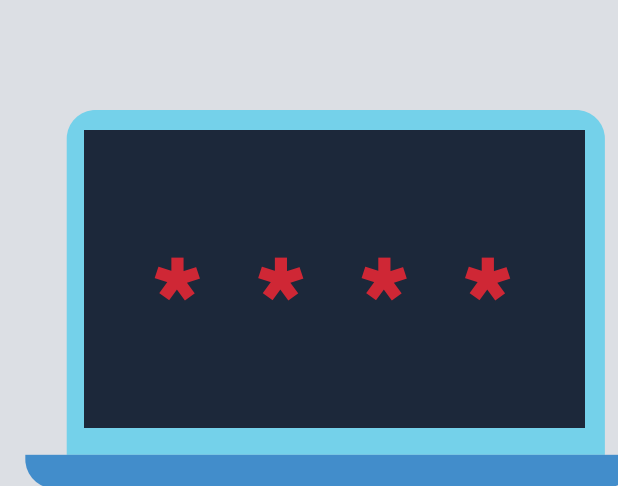
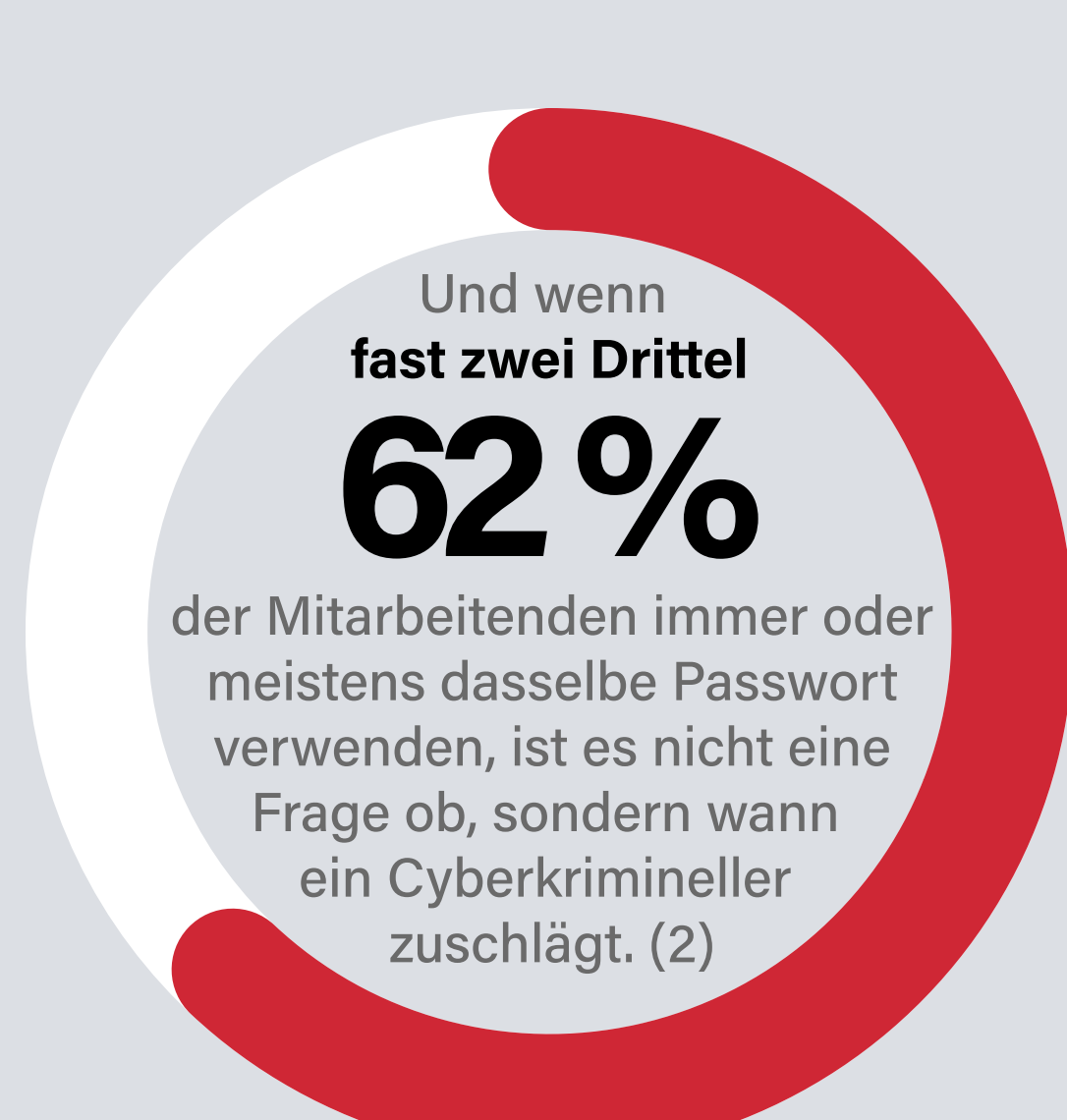
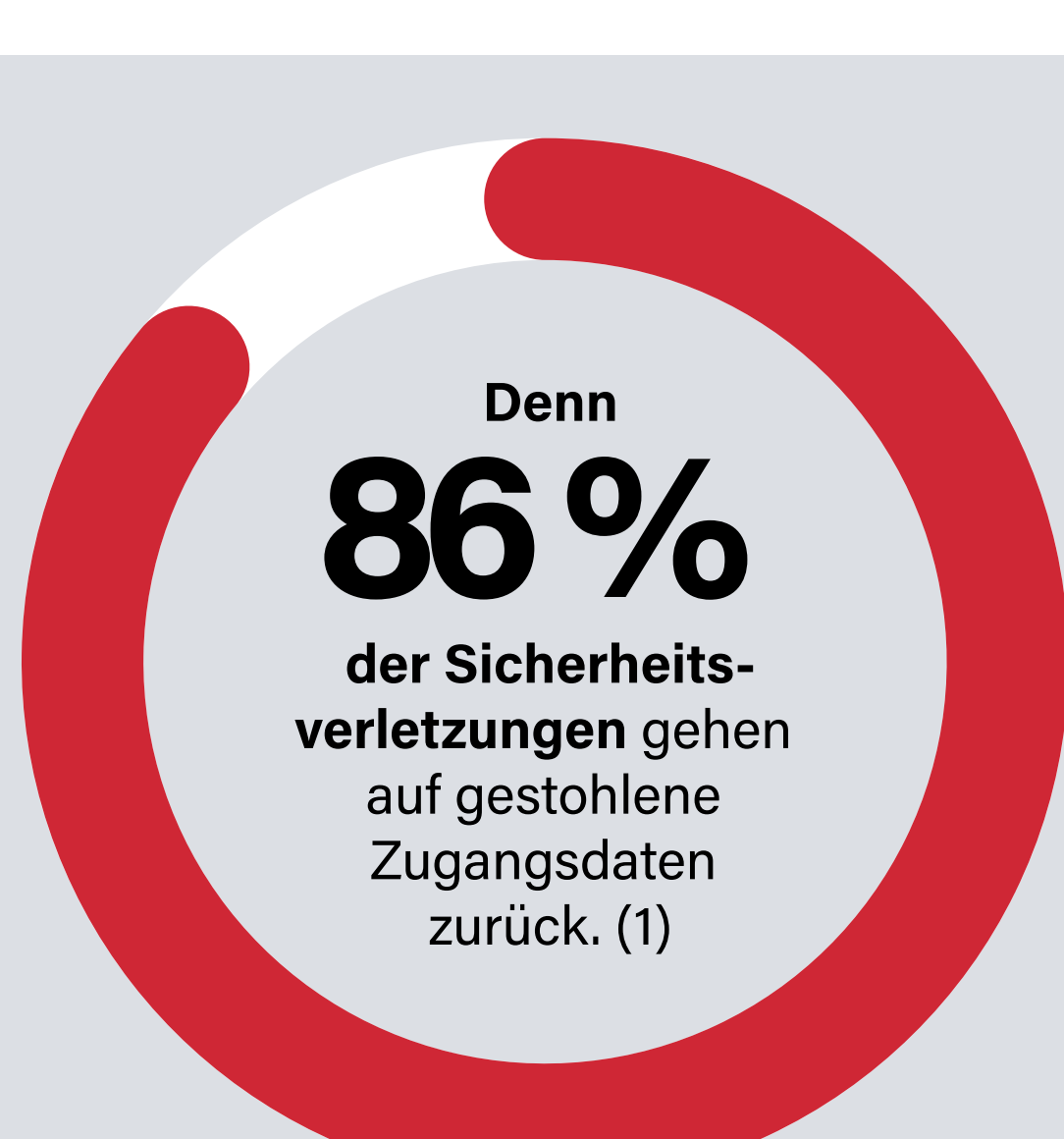


Post-its eignen sich nicht für Passwörter:

Was eine Sicherheitsverletzung Ihr Unternehmen kosten könnte

Fluffy123

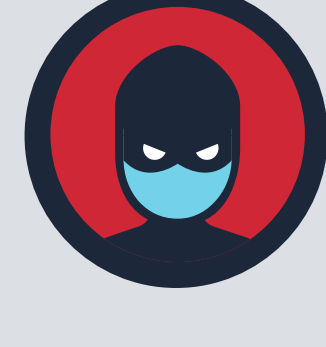
Sie denken, dass Passwörter auf Post-its ungefährlich sind? Falsch gedacht.



Gestohlene Passwörter können Ihr Unternehmen unter Umständen teuer zu stehen kommen.

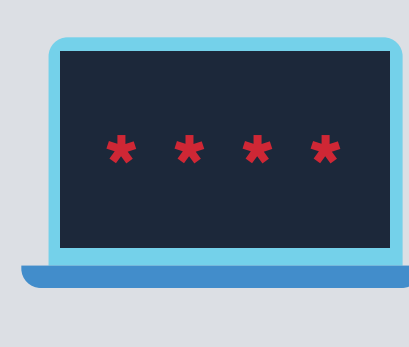
2023 beliefen sich die durchschnittlichen Kosten einer Datenschutzverletzung weltweit auf

4,45 Mio. USD.



4,76 Mio. USD

betragen die durchschnittlichen Kosten einer Datenschutzverletzung aufgrund von **Phishing**.



4,67 Mio. USD

betragen die durchschnittlichen Kosten einer Datenschutzverletzung aufgrund **kompromittierter geschäftlicher E-Mail-Konten**.

Bei Sicherheitsverletzungen ist Zeit von entscheidender Bedeutung.



Ein Datenleck von über **200 Tagen** Dauer kostet im Schnitt **4,95 Mio. USD.**



Wie lange dauert es durchschnittlich, um Sicherheitsverletzungen aufgrund gestohlener oder kompromittierter Zugangsdaten zu erkennen und einzudämmen?

328 Tage. (3)

Kompromittierte Zugangsdaten kosten Unternehmen viel Geld. Wie können sie sich schützen?

Mit einem Passwort-Manager!



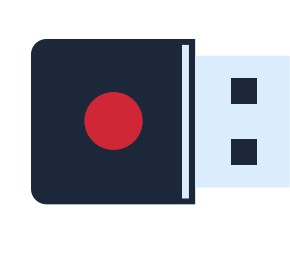
Keine Wiederverwendung von Passwörtern durch Mitarbeitende



Verwaltung aller Passwörter an einem Ort



Schutz für sensible Daten Ihrer Mitarbeitenden



Freigabe von Passwörtern erfolgt einfach und sicher



Post-its haben sich ausgeklebt. Passwortstress adieu.

LastPass erleichtert Ihren Mitarbeitern den Umgang mit Passwörtern und gibt Ihrem Unternehmen gleichzeitig mehr Kontrolle über Zugangsdaten.

Mit mehr als einer Milliarde abgesicherter Websites, Millionen Nutzern und 100.000 Geschäftskunden bietet LastPass durchgängigen Passwortschutz und macht Onlinesicherheit einfach.

[Vertrieb kontaktieren](#)