

Meine Daten gehören mir!



Benutze verschiedene und sichere Passwörter!

Auf verschiedenen Seiten sollten nicht die gleichen Passwörter benutzt werden!
Je länger ein Passwort ist, desto sicherer ist es auch. Sichere Passwörter kannst du dir ganz einfach mit einem leicht zu merkenden Satz erstellen.
Benutze einen Passwort-Manager oder Passwort-Safe, damit du deine Passwörter sicher verwahren kannst.

Lösche Cookies regelmäßig!

Cookies sind kleine Datenpakete, die Informationen über Internetnutzer speichern, sie können einfach im Browser gelöscht werden. Anleitungen dazu findest du im Internet.

Logge dich aus!

Nach der Benutzung eines Onlinedienstes solltest du dich gleich wieder abmelden. So kann nicht einfach jemand anderes auf dein Konto zugreifen und die Seite speichert keine zusätzlichen Informationen über dich.

Vorsicht bei öffentlichem W-LAN oder öffentlichen Computern!

Sei besonders vorsichtig, wenn du öffentliche Rechner benutzt – hier können Programme installiert sein, die deine Passwörter sammeln.
Auch im öffentlichen W-LAN können andere Menschen mitlesen! Vermeide diese, wenn möglich.

Schalte Ortungsdienste und Bluetooth nur bei Bedarf an!

Ortungsdienste, also Dienste, die auf einem Smartphone oder Tablet deinen Standort weitergeben, solltest du nur anschalten, wenn du sie brauchst.
Auch Bluetooth sollte nur eingeschaltet sein, wenn es notwendig ist.
Generell sollten beide Dienste abgestellt sein.

Die wichtigste Regel: Gib nur die Informationen von dir Preis, die nötig sind.

Im Internet sollte man Informationen nicht weitergeben, wenn man sie auch keinem Fremden auf der Straße erzählen würde.

Weitere Infos findest du unter <https://www.klicksafe.de>.

Version Oktober 2020