LastPass •••|

Psychologie der Passwörter

Wie (Fehl-)Verhalten von Mitarbeitern das Risiko für Ihr Unternehmen erhöht und was Sie dagegen tun können.

Mehr Sicherheit und bessere Compliance – ohne mehr Komplexität

Privates und Berufliches verschmelzen immer stärker miteinander. Deshalb sind gute Passwortgewohnheiten wichtig für die Sicherheit und den Erfolg von Unternehmen. IT-Teams müssen jetzt in einer komplexer und flexibler gewordenen Arbeitswelt für die Sicherheit von Mitarbeiterzugangsdaten sorgen.

Unser Bericht zur Psychologie der Passwörter basiert auf einer Befragung von 3.750 Unternehmensmitarbeitern weltweit. Sie erfahren darin mehr zu folgenden Themen:

- **Wie Sie für mehr Sicherheitsbewusstsein** und ein besseres Passwortverhalten sorgen
- **Mit welchen Best Practices** Sie die Wiederverwendung von Passwörtern verhindern und Passwörter sicher speichern
- **Wie Sie Ihr Ziel** „Mehr Sicherheitsbewusstsein“ in einer Remote-Arbeitswelt erreichen

LastPass Business unterstützt Ihre Mitarbeiter, indem es administrativen Aufwand für Anwender und IT-Teams reduziert und gleichzeitig die Sicherheit messbar erhöht. **Sparen Sie Zeit mit einer einfachen, zentralen Passwortverwaltung. Geben Sie Ihren Administratoren mehr Kontrolle** durch erweiterte Berichterstattung und über 100 konfigurierbare Sicherheitsrichtlinien.

Weitere Informationen finden Sie unter
LastPass.com/business

Passwortsicherheit 2021: Hacker nutzen menschliche Schwächen

Die Corona-Pandemie hat die Arbeitswelt von Millionen Menschen weltweit auf den Kopf gestellt. Büros wurden geschlossen, viele Mitarbeiter wechselten ins Homeoffice. In den Lockdown-Phasen verbrachten alle mehr Zeit im Internet.

Menschen und Unternehmen sind gefährdeter denn je

Hackern kommt die aktuelle Entwicklung sehr gelegen: Mehr Remote-Arbeit, längere Internetnutzung. Entsprechend haben sie ihre Angriffsstrategien angepasst, um sich menschliche Schwächen zunutze zu machen.

Der Data Breach Investigations Report 2021 zeigt: Cyberkriminelle greifen immer häufiger Geräte einzelner Benutzer an.

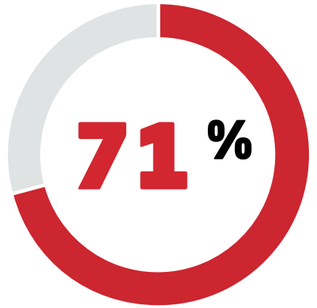
85 %

Erschreckende 85 % der Datenschutzverletzungen basieren auf gedankenlosem und fehlerhaftem Handeln, das Phishing und den Diebstahl von Zugangsdaten begünstigt.

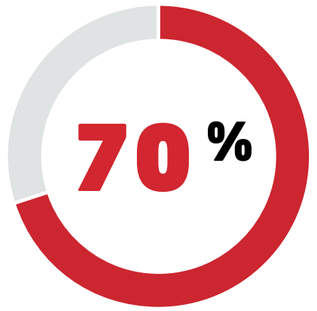
36 %

36 % der Datenschutzverletzungen im vergangenen Jahr resultierten aus Phishing-Angriffen – das sind 11 % mehr als zuvor.

Während der Pandemie:



haben ganz oder teilweise im Homeoffice gearbeitet.



haben bei der Arbeit und privat mehr Zeit online verbracht.

Unsere Umfrage – Zahlen und Fakten

Für den Bericht „Psychologie der Passwörter“ haben wir 3.750 Arbeitnehmer in sieben Ländern zu ihrem Passwortverhalten befragt. Es ging um ihre Einschätzungen und Verhaltensweisen rund um das Thema Online-Sicherheit.

Die Befragten stammten aus folgenden Ländern:

- USA
- Vereinigtes Königreich
- Deutschland
- Frankreich
- Australien
- Singapur
- Indien

Viel Wissen, zu wenig Umsetzung

Aussagen Befragter:

79 %
wissen um die Gefahr des Diebstahls von Passwörtern ...

92 %
wissen, dass die Wiederverwendung von Passwörtern riskant ist ...

Handlungen Befragter:

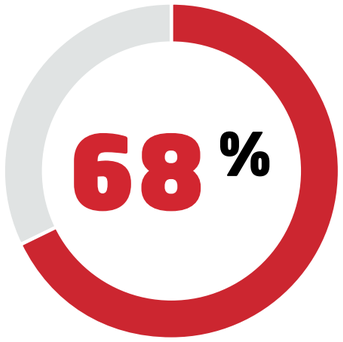
51 %
... verlassen sich bei Passwörtern auf ihr eigenes Gedächtnis.

65 %
... verwenden (fast) immer dasselbe Passwort oder Varianten davon.

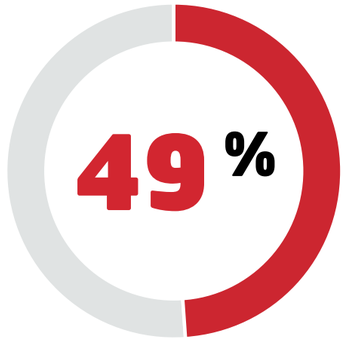
45 % TAUSCHEN PASSWÖRTER NICHT AUS

45 % der Befragten haben im letzten Jahr nach dem Bekanntwerden eines Datenlecks ihr Passwort nicht geändert.

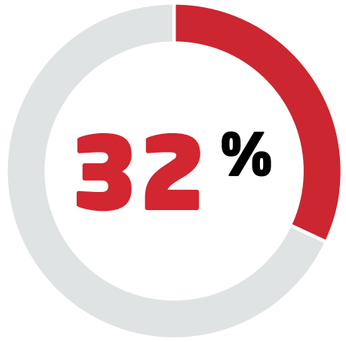
Selektive Passwortsicherheit: Benutzer würden stärkere Passwörter erstellen für …



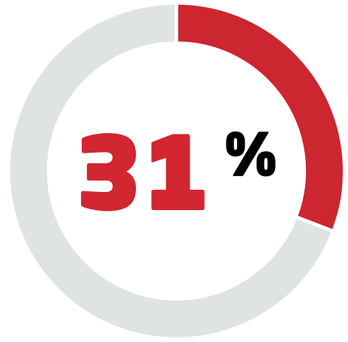
Online-Banking



E-Mail-Konten



Dienstliche Konten



Gesundheitliches/ Patientenakten

8 %

Nur 8 % ist bewusst, dass ein starkes Passwort nicht auf persönliche Informationen hinweisen sollte.

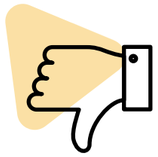
Die meisten Benutzer erstellen also Passwörter, die persönliche Informationen wie den eigenen Geburtstag oder Wohnort enthalten.

PROFITIPP

Statt einen echten Begriff als Passwort zu verwenden, sollten Ihre Mitarbeiter die Anfangsbuchstaben der Worte in einem sinnfreien, aber merkwürdigen Satz als Kennwort nutzen. Darin verteilte Ziffern machen es sogar noch sicherer. So ist das Passwort schwerer zu stehlen.

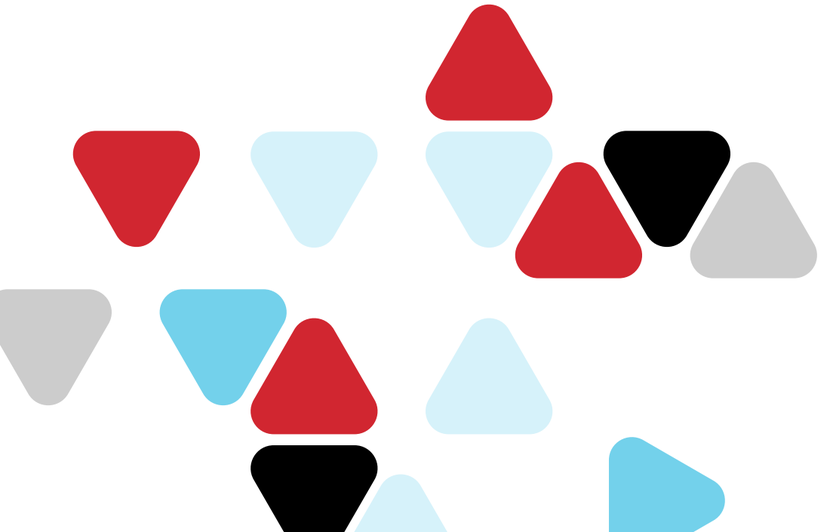
Licht und Schatten

Auffällig ist eine gewisse kognitive Dissonanz. Welche Daten schutzbedürftig sind, entscheiden viele Benutzer aus dem Bauch heraus. Das Resultat sind riskante Passwortgewohnheiten. Das ist gerade heutzutage ein Problem, weil beruflich und privat so viel Zeit online verbracht wird.



83 % wissen nicht, ob Zugangsdaten von ihnen im Darkweb zirkulieren.

76 % nutzen MFA bei der Arbeit und privat – 10 % mehr als im Vorjahr.



PROFITIPP

Betrachten Sie alle Zugangsdaten als schutzbedürftig. Das Konto eines Mitarbeiters bei einem Fitness-Studio mag für Hacker uninteressant sein. Wenn aber das Passwort dafür identisch mit einem ist, das er bei der Arbeit verwendet, geraten Ihre Unternehmensdaten dadurch schnell in Gefahr.

Wachsende Digitalität

Mehr Online-Konten denn je:

91 % der Befragten haben in 2021 mindestens ein neues Konto angelegt.

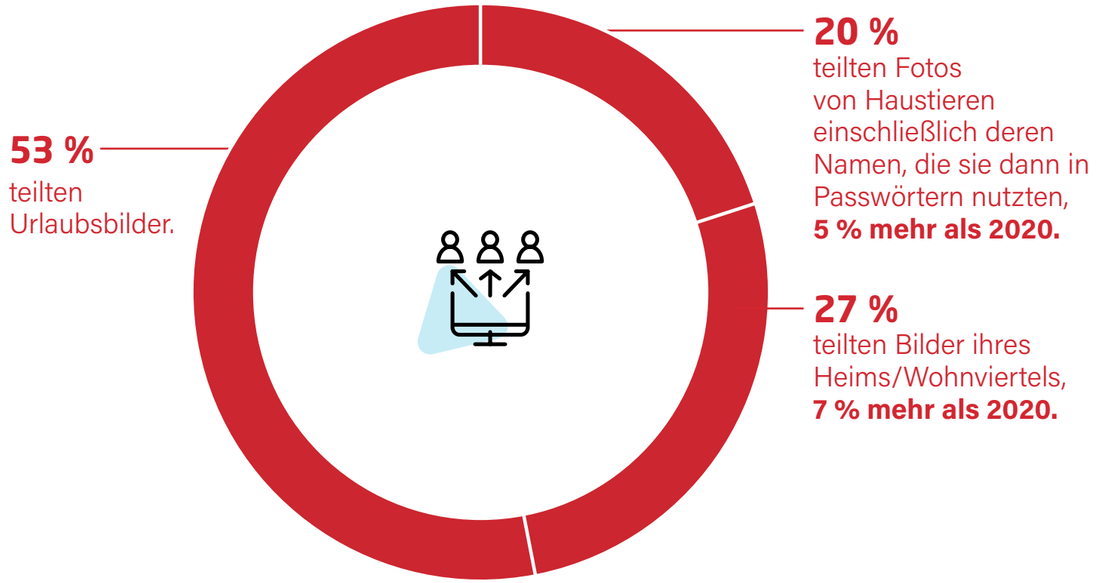
90 % der Befragten haben bis zu 50 Online-/App-Konten.

50 % Die Befragten besitzen im Jahr 2021 50 % mehr Konten als 2020.

Je digitaler das Leben wird, desto wichtiger wird der Schutz von Mitarbeitern und Unternehmen

Währen der Pandemie ist unser aller Leben rasant digitaler geworden. Durch die starke soziale Isolation im Alltag wuchs der Wunsch, wenigstens online in Verbindung zu sein. Das Ergebnis: immer mehr Online-Konten, immer mehr digitaler Austausch persönlicher Daten.

Immer mehr Persönliches online:



PROFITIPP

Kriminelle suchen in öffentlichen Social-Media-Profilen nach vermeintlich harmlosen Informationen, die ihnen Rückschlüsse auf anderweitig genutzte Passwörter erlauben – ein weiterer Grund, Ihre Mitarbeiter dringend vor der Verwendung persönlicher Informationen für die Passwortvergabe zu warnen.

Remote-Arbeit: die Perspektive von Angestellten und Arbeitgebern

Mitarbeiter im Homeoffice-Modus:

47% haben ihr Online-Sicherheitsverhalten nach dem Wechsel ins Homeoffice nicht verändert.

46% haben sich im Homeoffice keine stärkeren Passwörter zugelegt.

44% haben im Homeoffice sensible Daten und Passwörter für beruflich genutzte Konten geteilt.

Unternehmen im Homeoffice-Modus:

39% haben dafür gesorgt, dass sich Mitarbeiter im Homeoffice auf sicheren Wegen im Unternehmensnetzwerk anmelden.

35% haben dafür gesorgt, dass Mitarbeiter ihre Passwörter häufiger austauschen.

35% haben Authentifizierungsmethoden verbessert.

IT-Administratoren müssen wachsam sein. Ein Vorhandensein von Risiken bringt Menschen nicht automatisch dazu, sich sicherer zu verhalten. Fast die Hälfte der Mitarbeiter zeigt bei der Arbeit im Homeoffice bedenkliche Passwortgewohnheiten.

IT-Administratoren müssen ihre Sicherheitsstrategien so grundlegend überdenken, wie Benutzer ihre Arbeitsweisen verändern.

PROFITIPP

Investieren Sie in einen **Passwortmanager**, um die Passwortgewohnheiten und die IT-Sicherheit zu verbessern. Führen Sie **SSO** und **MFA** ein, um alle Zugriffspunkte abzusichern. Informieren und überzeugen Sie Benutzer mithilfe von Sicherheitsschulungen.

Regionale Unterschiede

Vereinigtes Königreich

61 % wissen, dass ein starkes, einmaliges Passwort nicht auf Persönliches hinweisen sollte.

Der Anteil derer, die persönliche Informationen teilen, ist im internationalen Vergleich am geringsten **(41 %)**.

Deutschland

Am häufigsten sind Befragte zum Thema Darkweb in Deutschland informiert **(79 %)**.

Ob ihre Passwörter im Darkweb zirkulieren, wissen allerdings nur **14 %**.

Frankreich

Nur **15 %** der französischen Befragten arbeiteten während der Pandemie im Homeoffice.

Nur **43 %** änderten ihr Online-Sicherheitsverhalten nach dem Umzug ins Homeoffice.

Singapur

In Singapur ist das Problembewusstsein in puncto Passwortdiebstahl am höchsten **(93 %)**.

Die dortigen Befragten wissen auch am ehesten, was sie im Fall eines Passwortdiebstahls tun müssen **(74 %)**.

Indien

Der Anteil derer, die Passwörter in einem Passwort-manager oder im Browser speichern, ist deutlich höher als in anderen Ländern **(64 %)**.

Was die Änderung des eigenen Sicherheitsverhaltens im Homeoffice angeht, sind die Befragten aus Indien Vorreiter **(81 %)**.

Australien

71 % der australischen Befragten nutzen (fast) immer dasselbe Passwort (in Varianten).

Hier wurde während der Pandemie jedoch im Vergleich weniger Zeit online verbracht **(61 %)**.

USA

Befragte in den USA nutzten im Fall kompromittierter Konten am ehesten Kontoüberwachungsdienste **(31 %)**.

Allerdings sahen **39 %** keinen Anlass, ihr Online-Sicherheitsverhalten im Homeoffice zu ändern, da sie dieses bereits für ausreichend hielten.

Die Gründe verstehen

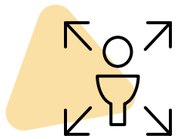
Warum zeigen Menschen riskante Passwort-gewohnheiten, obwohl sie es besser wissen?

68 % verwenden Passwörter mehrfach aus Sorge, ihre Zugangsdaten zu vergessen.

52 % verwenden Passwörter mehrfach, weil sie möglichst alle Zugangsdaten im Kopf haben wollen.

36 % meinen, dass Hacker an ihren Konten kein Interesse haben.

Warum ist Passwortwiederverwendung angesichts der zunehmenden Digitalisierung so gefährlich?



Eine einzige gestohlene Benutzernamen-Passwort-Kombination kann Hackern die Tür zu vielen Konten öffnen.

Hacker, denen es gelingt, ein privat und beruflich genutztes Endgerät zu kapern, können darüber schnell in Unternehmensnetzwerke eindringen.

DER NÄHRBODEN SCHLECHTER GEWOHNHEITEN

Die zunehmende Digitalisierung unseres Alltags, die mangelnde Unterstützung in puncto Cybersicherheit, das Festhalten an Gewohnheiten und das Gefühl, es sei nicht so dringend: Diese Mischung hält Menschen davon ab, ihr Verhalten zu ändern.

Schlechte Passwort-gewohnheiten bekämpfen

Die Corona-Pandemie hat unser aller Privat- und Arbeitsleben in unvorhersehbarer Weise verändert. Wir sind häufiger und länger online. Wir tauschen uns verstärkt auf digitalen Wegen aus. Wer ein unliebsames Verhalten ändern möchte, muss verstehen, warum Menschen es an den Tag legen.

Wie sieht ein gutes Passwortverhalten aus?

- Jedes Konto hat ein eigenes Passwort.
- Jedes Passwort besteht aus einer sinnfreien Zeichen- und Ziffernfolge.
- Einsatz von Multifaktor-Authentifizierung.
- Austausch von Passwörtern nach einer bekannt gewordenen Datenschutzverletzung.

Schluss mit der Angst vor Kontrollverlust

Nutzen Sie einen **Passwortmanager**, um Passwörter zu verwalten und zu speichern. Die Software kann komplexe Passwörter erstellen, memorieren und eingeben.

Schluss mit der Angst vor Datendiebstahl

Stellen Sie über **Multifaktor-Authentifizierung (MFA)** sicher, dass nur Befugte an die Daten und Anwendungen Ihres Unternehmens gelangen.

Schluss mit der Apathie

Überwachen Sie Ihre Daten und lassen Sie sich von einem **Darkweb-Überwachungsdienst** zu Datenlecks informieren, die Ihr Unternehmen und Ihre Mitarbeiter direkt betreffen.

LastPass •••|

LastPass Business bietet Mitarbeitern ein reibungsloses Nutzungserlebnis und erhöht die Kontrolle und Transparenz für die IT-Abteilung – mit einer Passwortmanagementlösung, die einfach zu verwalten und zu bedienen ist.

Mit LastPass Business können Mitarbeiter Zugangsdaten nahtlos generieren, absichern und freigeben. Das Zero-Knowledge-Prinzip sorgt dabei für optimalen Schutz.

Mehr erfahren

Mehr als 30 Millionen Benutzer und 85.000 Unternehmen weltweit vertrauen auf LastPass.

Mehr erfahren

LastPass •••|

LastPass Business bietet Mitarbeitern ein reibungsloses Nutzungserlebnis und erhöht die Kontrolle und Transparenz für die IT-Abteilung – mit einer Passwortmanagementlösung, die einfach zu verwalten und zu bedienen ist.

Mit LastPass Business können Mitarbeiter Zugangsdaten nahtlos generieren, absichern und freigeben. Die Sicherheit nach dem Zero-Knowledge-Prinzip sorgt dabei für optimalen Schutz.