So schützen Sie Ihre Online-Accounts im KI-Zeitalter

Mit ein paar Tipps lassen sich Smartphones und Accounts heute (fast) **unknackbar** machen.

VON MATTHIAS SCHWARZER

FOTO: ELLIE ELLIEN / UNSPLASH

Der technische Fortschritt bringt nicht nur Vorteile. Auch Kriminelle machen sich technologische Entwicklungen zunutze – allen voran die Künstliche Intelligenz. Cyberangriffe sind in den vergangenen Jahren immer ausgereifter geworden. Wer nicht aufpasst, kann schnell seine Online-Accounts los sein. Oder noch schlimmer: sein Geld.

Erkannte man Phishing-Mails früher meist noch an den vielen Rechtschreibfehlern, lassen sie sich heute kaum noch von denen echter Unternehmen unterscheiden. KI kann auch eingesetzt werden, um auf das Opfer zugeschnittene Cyberattacken zu starten, Stimmen für Phishing-Angriffe zu klonen oder Passwörter zu erraten. Unerlaubter Zugriff auf Online-Accounts und persönliche Daten eignet sich perfekt für Identitätsdiebstahl, Erpressungsversuche oder Warenbetrug.

Die gute Nachricht: Nicht nur Cyberkriminelle sind professioneller geworden – es gibt auch immer bessere Sicherheitsmaßnahmen, die viele Nutzerinnen und Nutzer jedoch noch gar nicht aktiviert haben. Schon mit ein paar einfachen Tipps kann man Hackern das Leben sehr viel schwerer machen.

Passkeys statt Passwörter

Eine dieser Verbesserungen ist die immer größere Verbreitung sogenannter Passkeys. Grob gesagt funktionieren diese so: Wer sich in einen Online-Account einloggt, verwendet nicht mehr die klassische Kombination aus Nutzername (beziehungsweise E-Mail-Adresse) und Passwort. Stattdessen bestätigt man den Log-in-Versuch direkt auf seinem Gerät – entweder über den Fingerabdrucksensor oder die Gesichtserkennung. Für dieses Verfahren wird zuvor bei der Einrichtung ein geheimer „Schlüssel" – der Passkey – erstellt. Gespeichert wird er etwa im Google-Account (Android), im Apple-Account (iOS) oder in einem Passwort-Manager von Drittanbietern. So kann dieser selbst bei einem Gerätewechsel nicht verloren gehen.

Die übliche Kombination aus Benutzername und Passwort ist sehr betrugsanfällig, weil man sie versehentlich auch auf Phishing-Websites eingeben kann. Zudem können Passwörter durch Datenlecks im Darknet landen und dann von Cyberkriminellen missbraucht werden. Das ist bei einem Passkey so nicht möglich: Der Hacker bräuchte direkten Zugriff auf das betreffende Gerät – und könnte selbst dann wenig damit anfangen, weil ihm das nötige biometrische Merkmal (also Fingerabdruck oder Gesichtserkennung) oder der PIN-Code fehlt.

Die schlechte Nachricht: Viele kleinere Anbieter bieten in ihren Account-Einstellungen noch keine Passkeys an, dazu gehören auch viele deutsche E-Mail-Anbieter und Online-Shops. Bekanntere Dienste wie Paypal und Amazon haben die Funktion bereits umgesetzt. Und auch die Accounts von Google (seit 2023) und Apple (seit 2022) lassen sich auf diese Weise schützen – so wird der eigene Smartphone-Account zum sicheren Tresor und nur noch schwer zugänglich für Hacker.

Ganz besonders sicher: FIDO-Schlüssel

Wer sich besonders gefährdet sieht, kann noch einen Schritt weitergehen und als Passkey einen externen Sicherheitsschlüssel verwenden. Dabei handelt es sich um kleine USB-Sticks (auch FIDO2-Schlüssel genannt), die von verschiedenen Herstellern angeboten werden – bekannt sind etwa der Yubikey oder der Titan Security Key von Google. Auf diesem wird ein persönlicher Schlüssel gespeichert, der dann beim Log-in-Prozess Zugriff auf den Online-Account gewährt.

Beim Log-in gibt man kein Passwort mehr ein, sondern steckt stattdessen den Stick in seinen Computer – alternativ kann man ihn per NFC-Funktechnik an sein Smartphone halten. Das Gerät erkennt den privaten Schlüssel, und schon ist man eingeloggt. Auch hier wird das Verfahren von einigen großen Anbietern wie Google, Apple, Microsoft, Dropbox, Paypal oder Meta bereits unterstützt.

Ein Nachteil: Da dieses Verfahren besonders sicher ist, kann es schnell auch dazu führen, dass man sich selbst aus seinen Accounts aussperrt – zum Beispiel, weil man seinen Sicherheitsschlüssel verliert oder dieser beschädigt wird. Selbst die Anbieter können dann nicht mehr weiterhelfen, und der Account könnte unwiederbringlich verloren sein. Man sollte also immer darauf achten, noch eine zweite Anmeldemethode für Notfälle einzurichten – etwa die Bestätigung über ein Zweitgerät. Alternativ kann man auch mehrere Sicherheitsschlüssel anschaffen und sie an verschiedenen Orten sicher aufbewahren.

Zwei-Faktor-Methode ist Pflicht

Wem diese vergleichsweise jungen Sicherheitsmaßnahmen noch etwas zu unvertraut erscheinen, der sollte seine Online-Accounts zumindest über die gängigen Methoden absichern. Geradezu zwingend im KI-Zeitalter ist die Zwei-Faktor-Methode – bei vielen Online-Diensten ist sie inzwischen sogar standardmäßig aktiviert. Hier wird bei jedem Log-in eine E-Mail oder eine SMS mit einem Code versendet, mit dem man dann seine Anmeldung bestätigen muss. Diese Methode gilt allerdings auch bereits als unsicher und veraltet.

Deutlich sicherer ist das Log-in über eine Zwei-Faktor-App – etwa Google Authenticator, Microsoft Authenticator, Proton Authenticator oder Authy. In der App wird ein zufälliger Code generiert, der bei der Anmeldung eingegeben werden muss. SMS und E-Mail sind in der Regel nicht verschlüsselt – der Weg über die App erhöht die Sicherheit also deutlich.

Auch empfiehlt es sich, einen Passwort-Manager einzusetzen. Der Vorteil: Lässt man über die Dienste Passwörter generieren, sind diese nicht nur komplex und sicher – sie werden auf vertrauenswürdigen Websites auch automatisch ausgefüllt. Das senkt die Gefahr, dass man aus Versehen auf Phishing-Websites das Passwort eingibt. Nahezu alle Webbrowser haben Passwort-Manager direkt integriert, häufig sind diese jedoch auch Ziel von Cyberangriffen. Wer auf noch höhere Sicherheit setzen will, kann einen externen Passwort-Manager nutzen – etwa Bitwarden oder 1Password.

Ebenfalls wichtig: Verfügbare Updates von Apps und Betriebssystem sollte man stets zeitnah installieren – am besten aktiviert man dafür automatische Updates. Auf diese Weise stopfen Anbieter nämlich bekannte Sicherheitslücken, über die Hacker im Zweifel auch Zugriff bekommen können.

Phishing-Attacken mit Malware

Das Problem an all diesen Maßnahmen: Völlig unhackbar machen sie Online-Accounts nicht. Cyberkriminellen kann es gelingen, sich selbst an den besten Sicherheitsmaßnahmen vorbeizuschlängeln – und zwar immer dann, wenn Malware ins Spiel kommt.

Ein besonders perfider Trick ist etwa das sogenannte Session-Hijacking. Dabei verschicken Hacker eine Phishing-E-Mail mit einem Link. Klickt man ihn an, installiert sich auf dem eigenen Computer ein Virus, welcher die im Browser gespeicherten Session-Cookies ausliest und sie an den Abgreifer weiterleitet. Dieser kann sich dann zwischen den Nutzer und den jeweiligen Account schalten und Letzteren übernehmen – selbst wenn dieser mit Passkeys oder Zwei-Faktor-Methoden gesichert ist.

Verbreitet ist die Masche vor allem für Windows-Computer, außerdem richtet sie sich in der Regel an Personen von größerem Interesse – immer wieder sind zum Beispiel Influencer davon betroffen, deren Youtube- oder Social-Media-Accounts auf diese Weise gehackt werden. In der Theorie ist die Masche aber auch bei anderen Betriebssystemen und auch Privatnutzern möglich.

So vermeiden Sie Cyberangriffe

Selbst wer die wichtigsten Sicherheitsmaßnahmen aktiviert hat, sollte also dennoch ein paar zusätzliche Tipps befolgen:

- Sichern Sie Ihren E-Mail-Account und Ihre Accounts bei Apple und Google auf dem Smartphone ganz besonders ab – diese sind oft der Generalschlüssel zu privaten Daten und vielen anderen Online-Konten.
- Klicken Sie nicht auf Links in E-Mails von Unternehmen, am besten nicht einmal bei vermeintlich vertrauenswürdigen Absendern. Loggen Sie sich stattdessen immer über die offizielle Website in das jeweilige Online-Konto ein. Sollte der Anbieter tatsächlich etwas von Ihnen wollen, findet sich die Anweisung auch dort.
- Überprüfen Sie regelmäßig, ob Ihre Zugangsdaten geleakt wurden. Das funktioniert zum Beispiel über die Website Haveibeenpwned.com oder den Identity Leak Checker des Hasso-Plattner-Instituts.
- Geben Sie zur Anmeldung in Online-Diensten nicht Ihre echte E-Mail-Adresse heraus, weil diese durch Datenlecks im Netz landen kann. Nutzen Sie stattdessen separate Mail-Adressen für „unwichtige" Log-ins (etwa Online-Shops), eine andere für Hochsicherheitsbereiche (zum Beispiel Online-Banking) und eine weitere für die private Kommunikation. Viele Anbieter bieten auch die Möglichkeit, E-Mail-Aliasse einzurichten. Sollte es zu Datenlecks kommen, bleiben Ihre wichtigen E-Mail-Adressen unbekannt – und Sie können mögliche Phishing-Attacken auch besser zuordnen.
- Geben Sie Ihre Handynummer nicht heraus, wenn Sie nicht unbedingt müssen. Wenn Sie es doch müssen, kann sich eine günstige Zweitnummer als E-Sim lohnen, die Sie speziell für Online-Accounts nutzen. So bleibt die echte Handynummer privat sowie frei von Phishing-SMS und Spam-Anrufen.
- Laden Sie Apps nur aus seriösen Quellen herunter, etwa dem offiziellen Play Store von Google oder dem App Store von Apple.
- Loggen Sie sich aus Online-Accounts vollständig aus, wenn Sie sie nicht benutzen – nicht einfach nur den Tab schließen.
- Geben Sie in öffentlichen WLAN-Netzen keine sensiblen Daten ein.
- Werden Sie misstrauisch, sobald Sie jemand zu einem dringenden Handeln auffordert. Das kann auch für Anrufe von vermeintlichen Verwandten gelten, die um Geld bitten – auch deren Stimmen könnten mit KI geklont worden sein. Vereinbaren Sie mit Vertrauten ein gemeinsames Codewort, um echte Notfälle von Phishing-Anrufen unterscheiden zu können.