verbraucherzentrale
Nordrhein-Westfalen

07.04.2021

DATENSICHERHEIT BEI FACEBOOK

So können Verbraucher:innen das Risiko von Datendiebstahl verringern

tipp tipp tipp tipp tipp

Facebook-Mitglieder weltweit schreckten am Osterwochenende auf: Persönliche Daten von mehr als 530 Millionen Nutzer:innen sollen im Internet veröffentlicht worden sein. Darunter sollen auch Daten von rund sechs Millionen Menschen aus Deutschland sein. Nach Medienberichten wurden sie wohl über eine Sicherheitslücke erbeutet, die Facebook nach eigenen Angaben im August 2019 geschlossen hatte. „Apps, die Facebook als Plattform nutzen, können auch ohne Sicherheitslücke Daten der Mitglieder sammeln", erklärt Hauke Mormann, Online-Experte der Verbraucherzentrale NRW. „Über solche Anwendungen können Firmen an Daten von Facebook-Mitgliedern kommen, ohne dass diese es unbedingt wissen." Wie können sich Verbraucher:innen vor Datenmissbrauch schützen? Die Verbraucherzentrale NRW gibt praktische Tipps zum Umgang mit Facebook-Apps.

- **Facebook-Apps prüfen**
  Facebook-Apps sind kleine Programme wie Spiele, Umfragen oder Tests. Wer diese Apps nutzt, gibt Dritten möglicherweise Zugriff auf persönliche Facebook-Daten, ohne es zu merken. Verbraucher:innen sollten daher prüfen, welche Apps sie wirklich benötigen und auf andere Anwendungen verzichten.

- **Einstellungen ändern**
  In den Facebook-Einstellungen können Verbraucher:innen regeln, auf welche Daten Apps zugreifen und wie sie diese Informationen nutzen dürfen. Für jede App wird einzeln angezeigt, auf welche persönlichen Facebook-Daten sie zugreifen kann. Es ist empfehlenswert, so wenig Datenzugriffe wie möglich zu erlauben. Unter Umständen funktioniert die Anwendung danach nicht mehr wie zuvor. Interessenten müssen dann abwägen, ob sie der Anwendung den Zugriff auf die Daten trotzdem gestatten wollen oder ob sie auf die Nutzung der Anwendun[illegible] verzichten.

- **Mit eigenen Daten geizen**
  Geburtsdatum, echter Name, genutzte E-Mail-Adresse und Telefo[illegible] nummer sind wertvolle Daten für Kriminelle. Solche Informationen ten im Internet so wenig wie möglich öffentlich zur Verfügung stel Denn wer es darauf anlegt, kann sie auch aus unterschiedlichen len zusammentragen und ein umfassendes Profil erstellen.

- **Single-Sign-On vermeiden**
  Viele Internetshops und Plattformen bieten die Möglichkeit, sich [illegible]

Frankenwerft 35
50667 Köln
Tel.: (0221) 846 188-88
Fax: (0221) 846 188-33
koeln.quartier@verbraucherzentrale.nrw
www.verbraucherzentrale.nrw

dem Social-Media-Account einzuloggen. Auch das funktioniert, indem bei Facebook eine entsprechende App aktiviert wird, die Daten der Nutzer:innen sammeln kann. Betreiber:innen unseriöser Internetseiten könnten diese Infos für gefährliche Aktionen wie Phishing oder gar Identitätsdiebstahl nutzen. Der Komfort des Logins mit einem Social-Media-Account birgt weitere Risiken. Wie bei einem Generalschlüssel für ein Haus kann der Schaden beim Verlust eines "Single-Sign-On"-Account-Passworts besonders groß werden. Gelangt das Passwort für das eine Konto in die falschen Hände, erhalten Dritte nicht nur Zugang zu diesem Konto, sondern zu allen Seiten mit entsprechender Login-Möglichkeit. Umso wichtiger ist es, das Konto durch ein sicheres und einmaliges Passwort abzusichern. Für mehr Sicherheit kann das Konto über eine Zwei-Faktor-Authentifizierung geschützt werden – sofern man dem Anbieter eine Handynummer anvertrauen möchte. Der Login beziehungsweise bestimmte Aktionen, wie die Bestätigung einer Zahlung, klappen dann neben dem Passwort erst durch einen zweiten Schritt – etwa die Eingabe einer PIN, die per SMS oder spezieller App auf das Smartphone geschickt wird.

Weitere Informationen zum Thema Datensicherheit bei Facebook gibt es auf der Homepage der Verbraucherzentrale NRW unter https://www.verbraucherzentrale.nrw/node/25013.

Für weitere Informationen

Pressestelle Verbraucherzentrale NRW

Tel. (0211) 38 09-101

presse@verbraucherzentrale.nrw