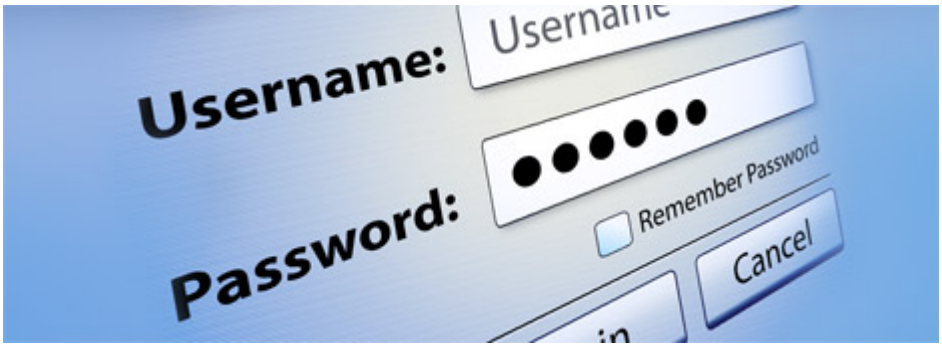
Passwörter ändern von Amazon bis Xbox

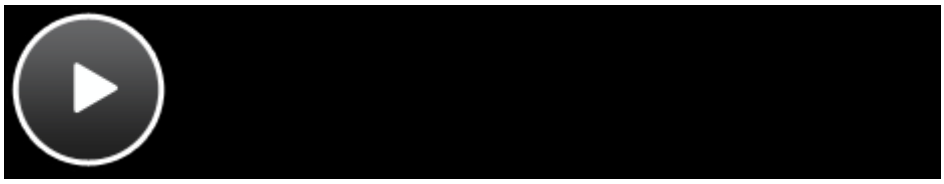
Von Claudio Müller, Jörg Geiger und Michael Humpa, 07.05.2015

Schmeißen Sie Ihre Passwörter weg. Der Grund, Passwörter sind nur dann sicher, wenn man sie regelmäßig ändert. Als Faustregel gilt: Nach sechs Monaten sollten Sie ein Passwort ändern. Wir zeigen, wie das am einfachsten geht.



Lesen Sie in diesem Beitrag:

Video: Hackademy: So wählen Sie ein sicheres Passwort



00:00 02:02

Hackademy: So wählen Sie ein sicheres Passwort

*space*play / pause

*q*unload | stop

*f*fullscreen

shift + ←→slower / faster (latest Chrome and Safari)

↑↓volume

*m*mute

←→seek

. seek to previous

12…6 seek to 10%, 20%, …60%

Bei Passwörtern und Zahnarztbesuchen gilt: Alle sechs Monate muss man ran, dann tut es auch nicht weh. Also auch wenn es erstmal schwer fällt, ändern Sie jetzt Ihre Passwörter und tun Sie damit viel für die Sicherheit Ihrer Daten. Der Grund: Neben sicheren Passwörtern ist auch der regelmäßige Wechsel ein wichtiger Teil jeder Sicherheitsstrategie.

Passwort ändern - so geht's	
Amazon Passwort ändern	AOL Passwort ändern
Ebay Passwort ändern	Facebook Passwort ändern
Freenet Passwort ändern	Fritzbox Passwort ändern
GarantiBank Passwort ändern	Gmail Passwort ändern
GMX Passwort ändern	Hotmail / Outlook / Skype Passwort ändern
Origin Passwort ändern	Paypal Passwort ändern
PlayStation Network Passwort ändern	Postbank Passwort ändern
Speedport Passwort ändern	Steam Passwort ändern
T-Online Passwort ändern	Targobank Passwort ändern
Vodafone Passwort ändern	Web.de Passwort ändern
Windows Passwort ändern	Xbox Passwort ändern
Yahoo Passwort ändern	

Passwort automatisch ändern

Der Grund, warum viele Nutzer das regelmäßige Andern von Passwörtern sein lassen, ist der Aufwand. Hat man zehn

oder noch mehr Passwörter, alle natürlich unterschiedlich und sicher, dann ist man in der Regel froh, wenn man sich diese merken kann. Dann jede einzelne Webseite ansurfen, in die Kontoeinstellungen wechseln und ein neues Passwort eingeben, ist aufwändig. Einfacher machen es Passwort-Manager. So kann beispielsweise LastPass auch in der kostenlosen Version Passwörter automatisch ändern. Sie müssen dazu nur den entsprechenden Eintrag des Dienstes in LastPass anklicken und danach auf "Passwort automatisch ändern" klicken. Auf rund 75 Webseiten, darunter Facebook, Twitter, Amazon oder Pinterest funktioniert die automatische Passwort-Anpassung bereits.

Sicheres Passwort: Das ist nicht zu knacken?

07.05.2015

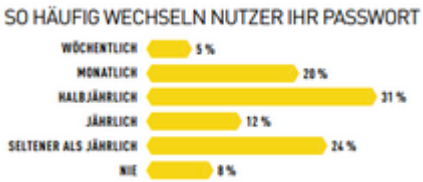
Dummerweise sind Sie bei Webdiensten auf Passwörter angewiesen, denn andere Möglichkeiten bieten die meist nicht. Doch ein sicheres, aber leicht zu merkendes Kennwort zu erstellen, ist leicht - wenn man die Tricks der Hacker kennt.

Fotostrecke: Die 25 schlechtesten Passwörter

Top 80: Die beliebtesten Passwörter.

Verwenden Sie keine echten Wörter, nicht einmal dann, wenn Sie etwa das "i" durch eine "1" oder das "E" durch eine "3" ersetzen. Bei Angriffen mit einem festen Passwortbestand (Wörterbuchattacken) probieren Passwortknacker inzwischen selbst diese Varianten automatisiert durch. Auch zu kurz sollte das Kennwort nicht sein. Denn sogar kryptische Zeichenketten knacken Brute-Force-Angriffe in weniger als einer Minute, wenn sie nur sechs Zeichen lang sind - laut How Secure Is My Password.
Und vor allem sollten Sie nie ein Passwort mehrfach verwenden. Knackt der Hacker diesen Generalschlüssel auf einer Seite, wären dann auch Ihre anderen Accounts gefährdet.

Eine leicht anwendbare Passwortstrategie verrät uns Markus Jakobsson, leitender Wissenschaftler für Nutzersicherheit bei PayPal. Sein Tipp: "Kombinieren Sie ein Masterpasswort mit einem seitenspezifischen Passwort. "DasMasterpasswort - zum Beispiel Hc84# (keineInitialen oder Ihr Geburtsdatum!) - ergänzen Sie mit einer für jede Website einzigartigen Zeichenkette. "Vermeiden Sie dabei vorhersehbare Zeichen, etwa den Namen der Seite", sagt Jakobsson. Nehmen Sie stattdessen etwa "Ozean*8" für Facebook (abgeleitet vom Facebook-Blau und der Zeichenzahl des Dienstes). Die seitenspezifischen Passwortteile können Sie laut Jakobsson aufschreiben und in Ihrer Brieftasche oder zu Hause aufbewahren - bloß nie zusammen mit dem Masterpasswortteil.



Accountsicherheit: Regelmäßig Passwort ändern.

Hacker sind mindestens so clever wie Sie

Ähnlich kreativ sollten Sie auch die Sicherheitsfragen zur Passwortwiederherstellung beantworten, die oft Teil der Registrierung bei einer Website sind. Ihre Lieblingsfarbe ist Rot? Das errät jeder Angreifer. Auch hier lässt sich die Jakobsson-Strategie anwenden. Die Lieblingsfarbe könnte dann etwa lauten: Ma+§Bordeauxrot§ (Ma für Mailaccount). Wenn Sie für die Passwortwiederherstellung zudem eine alternative Mailadresse angeben können, tun Sie das. Am besten legen Sie sich eine ausschließlich für diesen Zweck an.

Damit Ihnen im Worst-Case-Szenario, dem gehackten E-Mail-Konto, keine KettenreaktionAccounts droht, sollten Sie dieses Konto besonders schützen. Die Mailadresse ist nicht nur der Anker Ihrer digitalen Identität. Sie ist bei vielen Webdiensten auch der Nutzername und dient der Passwortwiederherstellung. Wer Ihren Mailaccount kontrolliert, kann sich also bei vielen Diensten problemlos die Log-in-Daten zuschicken lassen. Damit kauft er zum Beispiel mit Ihren hinterlegten Bezahlinformationen im Onlineshop ein, sieht Ihre persönlichen Fotos im Webspeicher an oder tritt in Ihrem Namen in sozialen Netzwerken auf. Ein Horrorszenario.

Password Generator: Online und als Download

Ein Passwort Generator hat nur eine Aufgabe, ein sicheres Passwort erzeugen. Doch das ist gar nicht so einfach, denn damit ein Passwort wirklich sicher ist, darf es keine "echten" Wörter oder Wortteile enthalten. Auch Namen oder Geburtsdaten sind in Passwörtern tabu, was gefragt ist, sind zufällige Zeichenfolgen mit einem Mix aus Groß- und Kleinschreibung sowie Sonderzeichen und Ziffern. Lassen Sie also Passwörter wie "123abc", "admin" oder "qwertz" links liegen und steigen Sie in die Liga von "_ejbxÄ.=z+x>" oder "u7DäPogFHH]B" auf. Doch selbst ausgedachte Passwörter, auch wenn sie zufällig erscheinen, sind oft alles andere als wirklich zufällig. Ein Passwort Generator greift Ihnen unter die Arme.

Passwort Generator online: Ohne Installation erzeugen Dienste auch online sichere Passwörter.

Passwort Generator Online

Am einfachsten funktioniert ein Passwort Generator Online. Sie besuchen einfach nur eine Webseite, lassen sich ein sicheres Passwort generieren und verwenden es bei einem Dienst. Doch Vorsicht: Ein schaler Beigeschmack bleibt bei diesen Diensten, denn mit bösen Absichten könnte der Betreiber natürlich auch ein online generiertes Passwort einfach mitschneiden. Ein vertrauenswürdiger Dienst ist Passwort Generator Online.

Zur Web-App: Password Generator Online

Einfach: PWGen erzeugt schnell und einfach sichere Passwörter.

Passwort Generator Download

Wenn Sie einen Passwort Generator als Download bevorzugen, gibt es zwei Möglichkeiten. Passwort Manager wie KeePass haben bereits einen Passwort Generator integriert. Damit erzeugen Sie also nicht nur sichere Passwörter, sondern speichern diese auch gleich ab. Wenn es nur um das Erzeugen von Passwörtern geht, haben wir aber auch einen reinrassigen Passwort Generator als Download im Angebot, PWGen. Die Freeware erstellt in Sekundenschnelle sichere Passwörter, etwa für eBay, GMail oder PayPal. Komfortabel können Sie dabei die Komponenten und Länge des Passworts wählen und mit nur einem Mausklick erzeugen. (jg)

Downloads: PWGen KeePass

Passwortkarte

Mit der Passwortkarte haben Sie all Ihre wichtigen Kennwörter immer dabei - völlig sicher!

Das Prinzip hinter der Passwortkarte ist simpel aber genial: Per Zufalls-Generator spuckt Ihnen die Webseite des Herstellers eine individuelle Anordnung von Groß- und Kleinbuchstaben sowie Zahlen aus. Diese sind wild durcheinander auf einer großen Tabelle verteilt.

Die Passwortkarte wird als downloadbare und vor allem druckbare PDF-Datei ausgegeben. Um Passwörter nun zu bestimmen, wählen Sie einfach eine Koordinate, Länge sowie Richtung aus. Dies können Sie sich sicher auf einem Zettel notieren.

Die mit der Passwortkarte erstellten Passwörter sind um einiges sicherer als von Personen gewählte Passwörter, da diese keine persönlichen Daten wie Geburtsdatum, Namen oder Telefon-Nummern enthalten.

Fazit: Die Passwortkarte ist eine pfiffige Möglichkeit, schwer knackbare Passwörter zu finden, die gleichzeitig sicher und von Nutzern einfach zu merken sind.

Hinweis: Der Download-Link verweist Sie direkt auf die Seite des Herstellers, auf der Sie mehrere Varianten von Passwortkarten herunterladen können.

http://www.chip.de/downloads/c1_downloads_auswahl_31494484.html?t=1431086041&v=3600&s=733d3621e294322c4564652d04b56629

E-Mail: Doppelt schützt besser

07.05.2015

Es ist vollkommen unverständlich, warum nicht alle E-Mail-Provider eine zweite Sicherheitsstufe neben dem Passwort anbieten. Sicherheitsexperten nennen das Single Point of Failure, denn wer das E-Mail-Passwort kennt, kann den Account übernehmen.

Fotostrecke: Die besten kostenlosen Sicherheits-Tools

Doppelt sicher: Die Zwei-Faktor-Authentifizierung.

Nur wenige Anbieter unterstützen die Zwei-Faktor-Authentifizierung. Neben dem Passwort müssen Sie sich dabei mit einem meist achtstelligen Zahlencode authentifizieren. Den bekommen Sie entweder per SMS zugeschickt oder erzeugen ihn mit einer App auf dem Smartphone. Wer sich einmal so authentifiziert hat, kann das dabei verwendete Gerät als vertrauenswürdig definieren. Bei zukünftigen Log-ins an diesem Gerät genügt dann wieder das normale Passwort. Bei Anmeldeversuchen von einem unbekannten Gerät bekommen Sie aber eine SMS zugeschickt. Und so haben Sie gleichzeitig ein Warnsignal, ob sich irgendjemand in Ihren Mailaccount hacken will.

In Google, neben Yahoo und Microsoft einer der großen Mailanbieter mit Zwei-Faktor-Authentifizierung, richten Sie die Methode so ein: Klicken Sie im

Gmail-Postfach auf den Pfeil rechts oben und wählen Sie »Konto |Sicherheit| Bestätigung in zwei Schritten | Einstellungen«. Ein Assistent führt Sie durch die weiteren Schritte. Halten Sie dabei das Handy parat, um den ersten Code per SMS zu empfangen. Bei anderen Anbietern finden Sie diese Einstellungen üblicherweise im Nutzerkonto unter »Sicherheit« oder »Kontoeinstellungen«.

Leider lässt sich Twitters Zwei-Faktor-Anmeldung laut dem Sicherheitsexperten Sean Sullivan vom Virenschutzanbieter F-Secure mit einigen simplen Tricks aushebeln: Grund dafür ist ein Twitter-SMS-Feature. Ein Twitter-User kann sich Tweets per SMS zustellen lassen. Dieser Service kann per SMS ein- und ausgeschaltet werden. Wird der Service per SMS abbestellt, sind ab sofort alle SMS-Benachrichtigungen ausgeschaltet, darunter auch die Zwei-Faktor-Authentifizierung.

OpenID: Mit einem Login überall anmelden.

Starke Authentifizierung - Sicher einloggen

Eine zweite Sicherheitsstufe bedeutet natürlich: weniger Komfort. Zudem dürfen Sie nicht vergessen, die hinterlegte Mobilnummer zu ändern, wenn Sie mal eine neue haben. Eine bequemere Lösung sind Passwortsafes, zum Beispiel LastPass. LastPass speichert Ihre Log-in-Daten in einem mit 256 Bit verschlüsselten und per Masterpasswort geschützten Onlinespeicher. Übersynchronisierte Browser-Plug-ins und Apps können Sie sich damit auf allen Geräten in Ihre Webkonten einloggen. Auf Wunsch füllt LastPass die Log-in-Felder automatisch aus. Das hat zwei Vorteile: Sie brauchen sich keine Passwörter mehr merken, und Keylogger-Trojaner können keine Passworteingaben von der Tastatur mitschneiden. Das große Risiko von Passwortsafes: Wer Ihr Masterpasswort klaut (vom PC oder vom Server des Anbieters), kennt all Ihre Log-in-Daten.

Ähnlich bequem sind OpenID-Verfahren, bei denen Sie sich eine universell nutzbare persönliche Kennung generieren lassen können, meist in Form einer URL. Diese URL geben Sie dann statt des Passworts ein. Ein echter Sicherheitsgewinn, denn jede Passworteingabe ist ein Sicherheitsrisiko. OpenID-Lösungen sind elegant, wenn auch nur so sicher wie die Server der Anbieter. Neben Google, Facebook oder Mozilla gibt es auch unabhängige wie my OpenID. Der einzige Nachteil: Sie können OpenIDs nur auf Seiten nutzen, die das Verfahren unterstützen - und das sind aktuell nicht sehr viele.

Passwort Manager kostenlos: Freeware laden

Passwort Manager gibt es kostenlos zum Download. Der Hauptzweck: Sie gewährleisten, dass Sie für jeden Dienst ein eigenes und sicheres Passwort verwenden können. Unsere Empfehlung ist die OpenSource-Software KeePass. KeePass ist Freeware und für Windows und unter dem Namen KeePassX auch für Mac erhältlich. Außerdem gibt es Apps für iOS und Android. Wichtig: Die Mac-Version unterstützt nur das alte Datenbankformat der Version 1.x. Wer also unter anderem auf einem Mac seine Passwörter nutzen will, muss auch auf anderen Systemen die alten Datenbanken verwenden.

Doppelschutz: Neben Masterkey können Sie auch ein Key-File zum Entschlüsseln verwenden.

Passwort Manager Freeware mit AES

Die Passwörter landen in einer verschlüsselten Datenbank, die Sie mit einem Masterpasswort schützen. Sie müssen sich also nur noch ein Passwort merken, mit dem schließen Sie die Datenbank auf und haben dann Zugriff auf alle anderen Passwörter. Gegen unbefugten Zugriff stellt KeePass eine AES-Verschlüsselung mit 256 Bit. Das Masterpasswort wird nicht in KeePass gespeichert, es dient nur als Input für eine SHA-256-Hashfunktion. Auch der komplette Prozess von KeePass wird verschlüsselt, sodass sich keine Daten aus dem Arbeitsspeicher klauen lassen. Für zusätzlichen Schutz kann man ein Keyfile auf einem USB-Stick speichern, das zum Entsperren der Datenbank neben dem Masterpasswort nötig ist.

Sichere Passwörter: KeePass erzeugt auf Wunsch auch sichere Passwörter.

Komfort-Features schützen Passwörter

Nett bei KeePass ist, dass es clevere Komfort-Features gibt, die das Hantieren mit den Passwörtern einfacher machen. So können Sie mit KeePass Login-Dateien automatisch einfüllen lassen. Außerdem erzeugt KeePass auf Wunsch auch sichere Passwörter. Dabei können Sie Länge und auch die verwendeten Zeichen auswählen und per Mausklick Passwörter zufällig erzeugen lassen. (jg)

Download: KeePass KeePassXKeePassDroid

Windows: Passwort für die Hosentasche

07.05.2015

Mit den bereits genannten Passwortregeln können Sie auch die Windows-Parole kreieren und so Ihren Rechner schützen. Doch statt es über die Tastatur einzugeben, sollten Sie einen USB-Stick als virtuellen Schlüssel verwenden. Den können Sie wie einen echten immer bei sich tragen.

Fotostrecke: Die besten kostenlosen Sicherheits-Tools

BitLocker: USB-Sticks sicher verschlüsseln.

Seit Windows Vista bietet Microsoft dafür eine integrierte Lösung an, allerdings nur in den Versionen Ultimate und Enterprise (beziehungsweise Windows8Pro). Mit der BitLocker-Laufwerksverschlüsselung kodieren Sie Ihre Datenpartition und schützen sie entweder per PIN-Code oder perStick (unsere Empfehlung). Der USB-Stick enthält dabei eine Schlüsseldatei, die das Laufwerk entsperrt, sobald Sie den Rechner starten. Einrichten können Sie dies unter »Systemsteuerung | System und Sicherheit | BitLocker-Laufwerksverschlüsselung«. Folgen Sie nach einem Klick auf »BitLocker aktivieren« einfach der Einrichtungsroutine.

Wer BitLocker nicht nutzen kann, installiert das Tool USBLogon. In dem Tool wählen Sie den USB-Stick aus und legen fest, ob der Log-in automatisch erfolgt, wenn der Stick angeschlossen ist, und was der Rechner tun soll, wenn Sie den Stick abziehen (etwa Standby, runterfahren oder Bildschirmschoner). Der Stick meldet Sie dann in Windows an. Lediglich auf die Festplattenverschlüsselung von BitLocker müssen Sie verzichten. Mit dem Tool TrueCrypt können Sie die aber selbst nachrüsten.

Downloads: USBLogon
TrueCrypt

Smartphone: Verräterische Schmierfinger

07.05.2015

Nach Webdiensten und dem Rechner bleibt jetzt nur noch, Ihre Mobilgeräte zu schützen. Die bewahren nahezu unser gesamtes digitales Leben in komprimierter Form in ihrem Flashspeicher - und sind oft absurd schwach geschützt.

Fotostrecke: 15 Must have Security-Apps für Android

Swipe: Die Wischgesten sind simpel und damit gefährlich.

Gegen einige ihrer Sicherheitslücken ist man machtlos. Angreifer konnten etwa beim iPhone und beim Samsung Galaxy S3 über die Notruffunktion im Sperrbildschirm die Telefonsperre umgehen. Bei Mobilgeräten sind Sie zudem davon abhängig, welche Gerätesicherung und Nutzerauthentifizierung sie überhaupt bieten. Biometrische Verfahren sind leider immer noch kaum über den Prototypstatus hinaus.

Bei den meisten Mobilgeräten können Sie neben der PIN-Nummer der SIM-Karte lediglich einen Sperrcode anlegen - eine vierstellige PIN oder eine Swipe-Geste über ein Raster von neun Punkten. Die IT-Sicherheitsfirma Symantec fand bei einer Analyse gestohlener Smartphones heraus, dass 40 Prozent der Geräte mit dem Code [1234] gesichert waren. Auch wenn ein Telefondieb nur drei Versuche für die Eingabe hat, auf solche Codes kommt er vermutlich schnell. Ähnlich unsicher sind die Gesten, die man über die Fingerabdrücke auf dem Display nachvollziehen kann (Smudge-Attack).

Windows 8 Picture Password: Bildcode als Zugangskontrolle.

Windows 8: Anmeldung mittels Picture Password

Im Vergleich zu Apple und Google ist Microsoft schon einen Schritt weiter beim Schutz mobiler Geräte. In Windows 8 können Sie nämlich Bilderpasswörter nutzen. Dabei zeichnen Sie Gesten auf einem Bild, etwa einen Punkt, einen Kreis oder eine Linie zwischen zwei Bildelementen. Der Vorteil: Die Gesten sind ähnlich sicher wie komplexe Passwörter, lassen sich aber auf Touchgeräten komfortabler eingeben. Zudem funktionieren sie auch am PC, wo Sie die Gesten per Maus nachzeichnen.

Und so richten Sie ein Bilderpasswort ein: Öffnen Sie die CharmBar [Win]+[C] und gehen Sie auf »Einstellungen | PC-Einstellungen | Benutzer«. Dort kreieren Sie ein Windows-Kennwort und klicken danach auf »Bildcode erstellen«. Folgen Sie nun dem Einrichtungsassistenten. Unser Tipp: Verwenden Sie keine Punktgesten, sondern nur Linien und Kreise. Die sind sicherer, da sie sowohl Positions- als auch Richtungsdaten enthalten. Außerdem sollten Sie keine vorhersehbaren Gesten wählen, etwa ein Kreis um ein Gesicht. Vor allem am PC ist diese Methode ein hervorragender Ersatz für das Passwort, da hier nicht einmal Wischspuren auf einem Display zurückbleiben. Wer unsere Passwortstrategien befolgt, braucht die Parolen (im Gegensatz zur Zahnbürste) auch nicht regelmäßig zu wechseln. Es sei denn, Passwort, Stick oder Smartphone waren in falschen Händen. Dann sollten Sie bei allen Accounts das Kennwort ändern. Sicher ist sicher.

Passwort-Apokalypse: Die Sicherheitschlösser der Zukunft

07.05.2015

Einfache Passwörter sind als Schutz längst nicht mehr gut genug. Ob mit Log-in per Blick, 3D-Gesichtsanalyse oder Verhaltensmuster - das Einloggen wird in Zukunft wohl komplizierter. Welcher ist der passende Schlüssel zu mehr Sicherheit?

Fotostrecke: Die besten kostenlosen Sicherheits-Tools

Augenblick mal: Log-in per Blick.

Log-in per Blick: Flughäfen oder Polizeibehörden setzen schon seit Jahren Augenscanner ein. Die erkennen Menschen anhand der Kapillaren in der Netzhaut oder der Struktur der Iris. Unter optimalen Bedingungen ist diese Erkennung nahezu fehlerfrei. Doch Lichteinfall oder auch Verletzungen des Auges können die Identifikation stören. Zudem konnten Irisscanner schon durch Fotos des Auges überlistet werden. Und die meist mit Infrarottechnik arbeitenden Scanner taugen nicht für den Einsatz in Mobilgeräten - anders als die App EyeVerify. Die fotografiert Ihre Augen und erkennt Sie anhand der Adern im Augapfel, wofür laut Anbieter schon Kameras ab zwei Megapixel genügen. Von den vier Augenabdrücken - jeweils links und rechts der Iris in beiden Augen - muss nur einer übereinstimmen, damit die App das Telefon entsperrt. Auch mit einem blauen Auge können Sie also Ihr Handy freischalten und den Arzt rufen. Damit die Software ein Foto von einem echten Menschen unterscheiden kann, verändert sie zufallsgesteuert den Kamerafokus und prüft die Reaktion des Auges. EyeVerify soll im Sommer 2013 auf den Markt kommen.

Schau mich an: 3D-Gesichtsanalyse.

3D-Gesichtsanalyse: SeitAndroid 4.0 kann man Smartphones per Gesichtserkennung entsperren. Die Face-Unlock-Funktion arbeitet zuverlässig, allerdings nur bei guten Lichtverhältnissen. Bei Gegenlicht, etwa Sonnenschein, braucht es mitunter etliche Versuche. Ließ sich FaceUnlock anfangs noch per Foto überlisten, muss man heute blinzeln, um zu beweisen, dass man wahrhaft ein Mensch ist. PC-User können mit der Software Blink ebenfalls eine Gesichtserkennung nutzen. Die oft verwendete 2D-Erkennung authentifiziert Sie anhand von etwa 80 Merkmalen (Augenabstand, Breite der Nase), die sie per Berechnung eines Wertes oder Musterabgleich analysiert. Da eine 2D-Erkennung weder fehlerfrei noch fälschungsresistent ist, geht der Trend aber zum weniger lichtabhängigen 3D-Gesichtsscan. Eine mikrometergenaue Vermessung der Gesichtsoberfläche, die sogar aus Fotos errechnet werden kann, soll Menschen zuverlässiger identifizieren. Eine zusätzliche Oberflächentexturanalyse der Haut unterscheidet sogar eineiige Zwillinge. Militärs und Polizei nutzen das schon heute, etwa mit der Smartphone-App FaceR MobileID von Animetrics.

Schlüssel zu mehr Sicherheit?
Fingerabdruckscan und Verhaltensmuster.

Fingerabdruck-Scan: In Notebooks, Tastaturen oder externen USB-Scannern gibt es Fingerscanner schon seit Jahren. Gerüchten zufolge könnte auch das iPhone 5 einen im Home-Button haben. Ein interessantes Projekt ist myIDkey, ein per Fingerabdruck gesicherter USB-Stick, der Passwörter, Dokumente oder Bilder verschlüsselt speichert. Er verbindet sich per USB oder Bluetooth mit Geräten oder zeigt die Log-in-Daten auf einem Display an, erzeugt sichere Passwörter und löscht die Daten nach mehreren Fehlversuchen. Ab August soll er für etwa 100 US-Dollar auf den Markt kommen.

Auch die Interaktion mit Geräten erzeugt ein einzigartiges Muster. Die schwedische Firma BehavioSec hat dafür eine Erkennungssoftware entwickelt. Diese prüft eingegebene Passwörter oder Gesten nicht nur auf Korrektheit, sondern auch, wie sie eingegeben werden. Zu den analysierten Faktoren zählen die Tippgeschwindigkeit und der Tipprhythmus. Bei Touchscreens erkennt die Software den Druck und den Winkel der Gesten, an der Maus die Mausbeschleunigung und die Klickfrequenz. Diese Methode wäre ein einfacher Weg, eine weitere Sicherheitsstufe anzubieten.