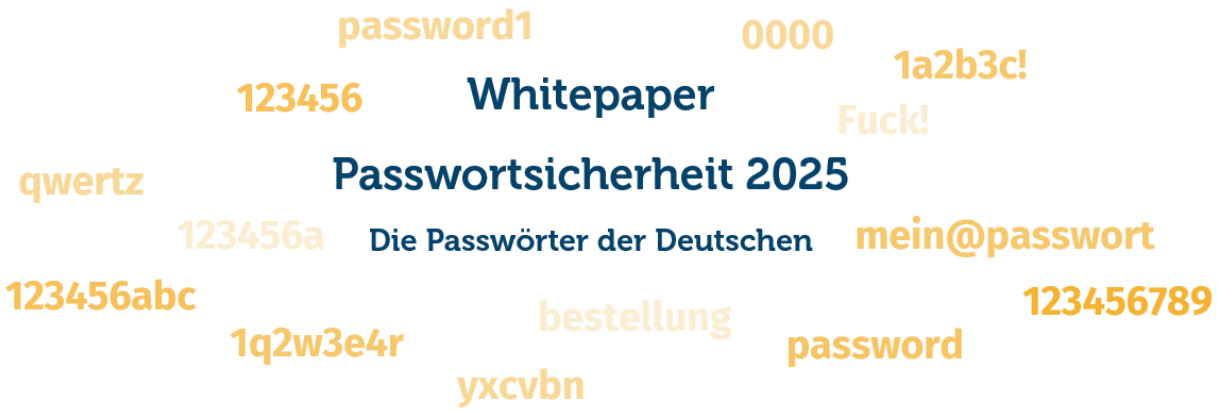
Passwortsicherheit 2025

Die Passwörter der Deutschen



Präambel

Identeco analysiert seit vielen Jahren große Mengen an Leakdaten und unterstützt Unternehmen dabei, Datenschutzanforderungen sowie Sicherheitsstandards wie BSI, ISO 27000 oder NIST zuverlässig zu erfüllen. Die Services des Unternehmens helfen, kompromittierte Accounts von Unternehmen und Plattformen frühzeitig zu erkennen und wirksam zu schützen.

Mit inzwischen über 57 Milliarden Datensätzen verfügt Identeco über eine der größten Leak-Datenbanken in Deutschland und Europa. In Zusammenarbeit mit der Universität Bonn wurden Leakdaten aus dem Jahr 2025 ausgewertet, um einen aktuellen Überblick über die Passwortpraxis in Deutschland zu gewinnen. Die Analyse basiert ausschließlich auf tatsächlich geleakten Datensätzen und erlaubt keine Rückschlüsse auf konkrete Sicherheitsvorfälle bei den genannten Organisationen. Der Fokus der Studie liegt auf Passwörtern, die gängigen deutschen Freemailern, den Domains der Vereine der ersten und zweiten Bundesliga sowie den größten deutschen Universitäten zugeordnet werden können.

1. Einleitung

Die Anzahl der Cyberangriffe auf Privatpersonen, Unternehmen und öffentliche Einrichtungen nimmt seit Jahren signifikant zu. Laut dem Bundeslagebild Cybercrime 2024 des BKA belief sich der durch Cyberkriminalität verursachte Schaden in Deutschland im Jahr 2024 auf rund 178,6 Mrd. €. Dies entspricht einer Zunahme von mehr als 30 Mrd. € gegenüber dem Vorjahr. Gleichzeitig ist ein deutlicher Anstieg von Phishing-Angriffen zu beobachten: Im Vergleich zu 2021 nahmen diese um fast 50 % zu, wobei der Einsatz KI-gestützter Sprachmodelle die Qualität und Glaubwürdigkeit entsprechender Phishing-Mails weiter erhöht hat (vgl. die Studie von Hoxhunt in diesem Zusammenhang). Auch das BKA stuft Phishing weiterhin als eine der effektivsten Methoden zur Erlangung sensibler Zugangsdaten ein.

Ein zentraler Angriffsvektor besteht in der missbräuchlichen Nutzung zuvor geleakter oder gestohlener Zugangsdaten. Solche Login-Daten gelangen häufig im Rahmen von Phishing-Angriffen oder infolge von Datenpannen in den illegalen Handel und werden dort systematisch als Handelsware genutzt.

Das vorliegende Whitepaper analysiert die Risiken, die sich aus kompromittierten Login-Daten ergeben, und untersucht insbesondere die Rolle von Passwortstärke und Passwortwiederverwendung bei Account-Übernahmen.

1.1 Accounts und Accountübernahmen

Ein Account ist ein digitales Benutzerkonto, das Personen oder Organisationen den Zugriff auf Dienste und Funktionen wie E-Mail, Online-Shops, soziale Netzwerke oder Unternehmenssysteme ermöglicht. Von einer Account-Übernahme spricht man, wenn Angreifer sich unrechtmäßig Zugriff auf einen solchen Account verschaffen. Dies geschieht in der Regel mithilfe gültiger Login-Daten, beispielsweise in Form einer Kombination aus E-Mail-Adresse und Passwort.

Gelingt es Kriminellen, einen persönlichen Account zu kompromittieren, können sie nahezu alle Funktionalitäten nutzen, die der Account bietet. Dazu zählen unter anderem das Lesen und Versenden von Nachrichten, der Zugriff auf persönliche Daten (Adressen, Kontoverbindungen etc.) oder das Auslösen von Bestellungen. Für die Betroffenen kann dies erhebliche und teils langfristige Konsequenzen haben. Insbesondere können im Namen der betroffenen Person weitere Straftaten wie Beleidigungen oder Phishing-Angriffe begangen werden. Gleichzeitig verliert der Plattformbetreiber den Überblick darüber, welche Aktivitäten tatsächlich vom legitimen Nutzer stammen. Weiterführende Informationen zu diesem Thema finden Sie in unserem Blog unter dieser URL:

https://identeco.de/de/blog/effects_of_ato.

Um einen Online-Account angemessen zu schützen, ist die Wahl eines sicheren Passworts unerlässlich. Einfach zu erratende Passwörter wie „123456“ werden von Angreifern gezielt und automatisiert getestet und führen häufig zu erfolgreichen Kompromittierungen. Die Qualität von Passwörtern ist daher

sowohl für den individuellen Schutz als auch für den Schutz angebundener Organisationen und Institutionen von zentraler Bedeutung.

1.2 Bedrohungslage und Herausforderungen durch geleakte Login-Daten

Ziel der vorliegenden Untersuchung ist es, einen Einblick in gängige Passwortpraktiken sowie die aktuelle Passwortqualität in Deutschland zu geben. Hierzu analysieren wir insbesondere Passwörter, die im Jahr 2025 im Rahmen von Datenleaks identifiziert wurden, und leiten daraus Rückschlüsse auf den tatsächlichen Umgang mit Login-Daten ab. Der Fokus liegt dabei auf Passwortgewohnheiten im privaten Umfeld sowie auf der Passwortkultur an den größten deutschen Hochschulen und bei Vereinen der ersten und zweiten Fußball-Bundesliga.

2. Methodik und Datenbasis

Identeco ist ein Bonner IT-Security-Unternehmen, das sich vollständig auf die Herausforderungen durch geleakte Login-Daten spezialisiert hat. Hierzu durchsucht Identeco kontinuierlich Quellen im Clear-, Deep- und Darknet nach geleakten Zugangsdaten, bereitet diese datenschutzkonform auf und integriert sie in eine eigene Leak-Datenbank, die inzwischen mehr als 57 Milliarden Datensätze umfasst. Identeco nutzt diese Daten, um Accounts, die von Account-Takeover bedroht sind, frühzeitig zu identifizieren und präventive Schutzmaßnahmen zu ermöglichen.

Grundlage der vorliegenden Studie sind Passwörter, die im Jahr 2025 im Rahmen dieses Prozesses identifiziert wurden. In die Analyse flossen ausschließlich Passwörter ein, die im Zusammenhang mit E-Mail-Adressen aus den betrachteten Domains standen, darunter Freemailer, die größten deutschen Hochschulen sowie Erst- und Zweitligisten der deutschen Fußball-Bundesliga. Auf diese Weise lassen sich gezielte Aussagen über das Passwortverhalten in diesen drei Bereichen treffen.

Alle Daten wurden vor der Auswertung anonymisiert: Nicht relevante Datensätze wurden verworfen, konkrete E-Mail-Adressen wurden nicht in der Untersuchung betrachtet, und Passwörter mit erkennbarem Bezug zu Personen oder Organisationen wurden durch neutrale Platzhalter ersetzt (d. h. das (fiktive) Passwort “Uni@Bonn123” haben wir durch den Platzhalter [*Uni*|*Stadt*] ersetzt). Dadurch werden direkte Rückschlüsse auf einzelne Institutionen vermieden, während gleichzeitig typische Muster der Passwortwahl erkennbar bleiben.

3. Unterschiede in der Passwortkultur

Die Analyse unterscheidet zwischen drei Bereichen: dem privaten Umfeld, dem wirtschaftlichen Kontext und dem öffentlichen Dienst. Diese Differenzierung offenbart deutliche Unterschiede in der Passwortkultur der jeweils betrachteten Gruppen. Sämtliche in diesem Abschnitt analysierten Datensätze stammen aus dem Jahr 2025.

3.1 Private Accounts

Für die Analyse privater Passwörter wurden ausschließlich Datensätze berücksichtigt, die mit E-Mail-Adressen gängiger Freemailer im deutschsprachigen Raum verknüpft waren. Insgesamt flossen fast eine Milliarde Datensätze in die Auswertung ein. Diese hohe Zahl erklärt sich durch die Vielzahl an Online-Accounts, die einzelne Nutzer typischerweise bei Shops, Streaming-Diensten oder sozialen Netzwerken unterhalten.

TOP20 privater Passwörter in Deutschland

Pos.	Passwort	Pos.	Passwort
1.	123456	11.	102030
2.	123456789	12.	123123
3.	12345678	13.	123
4.	[*Passwort*]	14.	1q2w3e4r
5.	1234	15.	ploplo01
6.	123456	16.	qwerty
7.	12345	17.	1q2w3e4r5t
8.	admin	18.	123456789
9.	qwerty123	19.	rr44tt55
10.	love8620	20.	Aa123456

Quelle: Identeco.de

Die Top-20-Passwörter zeigen gegenüber der Identeco-Studie aus dem Jahr 2024 ein weitgehend unverändertes Bild. Viele der am häufigsten verwendeten Passwörter sind identisch geblieben. Auffällig ist weiterhin das niedrige Sicherheitsniveau im privaten Umfeld: Zahlreiche Plattformen scheinen nach wie vor lediglich Mindestanforderungen an die Passwortlänge zu stellen, wodurch extrem einfache Passwörter wie „123456789“, „1111111“ oder sogar „password“ weiterhin weit verbreitet sind.

Solche Passwörter sind zwar leicht zu merken, bieten jedoch kaum Schutz. Sie gehören zu den ersten Kombinationen, die bei automatisierten Brute-Force-Angriffen getestet werden, und führen entsprechend häufig zu erfolgreichen Account-Übernahmen.

Auch regionale Einflüsse sind in der privaten Passwortwahl deutlich erkennbar. Städtenamen wie „Berlin“, „Hamburg“ oder „Dortmund“ tauchen regelmäßig auf. Darüber hinaus finden sich viele Passwörter mit Bezug zur Popkultur, etwa Variationen von „gollum“, „starwars“ oder Namen bekannter Pokémon.

Auffällig ist zudem der Einfluss unterschiedlicher Tastaturlayouts: Neben „qwertz“ (deutsche Tastatur) erscheint die US-Variante „qwerty“ sogar noch häufiger. Darüber hinaus nutzen viele Anwender Passwörter, die an den Namen eines Dienstes angelehnt sind, beispielsweise Varianten von „Netflix“. Diese finden sich zwar nicht in den Top 20, treten jedoch insgesamt häufig auf.

3.2 Vereine der ersten und zweiten deutschen Fußball-Bundesliga

Zur Analyse der Passwortkultur im Umfeld der Vereine der ersten und zweiten Fußball-Bundesliga wurden Passwörter betrachtet, die E-Mail-Adressen aus den jeweiligen Vereinsdomains zugeordnet werden konnten. Hier zeigt sich deutlich, dass Variationen des Vereinsnamens mit großem Abstand am häufigsten als Passwort verwendet werden. Gemeint sind dabei nicht die exakten Vereinsnamen, sondern Abwandlungen wie „Verein1905“ oder Leet-Speak-Varianten.

TOP20 der Passwörter der ersten und zweiten Fußball-Bundesliga

Pos.	Passwort	Pos.	Passwort
1.	[*Verein*]	11.	ballak
2.	bertolino	12.	Rakitic!
3.	Fussball	13.	Meister0809
4.	Garmin21	14.	effenberg1
5.	jonas131	15.	arschloch
6.	kartoffel1	16.	wolfsrudel
7.	QdIDLiIK123	17.	Aufstieg20!
8.	rakitic	18.	Justin123
9.	tapete191170	19.	1234567890!
10.	Weltfrieden1	20.	123456l

Quelle: Identeco.de

Dabei ist zu beachten, dass es sich überwiegend um Passwörter handelt, die im professionellen Kontext Verwendung finden. Trotz der Erwartung, dass professionelle Sportorganisationen erhöhte Sicherheitsstandards umsetzen, finden sich auch hier zahlreiche einfache und leicht ableitbare Passwörter. Neben klassischen Kombinationen wie „123456“ oder „password“ treten häufig leicht abgewandelte Varianten wie „Password1“ auf.

Auffällig ist zudem der häufige Bezug zu bekannten Spielernamen. So findet sich „ballak“ in den Top 20, ebenso wie Varianten von „effenberg“, „netzer“ oder „lahm“. Ergänzend tauchen Passwörter mit direktem Bezug zum sportlichen Geschehen auf, etwa „Aufstieg09“ oder „Meister24“. Der sportliche Ehrgeiz spiegelt sich damit auch in der Passwortwahl wider.

Insgesamt zeigt sich ein ausgeprägter „Vereinsstolz“, der sich in der häufigen Verwendung vereinsbezogener Passwörter manifestiert.

3.3 Hochschulen und Universitäten

Die Passwortkultur an Hochschulen und Universitäten wurde anhand von Domains deutscher Hochschulen analysiert, an denen laut öffentlich zugänglicher Quellen jeweils mehr als 20.000 Studierende immatrikuliert sind. Auch hier dominieren Passwörter, die sich aus Institutions- oder Städtenamen ableiten, wenngleich Trivialpasswörter seltener auftreten als im privaten Umfeld.

TOP20 der Passwörter von deutschen Hochschulen und Universitäten

Pos.	Passwort	Pos.	Passwort
1.	[*Uni*|*Stadt*]	11.	1hasseApple
2.	password	12.	abcd1234
3.	123456	13.	Alemaniaa
4.	Anika2fast4u	14.	fachschaft
5.	123456789	15.	appledrift06
6.	moritz	16.	BananA
7.	bestellung	17.	bastian
8.	Qwer3950	18.	blubber
9.	qwertz	19.	carolin
10.	Almamater	20.	D@niel12

Quelle: Identeco.de

Abseits der Top 20 finden sich häufig Passwörter, die auf einen angestrebten Studienabschluss hinweisen, etwa Variationen von „Bachelor2023“. Ebenso treten Passwörter mit Fachbezug auf, beispielsweise „Astrophysik123!“, oder Kombinationen aus beiden Ansätzen wie „PhD@Law2020“.

4. Allgemeine Veränderung im Vergleich zum Vorjahr

Obwohl die Top 20 der Freemailer weiterhin zahlreiche Trivialpasswörter wie „12345678“ enthalten, lässt sich im Vergleich zum Vorjahr eine deutliche Steigerung der Passwortqualität feststellen. Gleichzeitig gilt jedoch: Selbst ein sehr starkes Passwort bietet keinen ausreichenden Schutz mehr, sobald es öffentlich bekannt geworden ist.

Auffällig ist zudem die zunehmende Verbreitung sogenannter „verwandter“ Passwörter, also Passwörter, die auf demselben Stamm basieren, beispielsweise „HelmuT!rulez“ und „HelmuT@Rulez“. Zwar ist nicht auszuschließen, dass solche Passwörter von unterschiedlichen Nutzern stammen, das gehäufte gemeinsame Auftreten spricht jedoch für einen anderen Ursprung.

In Kombination mit der insgesamt hohen Qualität der gefundenen Datensätze deutet dies auf eine zunehmende Verbreitung sogenannter Stealer-Logs hin. Dabei handelt es sich um Datensammlungen, die durch Schadsoftware erzeugt werden, welche lokal gespeicherte Zugangsdaten – etwa aus Browsern oder Passwortmanagern – ausliest und an Angreifer überträgt. In solchen Fällen werden sämtliche Passwörter eines Nutzers gleichzeitig kompromittiert, insbesondere auch solche, die nach ähnlichen Mustern aufgebaut sind. Weiterführende Informationen zu diesem Thema finden Sie hier:

https://identeco.de/de/blog/die_unsichtbare_gefahr_wie_stealer_malware_ihre_informationen_stiehlt

5. Schutzmaßnahmen zur Erhöhung der Account-Sicherheit

Schwache und insbesondere geleakte Passwörter stellen ein erhebliches Sicherheitsrisiko für private Accounts und personenbezogene Daten dar. Der sorgfältige Umgang mit Zugangsdaten ist daher ein zentraler Bestandteil persönlicher Cybersicherheit. Neben den gängigen Schutzmaßnahmen, welche wir bereits an in der entsprechenden Studie des Jahres 2024 thematisiert haben, müssen wir an dieser Stelle noch einmal betonen, dass ein wesentlicher Aspekt der persönlichen Cybersicherheit die Sicherheit der eigenen Passwörter ist.

Hinweise für einen effektiven Accountschutz

1. Anlassbezogener Passwortwechsel
2. Vermeidung von Passwortwiederverwendung
3. Nutzung eines Passwortmanagers
4. Bewusste und ausreichende Passwortkomplexität
5. Aktivierung von Multi-Faktor-Authentifizierung
6. Regelmäßige Überprüfung der eigenen Leak-Betroffenheit

Um zu überprüfen, ob eigene Zugangsdaten bereits kompromittiert wurden, empfehlen wir eine regelmäßige Prüfung der eigenen E-Mail-Adresse mit dem **Leak Inspector**. Der Leak Inspector ist ein kostenfrei von Identeco bereitgestelltes Online-Tool, mit dem Endnutzer ihre Betroffenheit von bekannten Datenleaks ermitteln können. Die Möglichkeit zur Leak-Prüfung wird schon seit fünf Jahren in Eigenregie an der Universität Bonn angeboten und warnt Verbraucher vor Datenleaks. Ein Thema, das relevant ist wie nie.

Der Leak Inspector ist unter folgender Adresse erreichbar:

https://leak-inspector.de.

Neben der Verantwortung des Endverbrauchers können auch Plattformbetreiber Sicherheitsmaßnahmen ergreifen. Identeco bietet Lösungen an, mit denen Zugangsdaten vollautomatisiert, datenschutzkonform und ohne Einbezug der Plattformnutzer gegen die umfangreiche Identeco-Leak-Datenbank geprüft werden können. Auf diese Weise können Plattformen sicherstellen, dass potenziell kompromittierte Accounts frühzeitig erkannt und abgesichert werden.

Für eine individuelle Beratung können Sie unter der folgenden URL einen Termin mit den Identeco-Experten vereinbaren:

https://meeting.identeco.de/team/identeco/meet-identeco

Fazit

Die vorliegende Analyse zeigt, dass geleakte Login-Daten weiterhin ein erhebliches Sicherheitsrisiko für Privatnutzer und Organisationen darstellen, insbesondere für Hochschulen und Sportvereine. Trotz erkennbarer Verbesserungen in der Passwortqualität bleiben schwache oder leicht ableitbare Passwörter weit verbreitet. Häufig sind diese durch regionale Begriffe, Vereins- oder Institutionsnamen sowie persönliche Bezugspunkte geprägt. Gleichzeitig deutet das vermehrte Auftreten ähnlicher, qualitativ hochwertiger Passwörter darauf hin, dass zunehmend Stealer-Logs anstelle klassischer Datenpannen die Quelle vieler Leaks darstellen, was das Risiko großflächiger Account-Übernahmen weiter erhöht.

Um diesen Risiken nachhaltig zu begegnen, sind robuste Authentifizierungsverfahren, kontinuierliche Sensibilisierung für Passwortsicherheit und ein verantwortungsvoller Umgang mit Zugangsdaten unerlässlich.

Diese Studie wurde von Identeco in Zusammenarbeit mit der Rheinischen Friedrich-Wilhelms-Universität Bonn erstellt.