GEHACKTER ACCOUNT: CHECKLISTE FÜR DEN ERNSTFALL

Unbefugte haben sich Zugang zu einem Account verschafft: Nun können sie nicht nur die dort gespeicherten Daten, wie etwa Postanschrift und Kreditkarteninformationen, einsehen. Womöglich nutzen sie den fremden Account auch, um zum Beispiel illegal Waren zu verkaufen oder Spamnachrichten in fremdem Namen zu verschicken.

Besonders kritisch sind gehackte E-Mail-Accounts: Haben sie sich Zugang verschafft, können Kriminelle glaubwürdig mit hinterlegten Kontakten kommunizieren. Zudem ist die E-Mail-Adresse oft bei anderen Diensten hinterlegt, um dort das Passwort zurücksetzen zu können. Kriminelle bringen dann gleich mehrere Accounts unter ihre Kontrolle.

SO ERKENNEN SIE EINEN GEHACKTEN ACCOUNT

Wenn Sie nicht mehr auf Ihren Account zugreifen können, wurde das Passwort womöglich von Unbefugten ohne Ihr Wissen geändert. Ebenso kann es sein, dass der Anbieter den Fremdzugriff oder damit ausgeführte (illegale) Aktivitäten bemerkt und Ihren Account gesperrt hat.
Werden Sie auch misstrauisch, wenn Sie Aktivitäten oder Änderungen in Ihrem Account, die nicht Sie vorgenommen haben, entdecken. Dazu zählen beispielsweise verschickte Nachrichten, Anmeldungen über neue Geräte oder Rechnungen für Käufe oder Verträge, die Sie nicht getätigt haben.

DAS SOLLTEN SIE TUN, WENN…

… Sie keinen Zugriff mehr auf Ihren Account haben

- ✓ **Bitten Sie den Anbieter um Unterstützung!** Dieser kann den Account womöglich zurücksetzen oder wiederherstellen.
- ✓ **Warnen Sie Ihre Kontakte!** So schützen Sie diese, sollten sie zum Beispiel von Ihrem Account verschickte Phishing-Mails erhalten.

… Sie sich noch in Ihren Account einloggen können

- ✓ **Ändern Sie schnellstmöglich das Passwort!**
- ✓ **Beenden Sie alle aktiven Sitzungen!** Das ist meist mit einem Klick in den Account-Einstellungen möglich.
- ✓ **Kontrollieren Sie die Account-Einstellungen!** Gegebenenfalls haben Unbefugte beispielsweise automatische Weiterleitungen hinzugefügt.
- ✓ **Geben Sie Ihren Kontakten Bescheid!** Bitten Sie etwa darum, über von Ihrem Account verschickte Spamnachrichten informiert zu werden.

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

Außerdem gilt in jedem Fall:

- ✓ **Ändern Sie auch die Passwörter weiterer, potenziell mitbetroffener Accounts!** Das gilt für Accounts, bei denen Sie das gleiche Passwort wie beim gehackten Account nutzen, ebenso wie für Accounts, bei denen Sie die möglicherweise gehackte E-Mail-Adresse hinterlegt oder sich per Single-Sign-On (Anmeldung über Drittanbieter) mit dem möglicherweise gehacktem Account eingeloggt haben. Hinterlegen Sie (vorrübergehend) eine andere E-Mail-Adresse, wo nötig.
- ✓ **Behalten Sie Ihre Kontoaktivitäten im Blick!** Wenn Sie befürchten, dass Bankkonten, Accounts bei Zahlungsdienstleistern o. ä. betroffen sein könnten, kontrollieren Sie diese regelmäßig. Informieren Sie im Ernstfall die Bank oder den Dienstleister.
- ✓ **Sammeln Sie wichtige Informationen!** Notieren Sie alle Indizien, die auf einen gehackten Account hindeuten, und alle Konten, die betroffen sein könnten. So sind Sie vorbereitet, sollten Sie zum Beispiel Anzeige erstatten wollen.

SO SICHERN SIE IHRE ACCOUNTS IN ZUKUNFT AB

- › **Passkeys nutzen:** Mit der Alternative zu Passwörtern müssen Sie sich nicht mehr viele verschiedene Passwörter merken.
- › **Zwei Faktor-Authentisierung aktivieren:** Wenn Sie weiterhin Passwörter nutzen, schützt ein zweiter Faktor Ihren Account zusätzlich, sollte das Passwort in fremde Hände gelangen.
- › **Phishing-Mails erkennen:** Seien Sie wachsam, wenn Sie in einer E-Mail etwa dazu aufgefordert werden, sich per Link in Ihren Account einzuloggen, und Ihnen dringender Handlungsbedarf suggeriert wird.
- › **Bildschirmsperre einrichten:** Sollte beispielsweise Ihr Smartphone geklaut werden, verhindern Sie so, dass Fremde darauf zugreifen können und etwa über eine ungeschützte App Zugriff zu einem Account erlangen.
- › **Sparsam mit Daten umgehen:** Geben Sie online möglichst wenig über sich preis.
- › **Vorsicht bei Links und Anhängen:** Hinter E-Mail-Anhängen oder Links auf Webseiten kann sich Schadsoftware verbergen.
- › **Updates installieren:** Damit schließen Hersteller oft Sicherheitslücken, sodass Kriminelle diese nicht ausnutzen können.
- › **Virenscanner und Firewall nutzen:** Auf vielen Geräten sind diese bereits vorinstalliert. In manchen Fällen müssen sie in den Einstellungen jedoch noch aktiviert werden.
- › **Öffentliches WLAN meiden:** Mitunter werden dort zum Beispiel Daten unverschlüsselt übertragen.

Mehr Informationen zu Cybersicherheit für Verbraucherinnen und Verbraucher:
www.bsi.bund.de/VerbraucherInnen

Mehr Informationen für Opfer von Cybercrime:
www.polizei-beratung.de/infos-fuer-betroffene/cybercrime/

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen,
dass Sie
sicher leben.
Ihre Polizei