

Das sollte man über die Passwort-Alternative Passkey wissen

Die Anmeldung in Internetkonten soll dank Passkey einfacher und vor Hackern sicher sein. Bequemer ist Passkey bereits – sicherer nicht.

Wer sich bei einem Internetkonto anmeldet, braucht dazu normalerweise seinen Benutzernamen und ein Passwort. Bei vielen Programmen erscheint die Frage, ob man stattdessen einen sogenannten Passkey einrichten will. So ist es aktuell etwa bei Google, Microsoft und Amazon, aber auch beim Login ins Benutzerkonto der Migros oder bei der

App der Krankenkasse Helsana. Passkey ist eine neue Anmelde-möglichkeit für Konten im Internet. Sie soll künftig das An-melden mit Passwort ersetzen.

Wie funktioniert Passkey?

Mit Passkey wird das Internet-konto direkt mit einem be-stimmten Handy oder Compu-ter verbunden. Die Internetseite erkennt mittels Passkey, dass ein Benutzer das verbundene Gerät verwendet, und meldet diesen an – ganz ohne Passwort. Das funktioniert, weil beim Ein-richten von Passkey auf dem Handy oder Computer ein ge-heimer Schlüssel gespeichert wird, also eine sehr lange, kom-

plexe Zeichenfolge. Ein zweiter Schlüssel liegt auf dem Portal, auf dem man sich anmelden will – zum Beispiel bei Google oder Amazon. Beim Anmelden werden automatisch die beiden Schlüssel abgeglichen. Passen sie zueinander, erfolgt die Anmeldung. Zusätzlich wird auf Handys meist noch die Bestäti-gung via Gesichtserkennung, Fingerabdruck oder PIN ver-langt, bevor die beiden Schlüs-sel abgeglichen werden.

Was sind die Vorteile?

Hinter dem Passkey steckt die FIDO Alliance, das ist eine Ver-einigung von grossen US-Tech-nologiekonzernen wie Apple,

Google oder Microsoft. Ent-sprechend bewirbt etwa Google den Passkey mit der Aussage, er sei «einfacher und sicherer». Mit einfacher ist gemeint: Man muss sich kein Passwort mehr merken. Sicherer ist der Pass-key, weil er anders als ein Pass-word nicht zu einfach oder zu kurz sein kann. Also schützt der Passkey auch vor unbefugtem Zugriff auf Benutzerkonten durch gehackte oder gestohlene Passwörter. Auch das Anmelden auf gefälschten Internetseiten – indem man auf Links in Phishing-E-Mails klickt – klappt dann nicht mehr, weil auf die-sen Internetseiten der nötige Schlüssel nicht vorhanden ist.

Verschiedene Anmeldemethoden im Sicherheits-Check



Spezialschlüssel:

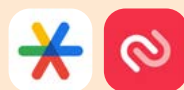
Sehr hohe Sicherheit. Man steckt bei der Anmeldung einen Spezialschlüssel wie den «Yubikey» (Bild) in den PC oder ins Handy. Mit Passwort und Schlüs-sel zusammen meldet man sich an. Im Gegen-satz zu den anderen Me-thoden, die gratis sind, kostet ein «Yubikey» ein-malig 50 bis 90 Franken.

Bewertung:



Passkey: Wenn man die Anmeldung mit Passwort deaktivieren kann, ist diese Methode sehr sicher. Wenn man das Passwort beibehalten will, sollte man zumindest komplexe, lange Passwörter mit vielen Sonderzeichen und Zahlen verwenden.

Bewertung:



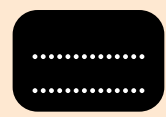
Authentifizierungs-App: Hohe Sicherheit. Benötigt Spezial-Apps wie «Google Authenticator» (linkes Symbol) oder «Authy». Man muss die App mit dem Konto in den Konto-einstellungen verknüpfen. Danach erstellt die App einen ständig wechseln-den Zahlencode, den man bei der Anmeldung einge-ben muss.

Bewertung:



SMS: Mittlere Sicherheit. Man erhält per SMS einen Code, den man beim Anmelden eingeben muss. Theoretisch kann das SMS von Fremden abgefangen werden.

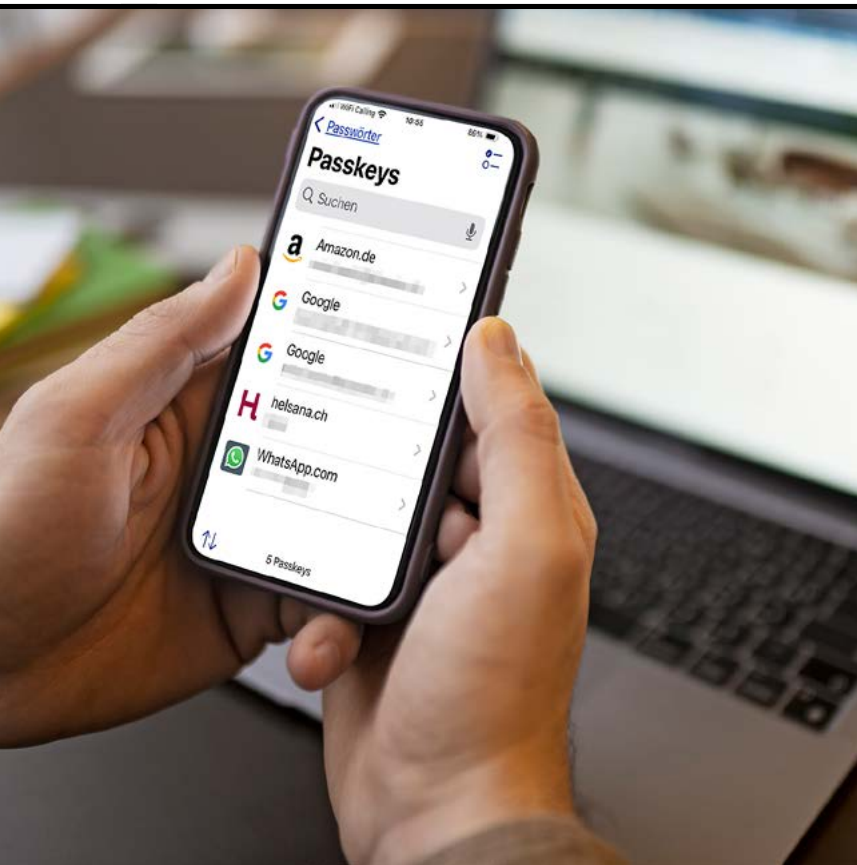
Bewertung:



Benutzername und Passwort: Unsicher. Werden Konten auf Inter-netseiten gehackt, können die Passwörter in falsche Hände gelangen. Zudem können Computer inner-halb von Sekunden ein-fache Passwörter kna-cken. Daher sollte man unbedingt lange, kompli-zierte Passwörter mit Buchstaben, Sonderzei-chen und Zahlen wählen.

Bewertung:





Passkey: Verbindet Internetkonto direkt mit ausgewähltem Handy

Allerdings bieten Internetfirmen den Passkey nur als eine von mehreren Anmeldemöglichkeiten an. Bei Amazon, Google, Swiss ID oder Migros kann man sich auch nach dem Einrichten des Passkeys weiterhin einfach mit Passwort und Benutzernamen anmelden.

Gibt es auch Nachteile?

Ja. Die Funktion ist an das verwendete Gerät gebunden. Ist dieses defekt oder wird es gestohlen, muss man auf anderem Weg versuchen, Zugang zu seinem Konto zu erhalten. Das kann zum Problem werden, wenn die Passwortanmeldung deaktiviert ist. Eine Möglichkeit: Die Passkey-Schlüssel lassen sich mit der Cloud von Apple oder Google synchronisieren. Aktiviert man die Cloud auf einem anderen Gerät, hat man wieder Zugriff auf den Passkey. Aber dieses Vorgehen setzt den Gebrauch einer Cloud voraus, was den Datenschutz verringert.

Eine andere Variante: Man richtet auf mehreren Geräten einen Passkey für das Konto ein. Zum Beispiel auf dem Handy und dem Computer. So hat man trotz einem Geräteverlust weiterhin Zugang zum Konto.

Können Fremde trotz Passkey auf meine Konten gelangen?

Ja, wenn sie Zugang zum Gerät haben, auf dem ein Passkey gespeichert ist. Daher ist ein besonders sicheres und langes Anmeldepasswort für das Gerät wichtig. Bei Handys funktioniert Passkey meist mit der eingebauten Gesichtserkennung oder dem Fingerabdruck, falls jemand diese Funktionen benutzt. Wenn das nicht klappt - etwa wegen Dunkelheit oder nassen Fingern - kann man bei den meisten Handys als Bestätigung den Anmelde-PIN eingeben. Es ist also wichtig, dass der Handy-PIN komplex genug und damit sicher ist.

Marc Mair-Noack

Frage & Antwort



Marc Mair-Noack

Wie vergrössere ich die Schriften auf dem Mac?

«Mit meinem neuen Monitor ist die Auflösung hoch – und die Schriften auf dem Mac sind entsprechend klein. Wie kann ich Texte in Menüs oder Programmen wieder vergrössern?» Öffnen Sie die Systemeinstellungen und dort die «Bedienungshilfen». Unter «Anzeige» gibt es einen Abschnitt «Text». Klicken Sie dort auf «Textgrösse». Hier können Sie die Buchstaben-grösse für verschiedene Programme anpassen. Zum Beispiel für das E-Mail-Programm oder den Kalender. Ändern Sie die Textgrösse bei «Finder», ändert sich die Schrift- und auch die Ordnergrösse auf dem Desktop.

Wie zügle ich die Lesezeichen von Chrome zu Firefox?

«Ich möchte künftig statt mit dem Chrome-Browser mit Firefox ins Internet. Wie zügle ich meine Lesezeichen auf Firefox?»

Lesezeichen lassen sich zwischen verschiedenen Browsern einfach austauschen. Klicken Sie in Chrome auf die drei Punkte rechts oben, dann auf «Lesezeichen und Listen» → «Lesezeichenmanager». In diesem Fenster wählen Sie die drei Punkte oben rechts gleich unterhalb des vorherigen Menüs und klicken auf «Lesezeichen exportieren». Nun geben Sie einen Speicherort an. Die Liste mit den Lesezeichen wird als HTML-Datei gespeichert. Im Firefox klicken Sie auf die drei Striche oben rechts, dann auf «Lesezeichen» → «Lesezeichen verwalten». Im neuen Fenster klicken Sie auf das Symbol mit den zwei Pfeilen, dann auf «Lesezeichen von HTML importieren». Wählen Sie nun die gespeicherte Datei aus.



Was wollten Sie zum Thema Multimedia schon lange wissen?

Schreiben Sie an: redaktion@saldo.ch, Betreff «Multimedia-Fragen»