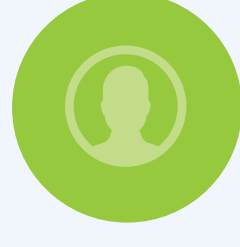




Befinden sich einzelne Nutzer und IT-Fachleute bezüglich der Sicherheit auf Augenhöhe?

Eine aktuelle Studie des Ponemon-Institutes zeigt, dass sowohl IT-Fachleute als auch einzelne User trotz zunehmender Bedenken hinsichtlich der Privatsphäre und der IT-Security riskante Sicherheitspraktiken anwenden. Allerdings gehen Erwartung und Realität innerhalb der beiden Gruppen oft auseinander, wenn es um die Umsetzung von praktikablen und wünschenswerten Sicherheitslösungen geht.

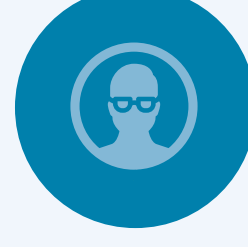


Individuen

vs.

IT-Fachleute:

Sicherheitsüberzeugungen und -verhalten



Personen in den USA, Großbritannien, Frankreich, Schweden, Australien und Deutschland

IT-Fachleute in Deutschland

25%

Sind in den letzten zwei Jahren **sehr besorgt** bezüglich der Privatsphäre und Sicherheit ihrer persönlichen Daten geworden.

39%

76%

Von den Einzelpersonen und IT-Fachleuten, die eine **Übernahme ihres Kontos** erlebt haben, änderten einige die Art und Weise, wie sie Passwörter verwalteten oder ihre Konten schützten.

67%

64%

Verwenden 2FA nicht als eine Form des Schutzes für persönliche Konten.

65%

39%

Geben an, **Passwörter** über Arbeitsplatzkonten hinweg **wiederzuverwenden**.

39%

51%

Teilen manchmal oder häufig **Passwörter** mit Kollegen.

45%

Schutz der Belegschaft

45% der deutschen IT-Fachleute gaben an, dass ihre Organisation einen **Phishing-Angriff** erlebt hat, 13% sind einem **Ransomware-Angriff** zum Opfer gefallen, weitere 12% einem **Diebstahl von Anmeldeinformationen** und 9% einem **Man-in-the-Middle-Angriff**.



35%

der deutschen IT-Fachleute geben an, dass ihr Unternehmen einen **Passwordmanager** verwendet; ein effektives Tool zur sicheren Erstellung, Verwaltung und Speicherung von Passwörtern.

34%

der deutschen IT-Fachleute geben an, dass ihre Organisation sich auf **Post-it Zettel** verlässt, um Passwörter zu verwalten.

51%

der IT-Fachleute geben an, dass ihre Organisation sich bei der Verwaltung von Passwörtern auf **das menschliche Gedächtnis verlässt**.

Passwortverwaltung & Verhinderung von Kontoübernahmen

50%

der IT-Fachleute in Deutschland sind auf die **Verwendung von 2FA angewiesen**, um Zugang zu Firmenkonten zu erhalten.

36%

der deutschen Betriebe, die 2FA zur Sicherung von Geschäftskonten implementiert haben, **verlassen sich auf mobile Authentifizierungs-Apps** und 33% auf **SMS-Codes**.



23% der Einzel-User in den Vereinigten Staaten, Großbritannien, Deutschland, Frankreich, Schweden und Australien glauben, dass SMS oder mobile Authentifizierungs-Apps als 2FA-Methoden **sehr unpraktisch** sind.

54%

dieser Befragten sind der Meinung, dass SMS oder mobile Authentifizierungs-Apps **ihren Arbeitsablauf stören**.



47%

dieser Befragten sind der Meinung, dass das Kopieren und Einfügen von Einmal-Codes **lästig** ist.

Sicherung mobiler Nutzer

52%

der deutschen Organisationen **erlauben die Nutzung von persönlichen mobilen Geräten**.

72%

der Unternehmen in Deutschland **glauben nicht**, dass sie die notwendigen Maßnahmen **zum Schutz von Informationen auf mobilen Geräten** ergreifen.

54%

der Einzelnutzer in den USA, Großbritannien, Frankreich, Schweden, Australien und Deutschland, die ein privates Gerät verwenden, um auf arbeitsbezogene Daten zuzugreifen, **nutzen keine 2FA**.

Schutz von Kundenkonten

Kundendaten und **personenbezogene Daten** stehen ganz oben auf der Liste der Informationen, die IT-Fachleute schützen müssen. Dennoch berichten 54% der deutschen Befragten, dass Kundenkonten bereits durch eine Kontoübernahme kompromittiert wurden.

55%

dieser Befragten geben an, dass sie glauben, Benutzernamen und Passwörter bieten **ausreichende Sicherheit**.

30%

der IT-Fachleute haben **keine Pläne**, Kunden 2FA zur Verfügung zu stellen.

45%

dieser Befragten geben an zu glauben, dass dies für Kunden **unpraktisch** sei.

Wenn es um den **Online-Zugriff auf Informationen** geht, bewerteten einzelne Benutzer in den Vereinigten Staaten, Großbritannien, Deutschland, Frankreich, Schweden und Australien **Sicherheit (56%), Erschwinglichkeit (57%) und Benutzerfreundlichkeit (35%)** als sehr wichtig.

Eine sicherere Zukunft erreichen

56% der US-amerikanischen, britischen, deutschen, französischen, schwedischen und australischen Bürger werden nur neue Technologien einsetzen, die einfach zu bedienen sind und die Sicherheit ihrer Konten deutlich verbessern.

55% der IT-Fachleute und Einzelpersonen in diesen Ländern bevorzugen eine Methode zum Schutz von Konten, die keine Passwörter beinhaltet.

57% der deutschen IT-Fachleute glauben, dass die Abschaffung von Passwörtern die **Sicherheit ihrer Organisation verbessern** würde.



50% der IT-Fachkräfte in Deutschland glauben, dass die Abschaffung von Passwörtern die **Benutzerfreundlichkeit verbessern** würde.

64% der deutschen IT-Fachleute glauben, dass der **Einsatz von Biometrie** das Sicherheitsniveau ihrer Organisation erhöhen würde.



53% der individuellen Nutzer in den Vereinigten Staaten, Großbritannien, Deutschland, Frankreich, Schweden und Australien glauben, dass der Einsatz von Biometrie eine **bessere Sicherheit** für ihre Konten bieten würde.

54% der deutschen IT-Fachleute glauben, dass ein **Hardware-Security Key** mehr Sicherheit bieten würde.



60% der US-amerikanischen, britischen, deutschen, französischen und australischen Nutzer wären bereit, **50 bis 60 Dollar zu zahlen**, um die höchste Form der Sicherheit für alle ihre Online-Konten zu erhalten.

Ausführliche Informationen zur Umfrage des Ponemon Institute finden Sie 2020 State of Password and Authentication Security Behaviors Report <https://www.yubico.com/authentication-security-behaviors-report-2020/>