D64

Zentrum für
Digitalen Fortschritt

D64 ist das Zentrum für digitalen Fortschritt. Wir begreifen die digitale Transformation als große Chance, das Miteinander unserer Gesellschaft zu verbessern. Die soziale, ökologische, technologische und politische Entwicklung wollen wir konstruktiv, kritisch und kreativ mitgestalten. Unser Ziel ist es, die Grundwerte Freiheit, Gerechtigkeit und Solidarität durch eine progressive Digitalpolitik zu verwirklichen. Jetzt Mitglied werden!
d-64.org

Melde dich beim D64-Ticker an, um über aktuelle Ereignisse aus der Digitalszene und dem politischen Umfeld auf dem Laufenden zu bleiben!
Du erhältst dann werktags jeden Morgen einen Newsletter mit entsprechenden Nachrichten.
ticker.d-64.org

D64 – Zentrum für Digitalen Fortschritt e.V.
V.i.S.d.P.: Ulrich Berger (Geschäftsführer)
Gipsstraße 3
10119 Berlin

Das kleine 01001100 01000X01 10010100 der IT-Sicherheit

Hundertprozentige Sicherheit gibt es nicht. Kein IT-System ist vollständig sicher. Allerdings gibt es elf einfache Regeln, wie du als Benutzer:in die Wahrscheinlichkeit verringern kannst, dass persönliche Daten in fremde Hände gelangen. In diesem Flyer liefern wir deshalb das Ein-Mal-Eins der IT-Sicherheit.

01 Teile einen Account für einen Dienst oder deinen Computer nie mit einer anderen Person. Lege für andere Personen entsprechende neue Accounts an.

02 Sichere jedes Gerät, auch und vor allem dein Smartphone, mit einem sicheren Kennwort oder PIN. Einfache Tippfolgen oder Sperrmuster sind keine Absicherung.

03 Kennwörter gehören nicht auf Post-Its an den Bildschirm oder an andere Orte, die leicht zugänglich sind. Verwende, wenn möglich, für jeden Dienst ein eigenes Kennwort. Benutze einen Passwortmanager!

04 Prüfe, ob der Dienst, den du verwendest, eine sogenannte Zwei-Faktor-Authentifizierung (2FA) anbietet. Wenn ja, verwende sie unbedingt.

05 Verwende niemals einfache Kennwörter, insbesondere nicht für einen Passwortmanager. Kennwörter müssen ausreichend lang und komplex sein. Kurze Sätze können gute Eselsbrücken sein.

06 E-Mails sind in der Regel unverschlüsselt. Bildlich kann man sich E-Mails als Postkarten im Internet vorstellen, die durch Unbefugte auf dem Transportweg mitgelesen werden können. Versende also nur das per E-Mail, was du auch auf eine Postkarte schreiben würdest!

07 Verwende für den Austausch wichtiger Informationen Messenger mit Ende-zu-Ende-Verschlüsselung wie Signal. SMS sind nicht sicher.

08 Verwende Ende-zu-Ende-Verschlüsselung für E-Mails, wodurch E-Mails nicht mehr auf dem Transportweg mitgelesen werden können. Die bekannteste und empfehlenswerte Lösung ist PGP. Teile keine wichtigen Informationen in Betreffzeilen, da sie nicht verschlüsselt werden.

09 Öffne Anhänge (Bilder, PDF, Office-Dokumente) nur, wenn dir die Absender:innen bekannt sind und die E-Mail vertrauenswürdig erscheint. Öffne niemals Dateien mit der Endung .exe. Sei besonders vorsichtig bei .rar oder .zip Dateien!

10 Online-Festplatten wie Dropbox, Google Drive und Microsoft OneDrive sind häufig unverschlüsselt und speichern Daten möglicherweise im EU-Ausland. Verwende diese nicht für sensible Daten.

11 Verschlüssele deine Festplatte, insbesondere wenn es sich um ein Notebook handelt. Zumindest aber sollten Verzeichnisse mit sensiblen Dokumenten nicht ohne Verschlüsselung sein.

d-64.org