D64

Zentrum für
Digitalen Fortschritt

D64 versteht sich als Denkfabrik des digitalen Wandels. Wir sind von der gesamtgesellschaftlichen Auswirkung des Internets auf sämtliche Bereiche des öffentlichen und privaten Lebens überzeugt. D64 will Taktgeber und Ratgeber für die Politik sein, um Deutschland für die digitale Demokratie aufzustellen. Leitgedanke des Vereins, ist die Frage, wie das Internet dazu beitragen kann, eine gerechte Gesellschaft zu fördern.
Jetzt Mitglied werden!

d-64.org/mitglied-werden

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 Meldungen.

ticker.d-64.org

D64 – Zentrum für Digitalen Fortschritt e.V.
Vorsitzender: Nico Lumma
Vorsitzende: Laura-Kristine Krause
Werftstraße 3
10557 Berlin

Informations–sicherheit

Das kleine 01101011101001110X11011010101001101011

100% Sicherheit gibt es nicht. Kein IT-System ist vollständig sicher. Jedoch wird das Sicherheitsniveau häufig durch die Benutzerinnen und Benutzer massiv herabgesetzt, da einfache Regeln nicht eingehalten werden. Deshalb bietet diese kleine Broschüre einige Tipps mit dem IT-Sicherheit Ein-Mal-Eins.

01

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

02

Wenn es sich nicht verhindern lässt und Account-Informationen weitergegeben werden müssen, versende niemals Benutzername und Kennwort über den gleichen Kommunikationsweg.

03

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

04

Kennwörter gehören nicht auf Post-Its an den Bildschirm oder andere Orte, die leicht zugänglich sind.

05

Verwende, wenn möglich, für jeden Dienst ein eigenes Kennwort. Benutze einen Passwortmanager!

06

Verwende niemals einfache Kennwörter, insbesondere nicht für den Passwortmanager. Kennwörter müssen ausreichend lang sein und sollten Sonderzeichen sowie Ziffern enthalten.

07

Prüfe, ob der Dienst, den du verwendest, eine so genannte „Zwei-Faktor-Authentifizierung“ anbietet. Wenn ja, verwende diese unbedingt. Dadurch wird dir z. B. bei jedem Login-Vorgang eine SMS mit einem einmaligen Kennwort geschickt.

08

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!

09

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.

10

Öffne Anhänge (Bilder, PDF, Office-Dokumente) nur, wenn dir der Absender bekannt ist und die E-Mail vertrauenswürdig erscheint. Öffne niemals Dateien mit der Endung .exe!

11

Verwende sichere Messenger, die u.a. Ende-zu-Ende-Verschlüsselung verwenden. SMS sind nicht sicher.

12

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.

13

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