Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Instahack

Social-Engineering-Angriffe auf Instagram-Accounts und wie Sie sich davor schützen

Immer wieder kapern Phisher fremde Instagram-Accounts, um Profit daraus zu schlagen. So auch im Fall einer deutschen Olympiaschwimmerin, die sich Hilfe suchend an c’t wandte. Wir sind der Sache nachgegangen und stießen dabei auf weitere Fälle. Wir erklären, wie Sie Ihren Account schützen.

Von Ronald Eikenberg und Marie-Claire Koch

kompakt

- Instagram-Accounts, egal ob sehr populär oder nahezu unbekannt, sind ein lukratives Angriffsziel für Cyber-Kriminelle.
- Es ist wichtig, den Account mehrstufig abzusichern, wenn man nicht Gefahr laufen will, ihn für immer zu verlieren.
- Wer eine Mail erhält, die angeblich von Instagram stammt, sollte in der App kontrollieren, ob die Mail echt ist.

Phisher versuchen immer wieder an Zugangsdaten für Social-Media-Dienste wie Instagram zu kommen, um Accounts zu kapern

und Profit daraus zu schlagen [1] – zum Beispiel durch Lösegeldforderungen oder dubiose Spam-Kampagnen. Dafür ist den Angreifern jeder Account gut genug, doch besonders hoch im Kurs stehen Instagram-Accounts, die der begehrte blaue Haken ziert. Er zeigt, dass es sich um ein durch Instagram verifiziertes Profil einer Person öffentlichen Interesses handelt. Aber auch mit nicht verifizierten Accounts können Phisher Geld machen, mangelndes öffentliches Interesse schützt Ihren Account daher nicht.

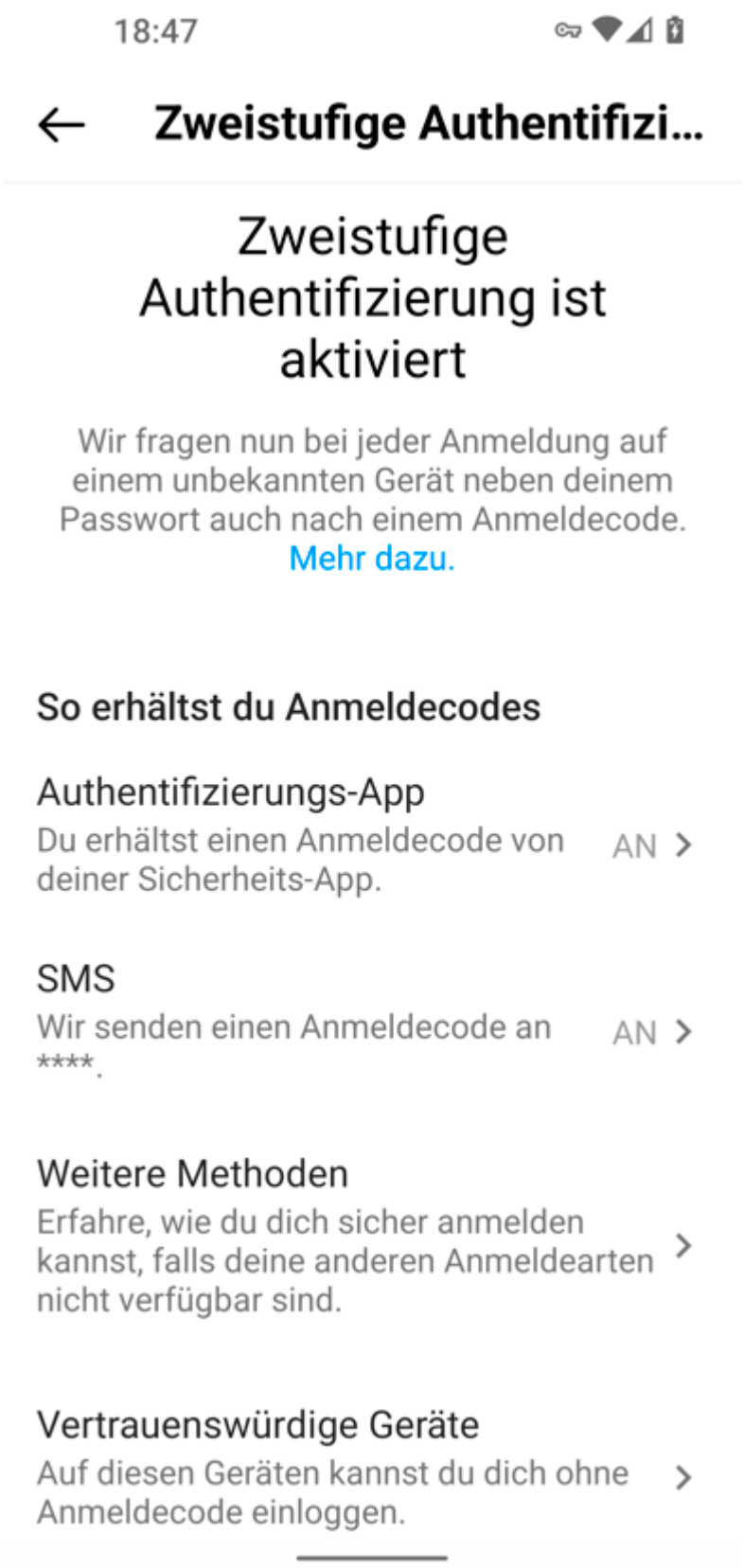
Der Instagram-Account einer Berliner Olympiaschwimmerin trägt diesen blauen Haken. Sie nutzt den Account, um mit ihren Fans in Kontakt zu bleiben und ihre Erfolge zu teilen – zum Beispiel ihre Teilnahme an den Olympischen Spielen in Tokio oder zuletzt an der Europameisterschaft in Rom. Vor einigen Monaten entdeckte auch ein Phisher die erfolgreiche Schwimmerin bei Instagram. Er kontaktierte sie über eine private Nachricht, gab sich als Instagram-Support aus, um sie in die Falle zu locken, und konnte letztlich die Kontrolle über ihren Account übernehmen.

Man spricht bei solchen Angriffen von Social Engineering, also der gezielten Manipulation des Opfers. Als die Schwimmerin bemerkte, wie ihr geschah, war das Kind bereits in den Brunnen gefallen. Der Angreifer hatte das Instagram-Konto bereits fest im Griff und die Account-Sprache auf Arabisch geändert. Die Schwimmerin wandte sich daraufhin an einen IT-Experten, der den Account jedoch auch nicht mehr retten konnte. Der Täter forderte unterdessen ein Lösegeld in Höhe von 150 Euro, zahlbar via PayPal.

Passwort: „Passwort“

Statt der dreisten Lösegeldforderung nachzukommen, wandten sich die beiden an c’t. Im Rahmen unserer Recherche stießen wir auf drei weitere Sportlerinnen und Sportler aus dem Umfeld der Schwimmerin, deren Accounts ebenfalls gehackt waren. In zwei Fällen war ebenfalls Social Engineering im Spiel, im

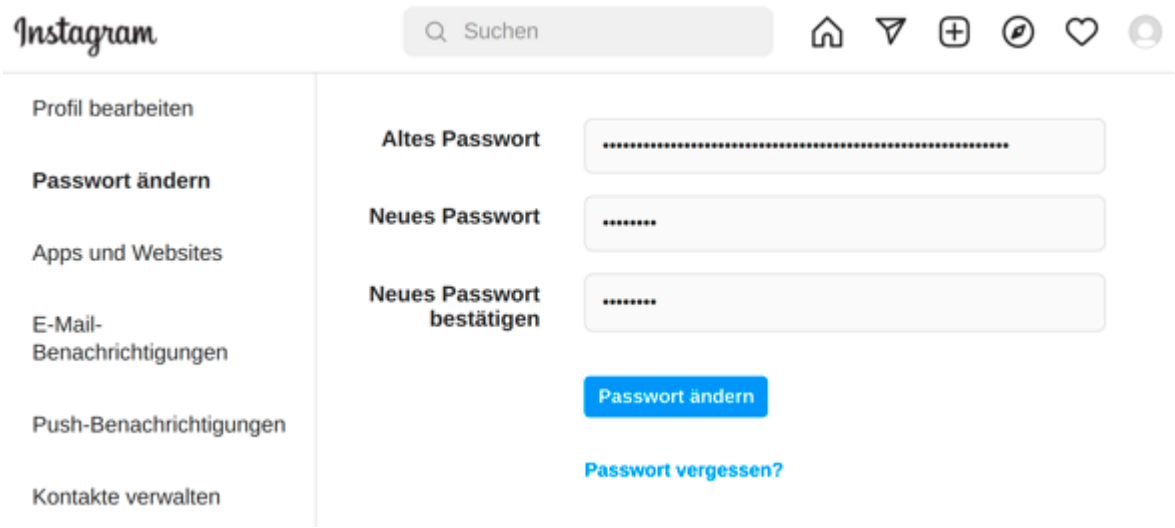
dritten wurde offenbar das Passwort erraten – es lautete schlicht „Passwort“. Alle betroffenen Accounts waren nicht nach Stand der Technik abgesichert: Die sogenannte Zwei-Faktor-Authentifizierung (2FA), die Angriffe auf Online-Accounts in den meisten Fällen vereiteln kann [2], war nicht eingeschaltet.



Wer einen Instagram-Account besitzt, sollte die zweistufige Authentifizierung einschalten.
Ist die 2FA aktiv, ist zumindest beim ersten Einloggen auf einem Gerät neben dem Passwort auch noch ein zweiter Faktor nötig. Das kann zum Beispiel ein kurzzeitig gültiger

Zahlencode sein, den man per SMS bekommt oder mit einer App wie dem Google Authenticator selbst generiert. Ein Hacker kommt in aller Regel nicht an SMS und erst recht nicht an das Geheimnis in der Authenticator-App. Mit einem erbeuteten Passwort kann er sich daher nicht einloggen.

Um die gehackten Instagram-Accounts der Athleten zu retten, kontaktierten wir die Pressestelle des Instagram-Betreibers Meta. Kurz darauf konnten die rechtmäßigen Account-Besitzer wieder auf ihre Konten zugreifen. Uns erreichen immer wieder ähnliche Zuschriften von Instagram-Nutzern, die Opfer von Cyber-Ganoven geworden sind. Weil wir nicht immer helfen können und damit es erst gar nicht so weit kommt, möchten wir Ihnen im Folgenden die wichtigsten Sicherheitstipps an die Hand geben, damit Sie Ihren Instagram-Account – oder die Accounts Ihrer Sprösslinge – angemessen absichern können.



Passwort: „Passwort“ – die Passwortanforderungen von Instagram sind eher locker, damit haben Cyber-Ganoven wie in diesem Fall dann leichtes Spiel.

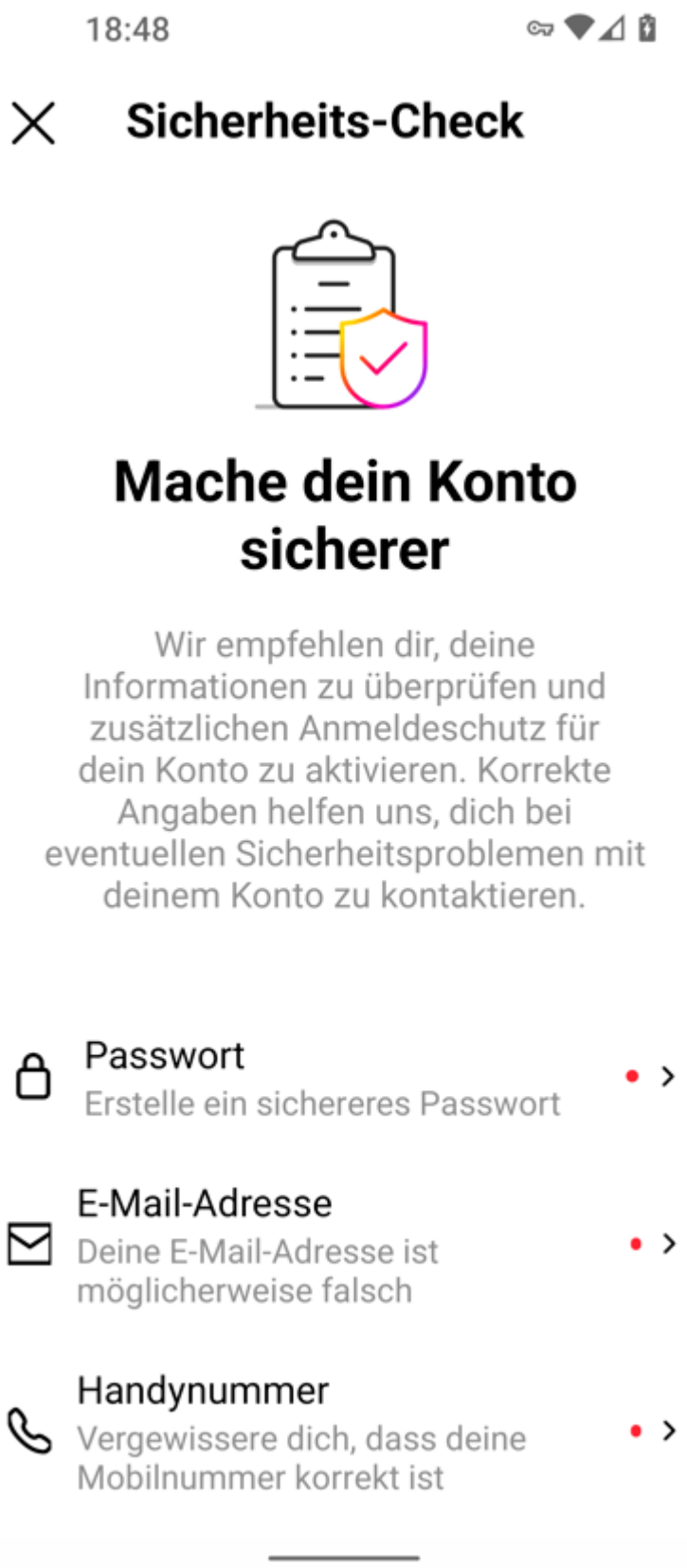
Instagram-Account absichern

Der beste Zeitpunkt, um sich um die Sicherheit Ihres Instagram-Accounts zu kümmern, ist genau jetzt, nicht später heute Abend oder am Wochenende. Sie müssen nur wenig Zeit investieren und ersparen sich früher oder später viel Ärger. Wenn Sie die von Instagram bereitgestellten Werkzeuge kennen

und nutzen, ziehen die meisten Angreifer unverrichteter Dinge zum nächsten Account weiter, der womöglich weniger gut abgesichert ist.

Den effektivsten Schutz gegen Phishing-Angriffe bietet die bereits erwähnte Zwei-Faktor-Authentifizierung (2FA), die Instagram „Zweistufige Authentifizierung“ nennt. In der Instagram-App aktivieren Sie den Schutz über den Menüknopf oben rechts und „Einstellungen/Sicherheit/Zweistufige Authentifizierung“, auf der Website klicken Sie in den Einstellungen auf „Privatsphäre und Sicherheit“, um die zweistufige Authentifizierung zu finden. Anschließend haben Sie die Wahl, ob Sie die zum Einloggen nötigen Zahlencodes per SMS zugeschickt bekommen möchten oder lieber selbst generieren wollen, mit einer Authenticator-App auf dem Smartphone.

Die SMS-Variante ist einfacher, aber auch unsicherer, weil es Angreifern gelingen kann, die SMS-Nachrichten mit den Codes abzufangen. Dennoch ist 2FA per SMS besser als nichts. Wir empfehlen die sicherere Variante „Authentifizierungs-App“, die sie jedoch nur mit der Instagram-App aktivieren können, nicht über die Website. Anschließend empfiehlt Ihnen Instagram geeignete Authenticator-Apps wie die von Google und erklärt Ihnen, wie Sie diese mit Ihrem Instagram-Account verknüpfen. Darüber hinaus sollten Sie ein langes Passwort für Ihren Account wählen, das nicht zu erraten ist und nur bei Instagram passt. Im besten Fall nutzen Sie einen Passwortmanager, um ein langes Zufallspasswort zu generieren und zu speichern.



Mit dem Sicherheits-Check überprüfen Sie die wichtigsten Security-Einstellungen bei Instagram.

Sicherheits-Check

Hilfreich ist der „Sicherheits-Check“, den Sie ebenfalls über die Sicherheitseinstellungen in der Instagram-App starten können. Diese Funktion macht auf gängige Sicherheitsprobleme wie ein schwaches Passwort aufmerksam und empfiehlt auch das Einschalten der 2FA, sofern sie nicht bereits aktiv ist. Zudem erinnert der Sicherheits-Check daran, dass man die Aktualität der hinterlegten Mailadresse und Telefonnummer kontrollieren sollte.

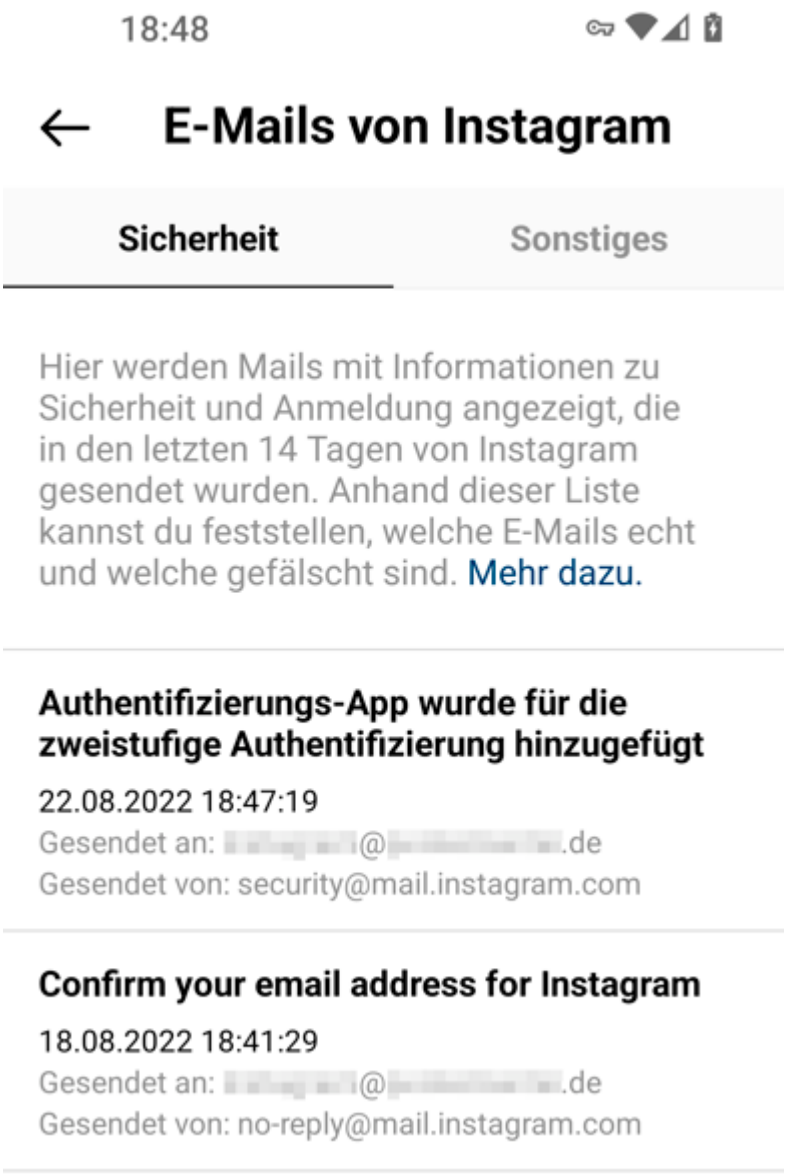
Wenn Sie Instagrams Betreiberfirma Meta diese Daten nicht anvertrauen möchten, funktionieren viele der Rettungsfunktionen von Instagram nicht, etwa weil das Unternehmen Ihnen im Fall der Fälle keinen Link zuschicken kann, über den Sie die Kontrolle über den gehackten Account zurückgewinnen können. Keine ganz leichte Abwägung, eventuell können Sie Instagram eine Zweit- oder Drittmailadresse zur Verfügung stellen – Hauptsache, Sie haben im Notfall sicher Zugriff darauf. Auch ein Profilfoto, auf dem Sie gut zu erkennen sind, kann die Rettung des Accounts erleichtern. Dazu gleich mehr.

Anti-Social-Engineering

Auch wenn Sie Ihren Account mit allen zur Verfügung stehenden Mitteln abgesichert haben: Technische Schutzmaßnahmen können Social Engineering nur erschweren, nicht verhindern. Angreifer hacken nicht Ihr Smartphone, sondern locken Sie trickreich in die Falle, etwa indem sie sich eben als Instagram-Support ausgeben und Sie mit einer plausibel klingenden Geschichte auffordern, Ihre Zugangsdaten auf einer externen Website einzugeben. Der zweite Faktor erschwert zwar einen solchen Phishing-Angriff, doch in jüngster Zeit fragen Online-Ganoven immer wieder auch nach dem temporären Einmalcode, mit dem sie den Account schließlich übernehmen können.

Allerdings können Sie sich vor dieser Form des Social

Engineering leicht schützen. Zunächst einmal sollten Sie sich darüber im Klaren sein, dass Sie Instagram niemals per Direktnachricht (Direct Message, DM) kontaktieren wird. Bei DMs ist Vorsicht geboten, auch wenn Sie den Absender kennen: Wurde ein Account gehackt, nehmen Angreifer schon mal Kontakt mit Freunden und Followern des Opfers auf, meist um die dazu zu bringen, eine gefährliche Website zu besuchen.



In der Instagram-App können Sie überprüfen, ob eine Mail, die angeblich von Instagram stammt, tatsächlich echt ist.

Mailcheck

Instagram kontaktiert Sie ausschließlich per Mail. Das wissen

allerdings auch die Cyber-Ganoven, sie verschicken täuschend echt aussehende Phishing-Mails im Instagram-Look. Wenn Sie eine Mail bekommen, die von Instagram stammen soll, sollten Sie sich also zunächst von der Echtheit überzeugen, bevor Sie die Mail ernst nehmen und auf einen Link aus der Nachricht klicken. Das ist bei Instagram erfreulich einfach: Öffnen Sie die Einstellungen in der App und tippen Sie auf „Sicherheit/E-Mails von Instagram“.

Dort listet die App alle Nachrichten auf, die Ihnen Instagram in den vergangenen 14 Tagen per Mail geschickt hat. Sie können die Nachrichten dort zwar nicht lesen, aber Sie erfahren Absender, Betreff und Sendedatum. Gleichen Sie diese Daten mit der Mail ab, um die Echtheit der Mail zu verifizieren. Der Absender sicherheitsrelevanter Instagram-Mails lautet stets security@mail.instagram.com. Wenn Sie auf Nummer sicher gehen wollen, dass der angegebene Absender nicht gefälscht ist, können Sie den Mail-Header inspizieren, wie in ct 19/2022 beschrieben [1].

Gehackten Account retten

Ist das Kind bereits in den Brunnen gefallen und Ihr Account wurde gehackt, dann müssen Sie schnell handeln. Je früher Sie aktiv werden, desto mehr Schaden können Sie abwenden. Nutzen Sie für sämtliche Rettungsversuche am besten ein Gerät, mit dem Sie bereits zuvor bei Instagram eingeloggt waren.

Beachten Sie die Mails von Instagram, um frühzeitig von einer Account-Übernahme zu erfahren. Der Dienst wird Sie über den Fremdlogin per Mail informieren und liefert Ihnen nicht nur den Zeitpunkt des Logins, Sie erfahren auch, welches Betriebssystem und welcher Browser mutmaßlich zum Einsatz kam. Zudem führt Instagram das Land an, aus dem die IP-Adresse des Nutzers stammt.

Auch wenn diese Daten nicht zu einhundert Prozent verlässlich sind: Sie eigenen sich gut, um darin Abweichungen zu Ihren

bisherigen Anmeldungen zu erkennen. Falls Ihnen bei der Kontrolle der Loginaktivität etwas komisch vorkommt, können Sie Ihren Account über den Link in der Mail („Sichere dein Konto hier“ oder „Secure your account here“) absichern. Achten Sie darauf, dass Sie auch tatsächlich auf https://www.instagram.com landen und nicht auf einer Phishing-Seite. Sie können über den Link ein neues Passwort setzen, das der Hacker nicht kennt. Überprüfen Sie von Zeit zu Zeit auch die „Login-Aktivität“ in den Sicherheitseinstellungen der App.

Informiert Sie Instagram ohne Ihr Zutun, dass Ihr Passwort oder die mit dem Account verknüpfte Mailadresse geändert wurde, sollten bei Ihnen die Alarmglocken läuten. Mit etwas Glück im Unglück können Sie aber auch in diesen Situationen die Kontrolle zurückgewinnen und die Änderung rückgängig machen, indem Sie in der Benachrichtigungsmail auf den Link „Sichere dein Konto hier“ klicken. Anschließend können Sie ein neues Passwort festlegen. Aber aufgepasst: Kontrollieren Sie auch in solch eiligen Fällen den Absender der Mail und das Ziel des Links genau, um sicherzustellen, dass es sich nicht um eine Phishing-Mail handelt. Geben Sie auf der verlinkten Seite nicht Ihr altes Instagram-Passwort ein.

Wurde der Account übernommen, kann ein Video-Selfie der letzte Ausweg sein.

Versteckter Rettungsweg

Für Härtefälle gibt es noch einen weiteren Rettungsweg über den Instagram-Support, der allerdings gut versteckt ist. Sie

erreichen ihn über die Instagram-App, indem Sie unterhalb des Login-Formulars auf „Erhalte Hilfe bei der Anmeldung“ tippen. Geben Sie oben Ihren Nutzernamen an und tippen Sie anschließend darunter auf „Du kannst dein Passwort nicht zurücksetzen?“. Die App fragt Sie daraufhin „Hast Du ein Foto von dir selbst in deinem Konto?“ – und das aus gutem Grund. Das Foto benötigt der Instagram-Support, um zu überprüfen, ob Sie der legitime Accountbesitzer sind. Falls Sie die Frage mit „Nein“ beantworten, ist Ihre Reise an dieser Stelle zu Ende und Sie landen im Hilfebereich.

Wenn Sie hingegen ein Foto in Ihrem Account haben und mit „Ja“ antworten, geht es weiter im Programm. Der genaue Ablauf variiert von Fall zu Fall. Instagram könnte Sie nach einem alten Passwort fragen und im darauffolgenden Schritt nach einem Bestätigungscode, den Sie sich an eine bei Instagram hinterlegte Mailadresse oder Handynummer schicken lassen können. Selbst wenn der Phisher die hinterlegten Daten geändert hat, stehen die Chancen gut, dass Sie hier noch Ihre wahre Rufnummer oder Mailadresse auswählen können und so an den Code kommen. Nach der Eingabe des Bestätigungscodes fragt Sie die App nach einer Mailadresse, über die Sie der Instagram-Support erreichen kann.

Video-Selfie

Haben Sie schließlich alle Hürden genommen, geht es ans Eingemachte: Die Instagram-App fordert Sie auf, Ihr Gesicht für ein sogenanntes Video-Selfie zu filmen. Im Rahmen dieses Vorgangs müssen Sie Ihren Kopf in vorgegebene Richtungen bewegen, um zu beweisen, dass Sie echt sind. Danach laden Sie das Video über den blauen „Senden“-Knopf hoch. Instagram beteuert, dass dieses Video maximal 30 Tage gespeichert wird und nicht zur Gesichtserkennung oder Speicherung biometrischer Merkmale genutzt wird. Wenn Sie das Video-Selfie hochgeladen haben, heißt es warten. Der Instagram-Support nimmt sich bis zu zwei Tage Zeit, um Ihr Anliegen zu bearbeiten.

Normalerweise geht es aber schneller. Nach der Überprüfung sendet Ihnen Instagram einen Link an die zuvor eingegebene Mailadresse, über den Sie ein neues Passwort festlegen können.

Falls Sie Ihren Facebook-Account mit Instagram verknüpft haben, gelten für diesen die gleichen Tipps: Nutzen Sie ein starkes Passwort, das nur bei Facebook passt, aktivieren Sie die Zwei-Faktor-Authentifizierung und achten Sie darauf, dass Ihre Kontaktdaten aktuell sind. Sie können zusätzlich die 2FA bei Instagram aktivieren, damit ein Angreifer, der bereits Kontrolle über Ihren Facebook-Account hat, nicht auch noch auf Ihr Instagram-Profil zugreifen kann.

Fazit

Instagram-Accounts stehen bei Cyber-Ganoven hoch im Kurs – insbesondere, aber nicht nur, wenn der begehrte blaue Haken das Profil ziert. Es ist daher wichtig, die Maschen der Angreifer zu kennen und frühzeitig geeignete Schutzmaßnahmen zu treffen. Wer sich nicht kümmert, riskiert sowohl, dass der Account gehackt wird, als auch, dass die vorhandenen Rettungsfunktionen ins Leere laufen, über die man die Kontrolle über einen gehackten Account zurückgewinnen könnte. *(rei@ct.de)*

1. Literatur
2. Ronald Eikenberg, E-Mails durchleuchtet, Phishing-Mails erkennen und abwehren, c’t 19/2022, S. 18
3. Niklas Dierking, Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c’t 9/2022, S. 18

Instagram-Hilfe zur Absicherung: ct.de/yqn6