

DIE SIEBEN TODSÜNDEN DER IT-SICHERHEIT

Helfen Sie, Ihren Arbeitsplatz und Ihre Geräte sicher und schadfrei zu halten, indem Sie diese sieben Todsünden vermeiden – kleine Fehler, die schnell zu ernsthaften Sicherheitsproblemen werden können.



1 FREMDE DATENTRÄGER

USB-Sticks und andere Datenträger können mit Schadprogrammen infiziert sein, die sich beim Anschluss an das eigene Gerät in der Akademie verbreiten können.



2 E-MAIL- ANHÄNGE

Über infizierte Anhänge in E-Mails oder über Links auf vermeintlich legitime Websites verschaffen sich Angreifer Zugriff auf Geräte und Daten des Opfers.



3 GLEICHE PASSWÖRTER

Wenn das Opfer eines Account-Hacks dasselbe Passwort für mehrere verschiedene Accounts verwendet, lässt sich der Schaden viel schwerer begrenzen.



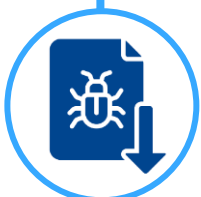
4 UNGESICHERTER ARBEITSPLATZ

Wenn Büros bei Abwesenheit nicht verschlossen werden, könnten Geräte entwendet werden. Bei nicht gesperrten Bildschirmen bekommen ggf. Unbefugte Einsicht in vertrauliche Daten.



5 VERMISCHUNG PRIVAT/ARBEIT

Private Daten können Einfallstore für Angriffe sein. Bei der Kommunikation über private E-Mail-Adressen kann nicht derselbe Schutz wie bei der Dienstadresse gewährleistet werden.



6 UNSERIÖSE DOWNLOADQUELLEN

Wer auf den erstbesten Downloadlink für z.B. eine Installationsdatei klickt, läuft Gefahr, unbemerkt auch andere Programme zu installieren (Bloatware, Adware, Würmer).



7 VERSCHWEIGEN VON VORFÄLLEN

Wenn (besonders selbstverschuldete) Sicherheitsvorfälle nicht möglichst schnell der IT mitgeteilt werden, wird der verursachte Schaden schnell noch größer.

Informieren Sie sich über Informationssicherheit und Maßnahmen zum Schutz Ihres Arbeitsplatzes über die [Handreichung Informationssicherheit](#) für Beschäftigte der Akademie.

Haben Sie noch Fragen? Kontaktieren Sie unsere [EDV-Abteilung](#) unter (0 62 21) 54 33 54

