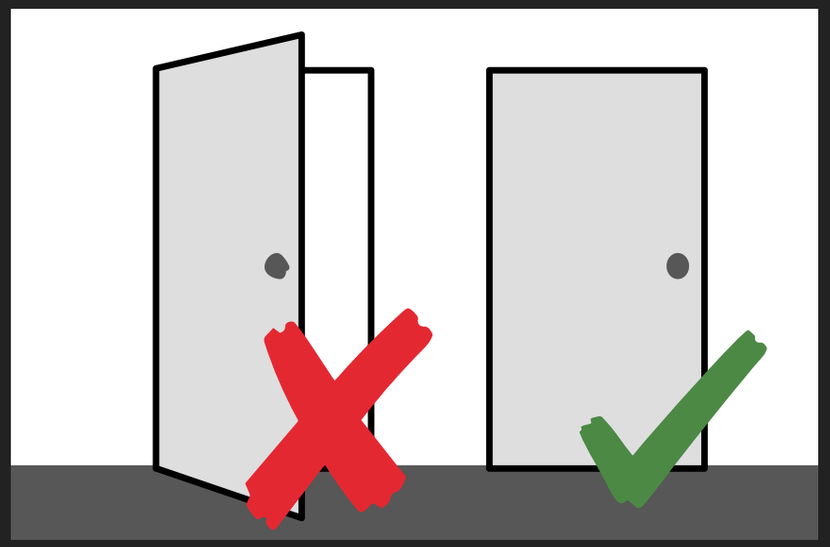


- Passwörter nicht sichtbar herumliegen lassen
- Internetnutzung nur
  a) dienstlich und nicht privat
  b) mit dienstlichen Endgeräten
  c) mit der gebotenen Sorgfalt

BEIM VERLASSEN DES ARBEITSPLATZES IMMER

1. Bildschirm sperren

2. Tür abschließen



3. Fenster schließen

WIE SCHÜTZE ICH MICH?

Awareness-Veranstaltung

von Dr. Christoph Eilenbrock

und Michael Gerdes

INHALTE

- Wie schütze ich mich? (Arbeitsplatz)
- Live-Hacking (USB)
- Wie schütze ich mich? (Büroalltag)
- Live-Hacking (WLAN)
- Wie schütze ich mich? (Best Practices)
- Live-Hacking (QR-Codes)

E-MAILS

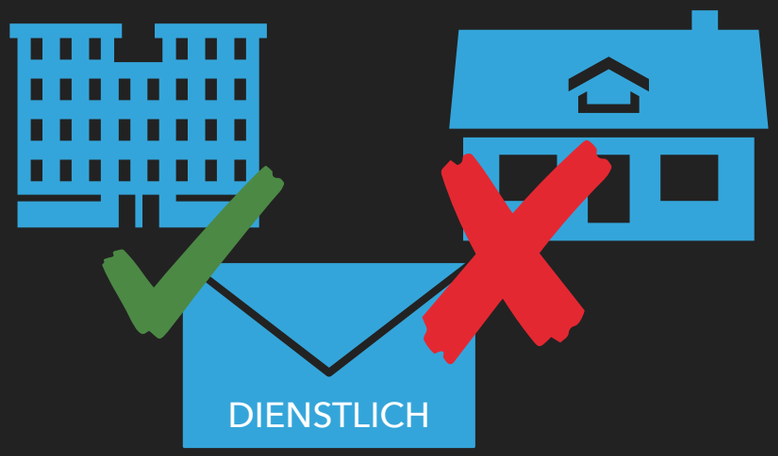
3-Punkte-Check des BSI:

1. Ist der **Absender** bekannt?
2. Ist der **Betreff** sinnvoll?
3. Wird ein **Anhang** von diesem Absender erwartet?

– – –

Weitere Hinweise:

- Kein privat-dienstlicher Austausch von E-Mails



WLAN-SICHERHEIT

- Fremde WLANs ≠ vertrauenswürdig
- Nach Nutzungsende entfernen / ignorieren

PASSWORTSICHERHEIT

- Sicher = lang + viele Zeichenarten (Groß- + Kleinbuchstaben + Zahlen + Sonderzeichen)
- Merksatz als Passwort oder als Hilfe einprägen

ALEIPM4Z+EK!

= Am liebsten esse ich Pizza mit 4 Zutaten und extra Käse!

- Keine Mehrfachverwendung

USB-SICHERHEIT

- Für Übertragungen immer den eigenen USB-Stick verwenden.

Wichtige Links zum Merken:

https://haveibeenpwned.com

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

DIE BESTE INFORMATIONSQUELLE SIND LEUTE, DIE VERSPROCHEN HABEN, NICHTS WEITERZUERZÄHLEN.

MARCEL MART

FRANZÖSISCHER SCHRIFTSTELLER (*1948)