KEEPER | Pressemitteilung

Was tun, wenn die Apple-ID gehackt wurde?
Bei diesen fünf Alarmsignalen ist Handeln angesagt

MÜNCHEN, 25. Februar 2025 – Eine Apple-ID ist für jeden Hacker besonders wertvoll, weil sich mit ihr eine Vielfalt an cyberkriminellen Handlungen einleiten lässt. Umso wichtiger ist es, diese zu schützen und darauf zu achten, ob es eventuell Anzeichen für einen Hackerangriff gibt. Auf fünf Alarmzeichen sollte geachtet werden. Keeper Security gibt zudem nützliche Tipps, die Anwender bei einem Hacking-Verdacht beachten sollten.

1. E-Mail-Information, dass sich jemand beim Apple Konto angemeldet hat
Wenn eine Apple-ID gehackt wurde, kann es sein, dass der ID-Besitzer darüber informiert wird, dass sich jemand mit einem anderen Apple-Gerät angemeldet hat. Diese E-Mail enthält meist Informationen zu Datum und Uhrzeit der Anmeldung, dem Betriebssystem des neuen Geräts und dem verwendeten Gerätetyp. Sollte keine eigene Anmeldung über das in der E-Mail genannte Gerät erfolgt sein, ist es wahrscheinlich, dass ein Hacker sich angemeldet hat.

2. Apple-Gerät kann nicht mehr verwendet werden
Das offensichtlichste Anzeichen dafür, dass eine Apple-ID gehackt wurde, ist, dass man ein Apple-Gerät nicht mehr verwenden kann. Denn sobald ein Hacker die Login-Daten hat und sich anmeldet, kann er die mit diesem Account verbundenen Geräte sperren. Sobald der Cyberkriminelle die Geräte, die mit der ID verbundenen sind, in den „Verloren-Modus“ versetzt, kann der eigentliche Besitzer nicht mehr darauf zugreifen.

3. Kein Zugriff auf das iCloud-Konto möglich
Ein weiteres Indiz für den Diebstahl einer Apple-ID ist, dass der Zugriff auf das iCloud-Konto verwehrt wird. Ein Hacker, dem der Zugriff auf das iCloud-Konto gelingt, kann durch die Änderung des Passworts dafür sorgen, dass der eigentliche Account-Besitzer nicht mehr darauf zugreifen kann.

4. Benachrichtigung über Änderungen beim Apple Konto
Wer eine E-Mail über Änderungen am Apple Konto erhält – ohne selbst etwas getan zu haben – der wurde vermutlich gehackt. Einer Apple-ID sind eine Telefonnummer sowie eine E-Mail-Adresse zugeordnet und diese Informationen kann der Hacker zu seinen Gunsten ändern, nachdem er den Kontozugriff erlangt hat.

5. Kontoauszüge weisen unbekannte Apple-Gebühren auf
Wer auf seinen Kontoauszügen unbekannte Belastungen von Apple bemerkt, sollte davon ausgehen, dass es sich dabei um eine nicht autorisierte Aktivität handelt. Auch dieser Vorgang ist ein Hinweis dafür, dass die Apple-ID von jemand anderem verwendet wird.

Das ist nach einem Hack der Apple-ID zu tun
Diese Schritte können helfen, die eigene Identität, Privatsphäre und Finanzen zu schützen.

1. **Passwort der Apple-ID ändern**
   Solange man Zugriff auf das Apple-ID-Konto hat, sollte sofort das Passwort geändert werden. Dabei sollte sichergestellt sein, dass das neue Passwort stark und einzigartig ist, und mindestens aus 16 Zeichen und einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen besteht.

2. **Kontowiederherstellungsfunktion nutzen**
   Es besteht die Möglichkeit, über die Kontowiederherstellungsfunktion den Zugriff auf die Apple-ID wiederherzustellen. In der Regel erhält man, nachdem die Kontowiederherstellung angefordert wurde, eine E-Mail, um die Anfrage zu bestätigen sowie ein Datum, zudem der Zugriff wieder funktionieren sollte. Es kann jedoch sein, dass dieser Prozess aus Sicherheitsgründen ein paar Tage dauert.

3. **Zwei-Faktor-Authentifizierung (2FA) aktivieren**
   Empfehlenswert ist zudem, die Apple-ID mit einer Zwei-Faktor-Authentifizierung zu schützen. Das ist eine Sicherheitsmaßnahme, bei der die Identität zusätzlich zu Benutzernamen und Passwort mit einer weiteren Methode authentifiziert wird.

4. **Auf Anzeichen von Identitätsdiebstahl achten**
   Falls eine Apple-ID gehackt wurde, sollte man darauf achten, ob es weitere Ungereimtheiten gibt, beispielsweise unbekannte Rechnungen oder unbekannte Informationen auf dem Kontoauszug. Sobald es Grund zur Annahme gibt, dass die ID gestohlen wurde, sollte bei der Kreditkarten-Hotline ein Betrug gemeldet werden. Zusätzlich und wenn möglich, sollte jede Zahlung im System des Finanzinstituts authentifiziert werden, bevor die Überweisung ausgelöst wird.

Eine Apple-ID umfasst viele vertrauliche Informationen und muss deshalb besonders vor fremdem Zugriff geschützt werden. Jeder sollte wachsam sein und im Verdachtsfall schnell und professionell handeln. Am besten ist es natürlich, seine Apple-ID bereits im Vorfeld mit einem starken Passwort, das für keinen anderen Account genutzt wird, zu schützen. Die einfachste Möglichkeit, ein Passwort zu aktualisieren und sicher zu speichern, ist die Verwendung eines Passwortmanagers, beispielsweise von Keeper. Damit lassen sich die Zugangsdaten nicht nur schützen, sondern sichere Passwörter mit dem integrierten Passwortgenerator auch erstellen.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de