LastPass •••|

Psychologie der Passwörter

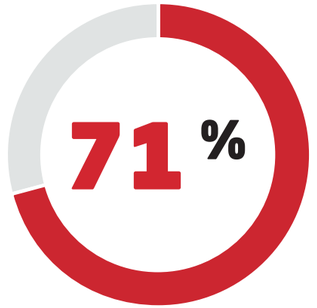
Passwortgewohnheiten in einer Welt wachsender Digitalität

Passwortsicherheit 2021: Hacker nutzen menschliche Schwächen

Die Corona-Pandemie hat die Arbeitswelt von Millionen Menschen weltweit auf den Kopf gestellt. Büros wurden geschlossen, ihre Nutzer 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: Sie machen sich menschliche Schwächen zunutze. Immer mehr Remote-Arbeit, immer länger im Internet: Entsprechend haben Hacker ihre Angriffsmaschen angepasst.

Während der Pandemie:



haben ganz oder teilweise im Homeoffice gearbeitet.

haben bei der Arbeit und privat mehr Zeit online verbracht.

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 %

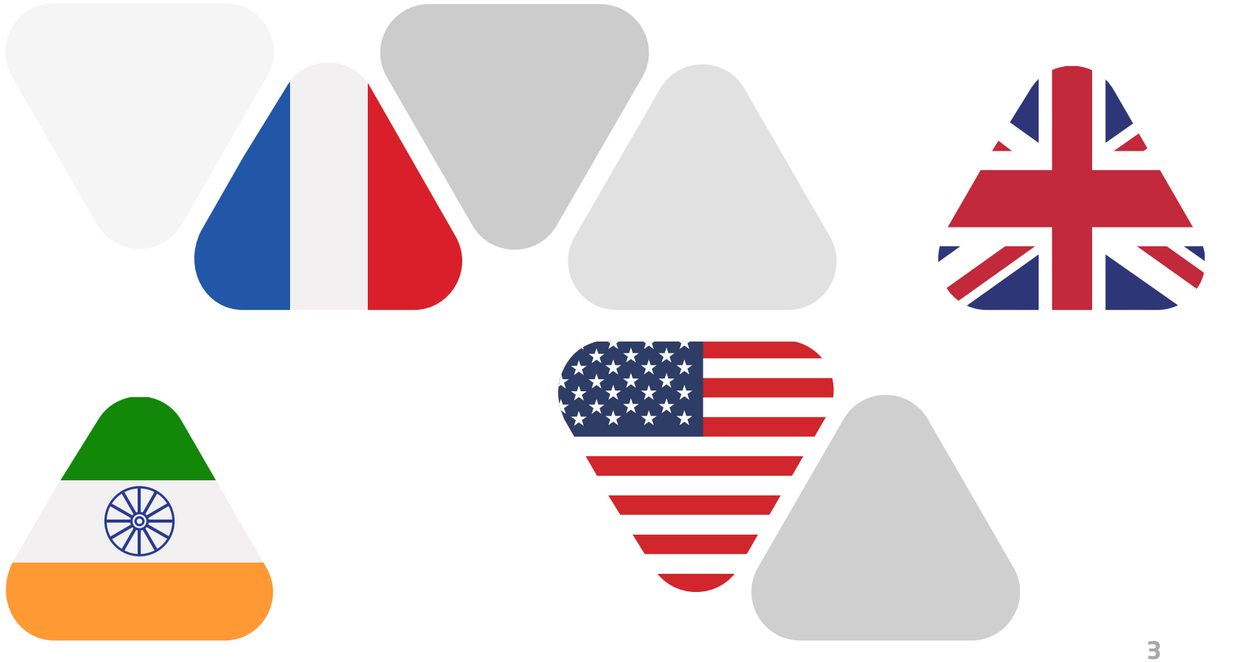
36 % der Datenschutzverletzungen im vergangenen Jahr involvierten Phishing – 11 % mehr als zuvor.

Unsere Umfrage – Zahlen und Fakten

Für den Bericht „Psychologie der Passwörter“ haben wir 3.750 Arbeitnehmer in sieben Ländern zu ihrem Passwort-verhalten 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:

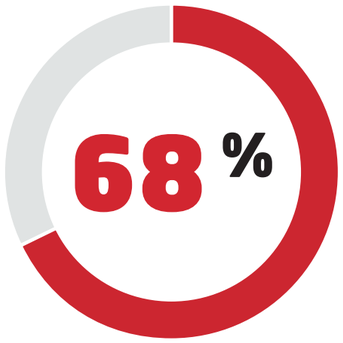
51 %
... verlassen sich bei Passwörtern auf ihr eigenes Gedächtnis.

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

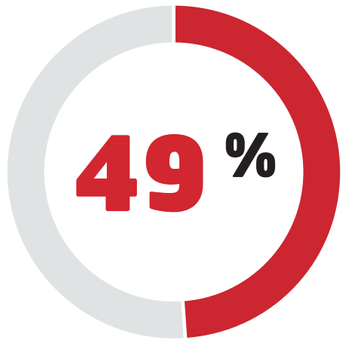
45 % TAUSCHEN PASSWÖRTER NICHT AUS

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

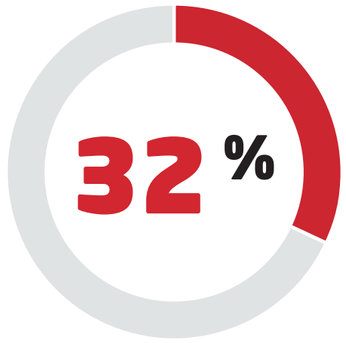
Selektive Passwortsicherheit: Benutzer würden stärkere Passwörter erstellen für …



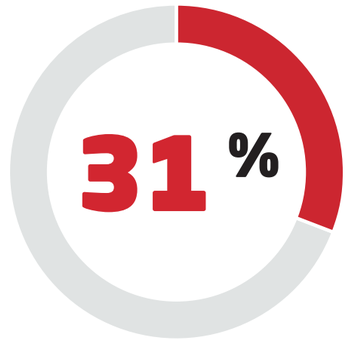
Online-Banking



E-Mail-Konten



Dienstliche Konten



Gesundheitliches/ Patientenakten

8 %

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

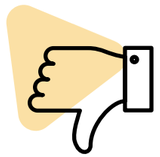
Die meisten Benutzer erstellen also Passwörter, die persönliche Informationen wie den eigenen Geburtstag oder Wohnort enthalten.

PROFITIPP

Um ein Passwort länger und stärker zu machen, nutzen Sie besser Anfangsbuchstaben von Nonsense-Phrasen mit darin verteilten Ziffern statt echter Begriffe. Dann ist das Passwort erstens einfacher memorierbar und zweitens 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 Passwortgewohnheiten, die riskant sind – zumal heutzutage, wo alle bei der Arbeit und privat so viel Zeit online verbringen.



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. Ihr Konto beim Fitness-Studio mag für Hacker uninteressant sein. Wenn aber das Passwort dafür identisch mit dem Ihres Online-Bankings ist, dann gerät Ihr Bankkonto schnell mit in Gefahr.

Wachsende Digitalität

Mehr Online-Konten denn je:

91 % der Befragten haben dieses Jahr mindestens ein neues Konto angelegt.

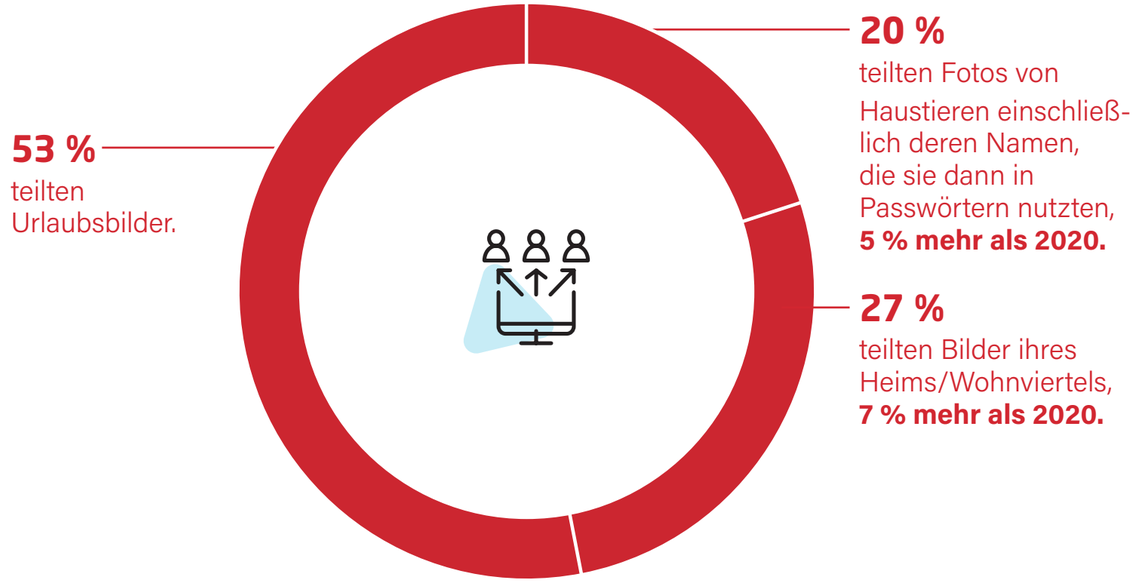
90 % der Befragten haben bis zu 50 Online-/App-Konten.

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

Je digitaler unser Leben wird, desto besser müssen wir persönliche Daten schützen.

Während der Pandemie hat sich die Digitalität unseres Lebens rasant entwickelt. Durch die starke soziale Isolation im Alltag wuchs unser Wunsch, wenigstens online in Verbindung zu sein. Das Ergebnis: Immer mehr Online-Konten, immer mehr Online-Austausch persönlicher Daten.

Immer mehr Persönliches online:



PROFITIPP

Halten Sie Social-Media-Posts möglichst privat; posten Sie so wenig wie möglich öffentlich. Kriminelle suchen öffentliche Profile nach verwertbaren, vermeintlich harmlosen Informationen ab, um in Konten außerhalb Ihres Social-Media-Umfeldes einzudringen.

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 bei der Arbeit 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.

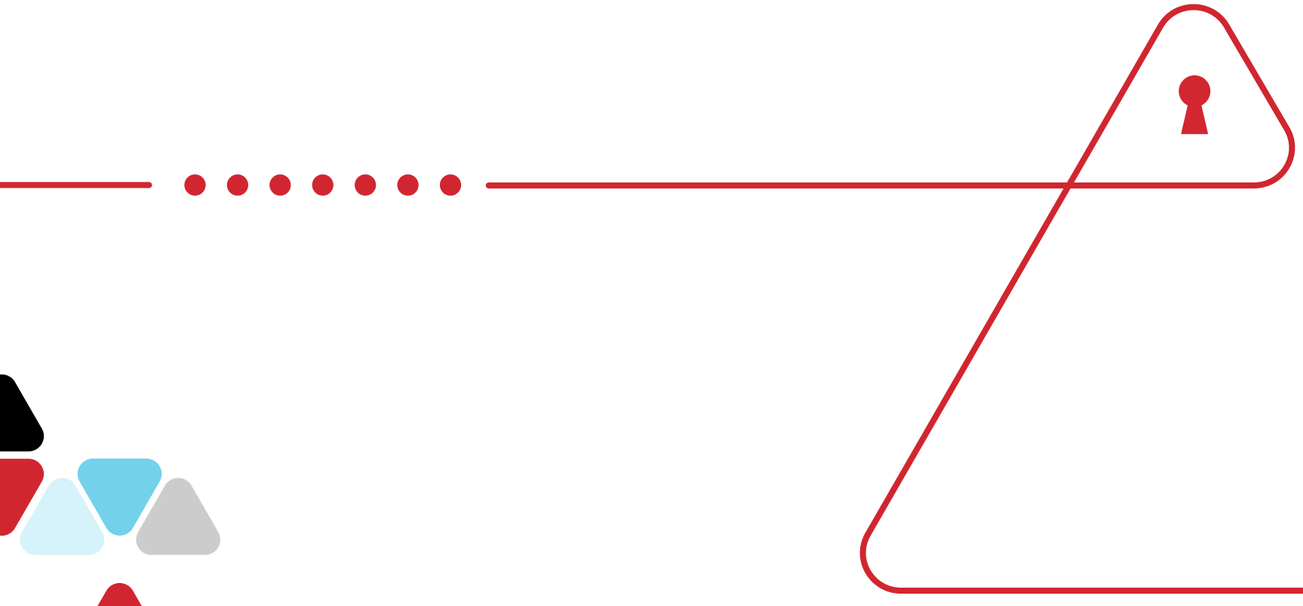
35 % haben Authentifizierungsmethoden verbessert.

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

IT-Administratoren müssen ihre Sicherheitsstrategien in dem Maße überdenken, in dem Benutzer ihre Arbeitsweisen verändern.

PROFITIPP

Investieren Sie in einen **Passwortmanager**, um die Passwortgewohnheiten und die Sicherheit zu verbessern. Führen Sie **SSO** und **MFA** ein, um alle Zugriffspunkte abzusichern. Informieren und überzeugen Sie Benutzer über 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 hier am niedrigsten **(41 %).**

Deutschland

Am häufigsten sind Befragte zum Thema Darkweb hier 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 hier 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

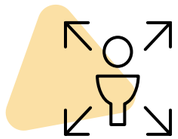
Warum zeigen Menschen (wider besseres Wissen) unsichere Passwortgewohnheiten?

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 bei der Arbeit genutztes Endgerät zu kapern, können darüber schnell in Unternehmensnetzwerke eindringen.

DER NÄHRBODEN SCHLECHTER GEWOHNHEITEN

Die zunehmende Digitalisierung unseres Alltags, eine mangelnde Unterstützung in puncto Cybersicherheit, dazu eine Mixtur aus Gewohnheiten, Emotionen und vermeintlich fehlender Dringlichkeit: diese Gemengelage 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?

- Sie haben für jedes Konto ein eigenes Passwort.
- Jedes Passwort besteht aus einer sinnfreien Zeichen- und Ziffernfolge.
- Sie verwenden die Zwei-Faktor-Authentifizierung.
- Sie tauschen nach einer bekannt gewordenen Datenschutzverletzung Ihre Passwörter aus.

Schluss mit der Angst vor Kontrollverlust!

Nutzen Sie einen **Passwortmanager**, um Ihre Passwörter zu verwalten und speichern. Diese Software kann für Sie auch Passwörter erstellen, memorieren und eingeben.

Schluss mit der Angst vor Datendiebstahl!

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

Schluss mit der Apathie!

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

LastPass •••|

Mehr als 30 Millionen Benutzer und 85.000 Unternehmen weltweit vertrauen auf LastPass beim Speichern und Eingeben von Passwörtern, Kreditkartendaten und anderen persönlichen Informationen. Nutzen Sie LastPass, um starke Passwörter zu erstellen und diese automatisch eingeben zu lassen, wenn Sie sich auf Websites oder bei Apps anmelden – auf allen Geräten.

Mehr erfahren