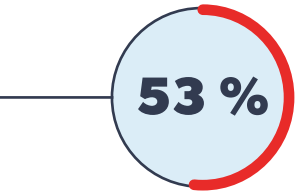
LastPass •••|
by LogMeIn

PSYCHOLOGIE DER PASSWÖRTER:

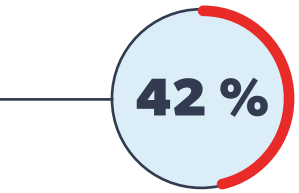
IHR ONLINE-VERHALTEN – SICHER ODER RISKANT?

KOGNITIVE DISSONANZ BEIM PASSWORT-VERHALTEN – WIRD 2020 DIE WENDE BRINGEN?

Dieses E-Book basiert auf einer weltweit durchgeführten Umfrage über das Online-Verhalten von 3.250 Personen. Ein Ergebnis: Alle wissen, dass man sich online vor Sicherheitsrisiken schützen soll, doch sie handeln nicht danach. Allgemein ist man sich der Gefahr bewusst und es herrscht ein Unwohlgefühl.



… haben in den letzten 12 Monaten keine Passwörter geändert, nachdem sie von einem Datenleck gehört hatten.



… finden es wichtiger, dass ihr Passwort einfach zu merken ist als dass es sicher ist.

Wir sind im Arbeits- wie im Privatleben immer häufiger online. Der Schutz unserer digitalen Identität ist also wichtiger denn je. Hackerangriffe, etwa durch Einschleusen von Malware aus nicht überprüften Softwaredownloads oder durch Phishing, nehmen stetig zu.

Kommen wir langsam an den Punkt, an dem wir uns mehr Gedanken um die Sicherheit unseres Online-Verhaltens machen?

Sicher oder riskant? Unsere Umfrage zeigt, was Nutzer digitaler Systeme und Angebote über Online-Sicherheit wissen und wie sie sich verhalten. Damit Sie nicht dieselben Fehler machen, sollten Sie jetzt weiterlesen.

ALLE WISSEN, WIE ES SEIN SOLL, TUN ABER DAS GEGENTEIL

Die meisten Menschen meinen, alles über das Risiko schlechter Passwortsicherheit zu wissen. Allerdings nutzen sie ihr Wissen nicht, um sich selbst vor Bedrohungen zu schützen.

Das sagen Nutzer digitaler Systeme

91 %

„Immer dasselbe Passwort oder eine Variation davon zu verwenden, ist riskant."

80 %

„Ich habe schon Bedenken, dass meine Passwörter herausgefunden werden könnten."

77 %

„Ich weiß, welche Maßnahmen in puncto Passwortschutz vernünftig sind."

Und das tun sie

66 %

... verwenden immer oder meistens dasselbe Passwort oder eine Variation davon – 8 % mehr als in unserer Umfrage aus dem Jahr 2018.

48 %

... ändern ihr Passwort nie, wenn sie nicht dazu gezwungen werden – 2018 waren das noch 40 %.

54 %

... schreiben sich ihre Passwörter irgendwo auf oder versuchen sie sich zu merken.

UNTERSCHÄTZEN SIE NICHT IHR RISIKO

Die Kluft zwischen Sagen und Tun aus unserer Umfrage mag beunruhigen, doch eines wird deutlich: Passwortsicherheit ist ein Thema und die meisten halten sich für gut informiert. Warum also wird das Wissen nicht genutzt, um sich selbst zu schützen?

Zum Teil deshalb, weil das eigene Risiko unterschätzt wird.

Viele machen sich nicht bewusst, wie stark sich ihr Leben online abspielt. Die Frage, wie viele Online-Konten sie haben, beantworten **71 % mit „1 bis 20"**. Anonymisierte LastPass-Benutzerdaten sagen da etwas anderes: **Ein LastPass-Benutzer hat durchschnittlich 38 Online-Konten** – also fast doppelt so viele, wie ein Großteil der Umfrageteilnehmer zu haben glaubt.

Was bedeutet das?

Jedes Online-Konto ist ein potenzielles Einfallstor für Hacker, und die wenigsten wissen, wie viele dieser Tore ihr eigenes digitales Dasein aufweist. Die Zahl an Online-Konten pro Nutzer dürfte künftig eher weiter zunehmen, schließlich wird unser Alltag immer digitaler.

So viele Online-Konten glauben die Befragten zu haben

1-20

So viele Online-Konten haben sie im Schnitt tatsächlich

~ 38

Jeder ist ein potenzielles Angriffsziel

Unterschätzt wird auch der Wert der eigenen Daten.

42 % der Befragten sind der Meinung, dass ihre Konten nicht wertvoll genug sind, um gehackt zu werden.

„Meine Konten sind nicht wertvoll genug, um gehackt zu werden."

42 %

Klotzen, nicht kleckern: Am liebsten stehlen Hacker gleich ganze Kundendatenbanken.

Eine einzige Kreditkartennummer bringt vielleicht nur **5 Euro im Dark Web**[1], aber wenn man hunderttausende Daten auf einmal erbeutet hat, läppert es sich. Noch besser: Mit den gestohlenen Daten von einer Website verschaffen sich Hacker Zugriff auf kritischere Systeme wie Ihr Online-Banking. **Vorsicht ist also geboten.**

IHR KONTROLLBEDÜRFNIS IST EINE GEFAHRENQUELLE

Unserer Umfrage zufolge ist die Passwortwiederverwendung der am häufigsten begangene Fehler. Auf die Frage, wie oft sie ein Passwort oder Varianten davon wiederverwenden, antworten **66 % „immer oder meistens"** – das sind **8 % mehr als in unserer 2018 durchgeführten Umfrage.**

Hat sich seit 2018 nichts geändert?

Der Hang zur kognitiven Dissonanz scheint ungebrochen. Die Befragten wissen genau, was sie tun müssten, tun es aber nicht.

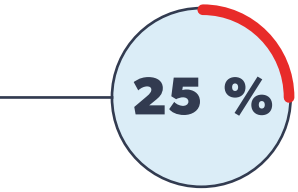
Warum?

Für die Gefahr, die von schwachen Passwörtern ausgeht, scheinen die Menschen keinen Sinn zu haben. Biometrische Verfahren nehmen einem die lästige Passworteingabe ab, und wenn man sich mal versehentlich ausgesperrt hat, klickt man eben einfach auf „Passwort vergessen".

Gefragt nach dem Grund für die Wiederverwendung von Passwörtern geben die Umfrageteilnehmer fast identische Antworten wie im Jahr 2018:

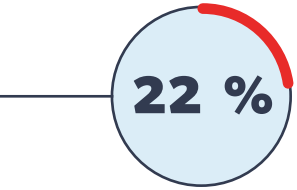
Das hier offenbarte Kontrollbedürfnis ist verständlich, jedoch fehlgelenkt. Für alles dasselbe Passwort zu verwenden, mag Ihnen ein Gefühl der Sicherheit geben. Leider ist dies jedoch nicht sicher, sondern viel gefährlicher, als wenn jedes Konto sein eigenes Passwort hat.

Sich alle seine Passwörter merken, ist auch nicht so einfach.



… setzen ihre Passwörter mindestens einmal pro Monat zurück, weil sie sie vergessen haben

Und genau darum wählt man eben ein schwaches und naheliegendes Passwort – um es sich merken zu können.



… sagen, dass sie das Passwort ihres Lebenspartners erraten könnten

Warum ist Passwort-wiederverwendung so riskant?

Weil ein Angreifer, sobald er ein wiederverwendetes Passwort gehackt hat, einfachen Zugang zu allen Konten erhält, für die es verwendet wird. Und wenn das wiederverwendete Passwort nicht nur privat, sondern auch beruflich eingesetzt wird, dann bringen gerät dadurch auch noch das Unternehmen in Gefahr, für das derjenige arbeitet.

WAS KÖNNEN SIE NOCH TUN, UM IHRE KONTEN ZU SCHÜTZEN?

Starke und nicht wiederverwendete Passwörter zu verwenden, ist der erste und sehr wichtige Schritt. Doch es gibt noch weitere Schutzmaßnahmen.

Als zusätzliche Sicherheitsebene lässt sich eine Multifaktor-Authentifizierung (MFA) einführen. Die gute Nachricht: MFA ist sehr bekannt und verbreitet. **Nur 19 % der Befragten** sagen, **sie wissen nicht, was MFA ist**. 54 % der Befragten geben **an,** MFA für ihre **persönlichen Konten** zu nutzen, und **37 % verwenden MFA bei der Arbeit**.

Gut vertraut sind die Befragten auch mit biometrischer Authentifizierung – der Anmeldung bei Geräten oder Konten per Fingerabdruck oder Gesichtserkennung. **65 % sagen, sie vertrauen biometrischen Faktoren wie Fingerabdrucks- oder Gesichtserkennung mehr** als herkömmlichen Passwörtern. Die Vertrautheit mit Biometrie lässt sich wahrscheinlich mit dem häufigen Einsatz auf Mobilgeräten erklären.

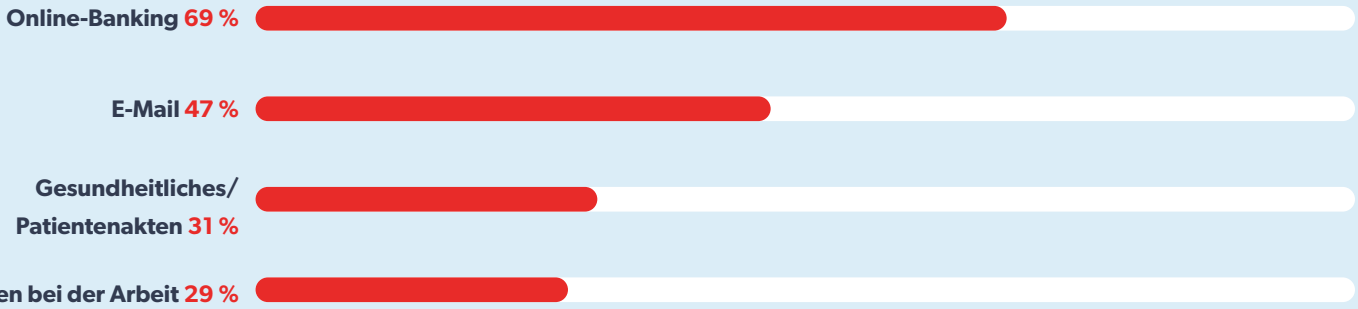
Was ist Multifaktor-Authentifizierung (MFA)?

Bei der MFA müssen Sie mehr als nur Ihre Zugangsdaten wissen, um sich bei einem Konto anzumelden. Von Benutzername und Passwort abgesehen verlangt MFA eine weitere Information – etwa einen Einmalcode oder Ihren Fingerabdruck.

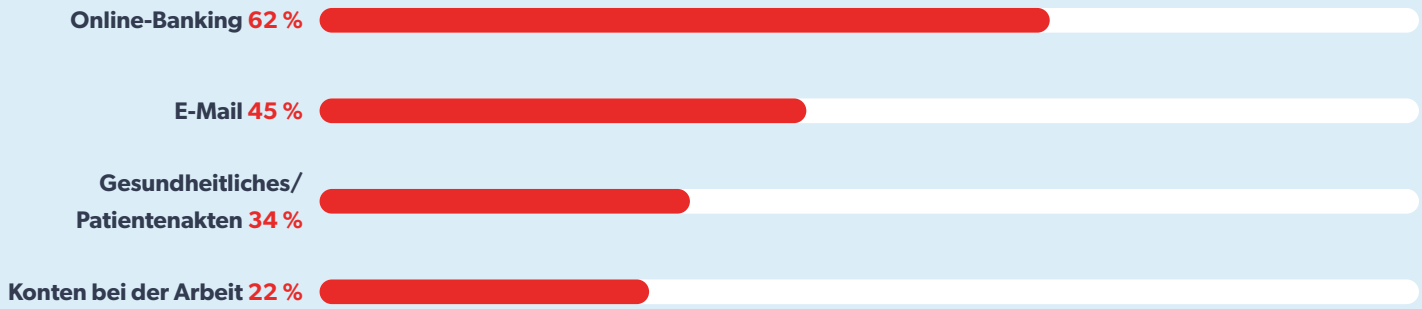
GROSSES SICHERHEITSBEWUSSTSEIN BEI E-MAIL UND BANKING

E-Mail und Online-Banking werden als besonders schützenswerte Konten angesehen, was äußerst klug ist. E-Mail ist Dreh- und Angelpunkt Ihres Online-Daseins und enthält oft Informationen, die Angreifer für den Identitätsdiebstahl und Zugriff auf weitere Konten verwenden können. Die Schutzbedürftigkeit von Online-Banking muss man nicht erklären: Es gibt Zugriff auf Ihr Geld, auf Kreditkarteninformationen und weitere sensible Daten.

Für welches Konto würden Sie ein stärkeres Passwort erstellen?



Für welche Konten haben Sie Multifaktor-Authentifizierung aktiviert?



Das Bewusstsein zum Schutz von E-Mail und Banking ist hoch – was beruhigend ist. Noch besser wäre es allerdings, diesen Schutz auf alle Konten auszuweiten.

Unternehmen aufgepasst!

Arbeitskonten werden tendenziell schlechter geschützt als private Konten. Außerdem: Wer im Privaten Sicherheitsfehler begeht, wird dies höchstwahrscheinlich auch in Ihrem Unternehmen tun.

REGIONALE UNTERSCHIEDE

Die bis hierher erwähnten Ergebnisse stammen aus der Auswertung der gesamten, global erhobenen Daten. Gibt es länderspezifische Unterschiede im Verhalten?

Deutschland: hohes Risikobewusstsein
Die **DSGVO** hat das Risiko eines mangelhaften Datenschutzes klar gemacht, doch die richtigen Verhaltensweisen fördert sie nicht.

94 % wissen, dass es riskant ist, dasselbe oder ein ähnliches Passwort mehrfach zu verwenden. Trotzdem verwenden 30 % ein bis zwei Passwörter in Varianten und weitere 30 % haben keinerlei Bedenken, dass ihre Passwörter gehackt werden könnten.

Brasilien: Hoffnungsträger
Mit dem (noch nicht verabschiedeten) Datenschutzgesetz **LGPD** wird sich das Online-Sicherheitsbewusstsein bessern.

94 % der Brasilianer haben Bedenken, dass ihre Passwörter gehackt werden, und 64,8 % halten ihre Konten aus Hackersicht für wertvoll.

78 % vertrauen biometrischen Methoden mehr als Passwörtern. Für sie könnte MFA eine gute Investition in noch mehr Online-Sicherheit sein.

Singapur: Vorreiter
Singapur ist ein Hotspot der **digitalen Wirtschaft**. So überrascht es nicht, dass 88 % seiner Einwohner wissen, wie riskant es ist, nur ein Passwort oder Varianten davon zu nutzen. Vielleicht der Grund für folgende Ergebnisse:

40 % nutzen bei beruflichen Konten stärkere und komplexere Passwörter.

MFA wird bei den Befragten zu 58 % bei dienstlichen zu 70 % bei privaten Konten genutzt.

Großbritannien: die meisten Konten
Das nationale Cybersicherheitszentrum **NCSC** bemüht sich um Aufklärung zur Online-Sicherheit, allerdings mit mäßigem Erfolg: 58 % ändern nach Bekanntwerden eines Datenlecks ihr Passwort nicht!

92 % wissen, dass es riskant ist, dasselbe oder ein ähnliches Passworts mehrfach zu nutzen, tun es aber trotzdem.

64 % wählen einfache Passwörter, weil sie sie im Kopf haben wollen.

Australien: wenig Trennung von Arbeit und Privat
Die Berichte zu Datenschutzverletzungen nach der **„Notifiable Data Breaches"-Regelung** zeigen anscheinend positive Wirkung: 80 % halten sich zu Passwort-Best-Practices für gut informiert. Aber:

Nur 18 % erstellen für ihre Arbeitskonten ein komplexes, einmaliges Passwort und 36 % trennen nicht zwischen Arbeits- und Privatkonten.

Zwar kennen 90 % das Risiko, meist oder immer dasselbe Passwort oder Varianten davon zu nutzen, doch tun 69 % genau dies.

USA: mangelhafte Passworthygiene, MFA beliebt

60 % haben Angst davor, ihre Zugangsdaten zu vergessen; entsprechend notieren 33 % sich ihre Passwörter.

67 % vertrauen biometrischen Methoden mehr als herkömmlichen Passwörtern.

42 % nutzen MFA für Konten bei der Arbeit und 58 % für private Konten – höhere Werte hat nur Singapur.

SCHLUSS MIT UNNÖTIGEN RISIKEN

Wir alle möchten sicher und wohlbehalten durchs Leben gehen und meiden Risiken deshalb, wo immer möglich. Vielleicht haben Sie sich noch keine Gedanken dazu gemacht, dass „Leben" auch Ihr digitales Leben meint – und die Risikovermeidung dort gar nicht einmal so schwer ist.

Machen Sie 2020 zum Wendepunkt in Ihrem Sicherheitsverhalten

Legen Sie sich einen Passwort-Manager zur Verwahrung und Verwaltung Ihrer Passwörter zu. Vielleicht ist es eine Herausforderung für Ihr Kontrollbedürfnis. Doch es ist nun einmal sicherer, für alle Konten starke, einmalige Passwörter zu haben und in einem verschlüsselten Tresor zu speichern. Sie müssen sich Ihre Passwörter nicht mehr merken und haben sie sofort parat, wenn Sie sie brauchen.

Verwenden Sie Multifaktor-Authentifizierung. Beginnen Sie mit Ihren wichtigsten und meistgenutzten Konten: E-Mail, Online-Banking, Kreditkarten, Steuern, Social Media. Prüfen Sie dann bei jeder Erstellung eines weiteren Kontos, ob es MFA anbietet, und aktivieren Sie diese dann.

Überwachen Sie Ihre Daten. Ob Sie Kreditkarten- oder Girokontoumsätze überwachen oder einen Dark-Web-Überwachungsdienst nutzen, sorgen Sie dafür, dass Sie von Datenlecks erfahren, die Sie direkt betreffen.

Mehr als 17 Millionen Benutzer und 61.000 Unternehmen weltweit vertrauen auf LastPass beim Speichern und der Verwaltung von Passwörtern, Kreditkartendaten und anderen persönlichen Informationen. Nutzen Sie LastPass, um starke Passwörter zu erstellen und diese automatisch auszufüllen, wenn Sie sich auf Websites oder bei Apps anmelden – auf allen Geräten.

Quellen:
1 https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

04.14.2020/LMI1249/PDF