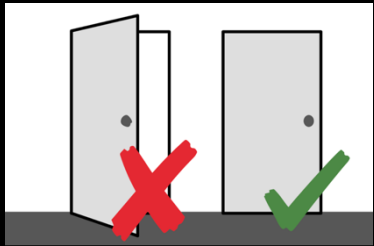


BEIM VERLASSEN DES ARBEITSPLATZES IMMER

1. Bildschirm sperren



2. Tür abschließen

3. Fenster schließen

Wichtige Links zum Merken:

- **Waren Sie bereits Opfer von Cyberkriminalität?**
<https://haveibeenpwned.com>
- **Testen Sie sich selbst im Phishing Quiz von Google:**
<https://phishingquiz.withgoogle.com>
- **Weitere Informationen und Empfehlungen des BSI unter:**
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)

🌐 <https://wie-schuetze-ich-mich.de/>
✉ kontakt@wie-schuetze-ich-mich.de



WIE SCHÜTZE ICH MICH?

Awareness-Veranstaltung
von Dr. Christoph Eilenbrock
und Michael Gerdes

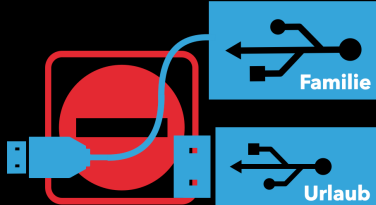
INHALTE

Ziel der Veranstaltung ist es, ein allgemeines Bewusstsein für die Bedrohungen und Risiken der Informationssicherheit im Büroalltag wie auch privat zu schaffen:

- 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)

ALLGEMEINE SICHERHEITSREGELN IM BÜROALLTAG

- Sorgsamer Umgang mit sensiblen Informationen
- Passwörter **nicht** offen ablegen

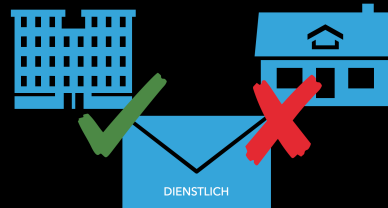


- **Keine** privaten Speichermedien an dienstlichen Geräten verwenden

- **Internet- und E-Mailnutzung** nur
 - a) dienstlich und niemals zu privaten Zwecken,
 - b) mit dienstlich bereitgestellten Endgeräten,
 - c) mit der gebotenen Sorgfalt!



- **Kein** privat-dienstlicher Austausch von E-Mails



- **IT-Geräte schützen** vor
 - unbefugtem Zugriff bei Nichtnutzung
 - unbefugter Einsichtnahme durch Dritte bei Benutzung
- Sicherheitsmerkmal (Token) und IT-Gerät getrennt aufbewahren
- Immer den eigenen **USB-Stick** verwenden!



WLAN-Sicherheit

- Fremde WLAN ≠ vertrauenswürdig
- Nach Nutzung entfernen / ignorieren

3-Punkte-Check des BSI für E-Mails



1. Ist die **Absender-E-Mail-Adresse** bekannt?
2. Sind der **Betreff** und der Text sinnvoll?
3. Wird ein **Link** / **Anhang** erwartet?

PASSWORTSICHERHEIT

- **Sicher** = lang (10-12 Zeichen) + viele Zeichenarten (Groß- + Kleinbuchstaben + Zahlen + Sonderzeichen)
- **Tipp:** Verwenden Sie einen kompletten Satz als Passwort oder prägen Sie ihn sich zumindest als Hilfestellung ein:



AleiPm4Z+eK!

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

Bleiben Sie misstrauisch!