ONLINETIPPS

zum Schutz der Privatsphäre im Internet

1 EIN STARKES PASSWORT

Verwende für jede Website oder digitalen Dienst ein eigenes Passwort! Wenn ein Konto gehackt wird, bleiben Deine übrigen Konten sicher.

TIPPS

- Verwende für jedes Konto ein langes, komplexes (Kombination von Sonderzeichen, Buchstaben und Ziffern) und einzigartiges Passwort!
- Bewahre Deine Passwörter sicher auf und nutze einen Passwortmanager!

2 BLEIBE AUF DEM STAND

Sicherheitslücken in Deiner Software, Deinen Anwendungen und Deiner Hardware können Hackern Zugang zu Deinen persönlichen Daten verschaffen.

TIPPS

- Aktualisiere Software, Apps und Geräte, sobald sie dir angeboten werden, um ihre Sicherheitslücken zu beheben.
- Aktiviere automatische Updates, wann immer möglich.

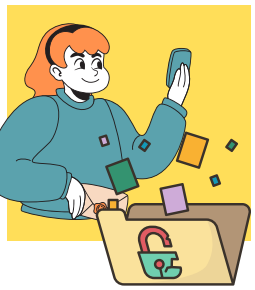
3 SICHERHEITSKOPIE

Sichere Deine Daten, um sie bei Hackangriffen, Diebstahl oder Geräteschäden nicht zu verlieren!

TIPPS

- Erstelle regelmäßig Sicherungskopien Deiner Daten auf einem zusätzlichen verschlüsselten Datenträger (USB-Stick, externe Festplatte, Cloud), um sie bei Problemen wiederherstellen zu können!

4 SELBSTKONTROLLE

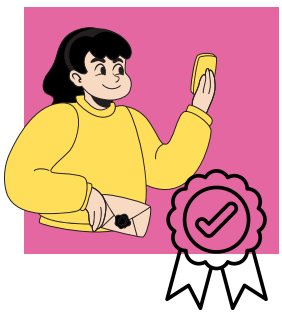


Das Teilen Deiner persönlichen Daten im Internet (Name, E-Mail, Fotos, Videos...) kann sie für missbräuchliche Nutzung anfällig machen.

TIPPS

- Vermeide es, Deine persönlichen Daten und die Deiner Bekannten weiterzugeben!
- Überprüfe die Privatsphäre Einstellungen Deiner Konten, um festzulegen, was für andere sichtbar sein darf!

5 QUELLENCHECK

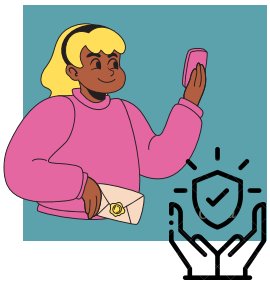


Viren, die Deine Geräte oder Konten gefährden können, verstecken sich auch oft in raubkopierter Software, Cheat-Erweiterungen für Videospiele oder auf illegalen Streaming-Websites.

TIPPS

- Lade keine illegalen Inhalte oder inoffiziellen Lösungen herunter!
- Installiere nur Apps von offiziellen Websites oder Stores der Hersteller!

6 BLEIBE AUFMERKSAM



Phishing bezeichnet eine Betrugsmasche, bei der Kriminelle versuchen, durch gefälschte betrügerische Nachrichten (E-Mails, SMS, soziale Netzwerke) oder Anrufe, bei denen sich Kriminelle als vertrauenswürdige Organisationen (z. B. Bank, Behörde) ausgeben. Ziel ist es, Deine persönlichen Daten zu stehlen, Dich zur Installation von Viren zu verleiten oder Dich zum Opfer eines Betruges machen.

TIPPS

- Sei immer misstrauisch und klicke oder antworte nicht vorschnell!
- Überprüfe die Informationen immer selbst, indem Du Dich direkt in Dein Konto beim betreffenden Dienst einloggst!