Mehr Sicherheit gegen Missbrauch

Google-Konto. Mit der Bestätigung in zwei Schritten erhöhen Sie den Schutz für Ihr Benutzerkonto, indem Sie unerlaubte Zugriffe erschweren.

Die Anmeldung mit einem Benutzernamen und einem dazugehörigen Passwort ist im Internet gang und gäbe. Es handelt sich um die Minimalvariante der Absicherung von Online-Konten, die allerdings nicht ohne Restrisiko ist. Solche Zugangsdaten können mit etwas Aufwand ausgespäht oder geknackt werden. Deshalb haben einige Anbieter zur Erhöhung der Sicherheit einen (meist optionalen) Zwischenschritt eingeschoben – unabhängig davon, ob man sich auf dem Computer, Smartphone oder Tablet anmeldet. Die Rede ist von der Zwei-Faktor-Authentifizierung, auch: Zwei-Wege-Authentifizierung, Zwei-Schritt-Verifizierung, zweistufige Überprüfung, Bestätigung in zwei Schritten. Hier zählt die Kombination aus Benutzername und Passwort als erster Schritt der Anmeldung beim Benutzerkonto.

Aktive Bestätigung

Als zweiter Schritt folgt die aktive Bestätigung Ihrerseits, dass Sie tatsächlich gerade im Begriff sind, sich bei Ihrem Konto anzumelden. Dies geschieht durch die Übermittlung eines Einmalcodes (PIN) an Sie, den Sie dann händisch eingeben müssen. Die Zusendung des Einmalcodes erfolgt beispielsweise per SMS, E-Mail oder Push-Benachrichtigung an eine von Ihnen bekannt gegebene Telefonnummer, E-Mail-Adresse oder ein Gerät, auf dem Sie mit Ihrem Konto angemeldet sind. Weitere Möglichkeiten sind: ein automatisierter Anruf, bei dem Ihnen der Einmalcode in Form einer Sprachnachricht mitgeteilt wird; die Nutzung einer Authenticator-App (z.B. von Google oder Microsoft), welche ohne Mobilfunkverbindung auf Ihrem Smartphone Einmalcodes generiert; der (bisher weniger verbreitete) Einsatz eines externen Sicherheitsschlüssels, quasi eine Authenticator-App in Form eines USB-Sticks (z.B. von der Firma Yubico; der Zahlungsdienstleister PayPal vertreibt sogar eigene externe Codegeneratoren); oder die Nutzung Ihres eigenen Android-Smartphones als Sicherheitsschlüssel (siehe Online-Fassung dieses Artikels).

Wofür Sie sich letztlich entscheiden, ist nicht nur eine Frage persönlicher Präferenzen, sondern hängt auch davon ab, welche Möglichkeiten der jeweilige Anbieter überhaupt zulässt und welche auf Ihren vorhandenen Geräten technisch umsetzbar sind. Damit es nicht noch komplizierter wird, beschränken wir uns diesmal auf die Bestätigung in zwei Schritten bei Google. Google-Konten sind aufgrund der hohen Nutzerzahlen bei Android-Smartphones weit verbreitet, die zahlreichen Google-Dienste (Google-Suche, Google Maps, Gmail etc.) sind aber genauso bei iPhone- und Computernutzern beliebt.

Aktivierung

Das Einrichten der Bestätigung in zwei Schritten erfolgt über Ihr Google-Konto, wobei es unterschiedliche Wege dorthin gibt: Im Internetbrowser melden Sie sich unter https://myaccount.google.com an, auf dem Android-Smartphone oder -Tablet tippen Sie auf „Einstellungen/Google/Google-Konto“, und falls Sie eine Google-App am iPhone oder iPad nutzen, gelangen Sie innerhalb der jeweiligen App über das Menü und „Einstellungen/(Ihr Konto)/Google-Konto verwalten“ dorthin.

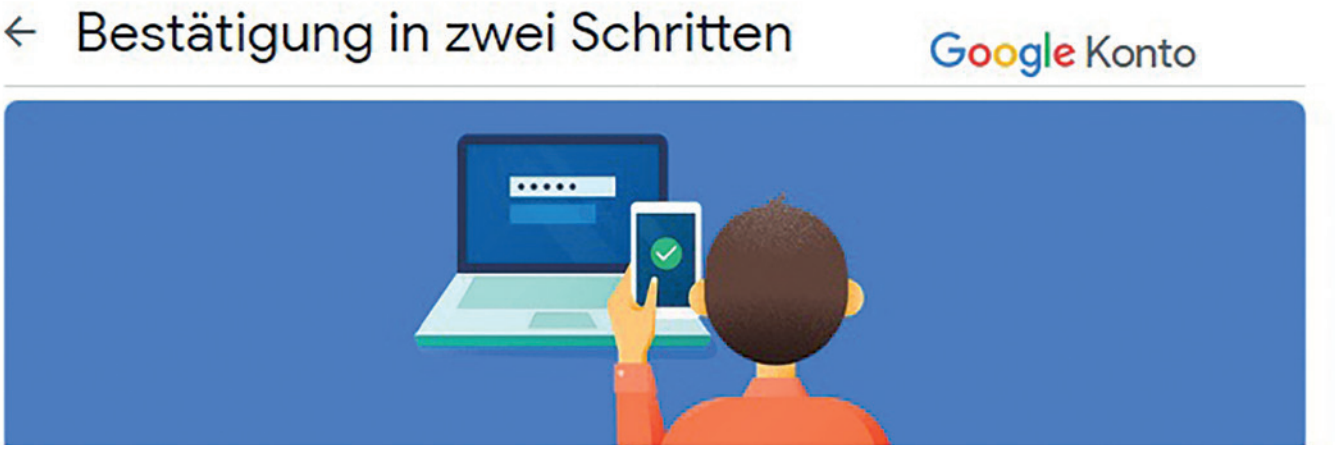
Klicken oder tippen Sie auf die Option „Sicherheit“ und unter der Überschrift „Bei Google anmelden“ auf „Bestätigung in zwei Schritten“. Mit „Jetzt starten“ beginnt die Einrichtung (möglicherweise erfolgt eine zusätzliche Identitätsprüfung, für die Sie Ihr Google-Passwort eingeben müssen). Sie befinden sich nun in der Option „Smartphone als zweiten Schritt bei der Anmeldung verwenden“. Es handelt sich um die Variante der Push-Nachricht an Ihr Gerät, welches Ihnen nun auch samt Marken- und Modellname angezeigt werden sollte. Unter „Andere Option auswählen“ können Sie als Alternativen einen vorhandenen externen Sicherheitsschlüssel (USB-Stick) wählen oder SMS-Nachrichten bzw. Telefonanrufe an Ihre Handynummer.

Wir entscheiden uns für die komfortable und – zumindest im Vergleich zu SMS und Anruf – als sicherer geltende Variante der Push-Nachricht und tippen/klicken auf „Jetzt ausprobieren“. Auf dem Display Ihres Smartphones erscheint die von Google stammende Anfrage, ob Sie gerade versuchen, sich auf einem anderen Gerät anzumelden. Stimmen die dortigen Angaben überein, bestätigen Sie mit „Ja“. Im nächsten Schritt werden Sie gebeten, eine Ersatzrufnummer anzugeben, falls die bevorzugte Variante nicht funktioniert.

Bedenken Sie, dass Sie das Gerät verlieren könnten und mit ihm die mit Ihrer Rufnummer verbundene SIM-Karte. Sie können später zwar zusätzlich Ihre eigene Handynummer hier angeben. Sinnvollerweise wählen Sie aber zunächst die eines gut erreichbaren Verwandten oder Freundes. An diese Nummer wird nun ein Einmalcode

Nachfrage deaktivieren

Da die Bestätigung in zwei Schritten mitunter als lästig empfunden wird, wird einem z.B. bei der Anmeldung im Browser angeboten, die Abfrage von Einmalcodes auf „vertrauenswürdigen“ Geräten (also etwa dem Stand-PC zu Hause) zu deaktivieren. Die entsprechende Option ist bei Google leider standardmäßig angehakt, während es bei anderen Anbietern sinnvollerweise genau umgekehrt ist. Seien Sie jedenfalls nicht zu großzügig damit, denn auf diese Weise wird ja die zweistufige Bestätigung auf dem jeweiligen Gerät bzw. im verwendeten Browser ausgehebelt. Die Liste der Geräte, auf denen Sie – bewusst oder unbewusst – zugestimmt haben, verwalten Sie unter „Bestätigung in zwei Schritten“ in Ihrem Google-Konto.



geschickt, durch dessen Eingabe Sie die Einrichtung der Bestätigung in zwei Schritten abschließen. Als Alternative zur Ersatzrufnummer stehen Ersatzcodes (Backup-Codes) zur Verfügung, die Sie – falls Ihre Wahl auf diese Option fällt – auf einem anderen Gerät (z.B. Ihrem Computer) abspeichern und/oder auf Papier ausdrucken und sicher verwahren sollten.

Authenticator

Über den Menüpunkt „Bestätigung in zwei Schritten" in Ihrem Google-Konto können Sie jederzeit Einstellungsänderungen vornehmen oder zusätzliche Bestätigungsmethoden einrichten. Eine praktische Möglichkeit ist eine Authenticator-App für Ihr Smartphone. Laden Sie z.B. den Google Authenticator (Anbieter: Google LLC) aus dem Play Store herunter.
Achtung! Für die Einrichtung dieser App können Sie zwar auch Ihr Smartphone verwenden, wesentlich komfortabler verläuft dies aber, wenn Sie die weiteren Schritte auf einem Computer, Tablet oder einem anderen Smartphone durchführen, wo Sie über den Internetbrowser in Ihr Google-Konto einsteigen.
Tippen oder klicken Sie in Ihrem Google-Konto unter der Überschrift „Authenticator App" auf „Einrichten", geben Sie an, ob Sie ein Android-Gerät oder ein iPhone besitzen, und tippen Sie auf „Weiter". Nun öffnen Sie auf Ihrem Smartphone den Google Authenticator, tippen auf „Starten", lesen oder überspringen die Einführung und wählen dann

– **„Barcode scannen"**, sofern Sie zwei Geräte zur Verfügung haben. Halten Sie nun die Kamera des Smartphones vor den auf dem zweiten Gerät angezeigten Barcode (bei dem es sich genau genommen um einen QR-Code handelt), und der Rest erfolgt automatisch.

– **„Schlüssel eingeben"**, falls Sie lediglich Ihr eigenes Smartphone zur Hand haben.

In diesem Fall tippen Sie unterhalb des angezeigten Barcodes auf „Sie können ihn nicht scannen?" und notieren sich der Übersichtlichkeit halber den 32-stelligen Schlüssel. Diesen sowie Ihre E-Mail-Adresse geben Sie nun im Authenticator ein. Unterhalb davon belassen Sie die Option „Zeitbasiert". Bestätigen Sie die Eingabe.
Der Google Authenticator zeigt Ihnen nun an, dass das Konto erfolgreich hinzugefügt wurde. Unterhalb sehen Sie einen sechsstelligen Bestätigungscode, der alle 60 Sekunden erneuert wird. Geben Sie einen dieser Codes innerhalb dieser 60 Sekunden auf Ihrem Google-Konto ein (dort zuvor auf „Weiter" tippen/klicken). Somit ist der Google Authenticator fertig eingerichtet. Der Vorteil einer Authenticator-App: Sie können dort weitere Konten hinzufügen, beispielsweise von Amazon, Facebook, Microsoft oder PayPal.

Glossar

Push-Benachrichtigung. Eine via App gesandte Mitteilung, die sofort auf dem Smartphone-Display aufscheint, auch wenn die betreffende App geschlossen ist.

Barcode. Auch als Strich- oder Balkencode bezeichnet. Enthält Informationen zu dem Produkt, auf dem er sich befindet, z.B. für Lagerhaltung, Versand oder Verrechnung.

QR-Code. QR = quick response = schnelle Antwort. Enthält meist Informationen in Form von Textnachrichten oder Internetlinks, siehe auch KONSUMENT 2/2019.

Rat und Hilfe für Verbraucher in Europa ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.

MEHR ZUM THEMA

Unter www.konsument.at/google-bestaetigung082019 finden Sie zusätzliche Informationen zu den Themen „Android-Smartphone als Sicherheitsschlüssel" und „App-Passwörter".