Bundeskanzleramt

wirksam regieren

Zwischenbericht

Schutz von Online-Konten

Ergebnisse der ersten Projektphase

Referat *wirksam regieren* im Bundeskanzleramt in Zusammenarbeit
mit dem Bundesamt für Sicherheit in der Informationstechnik

Stand: März 2020

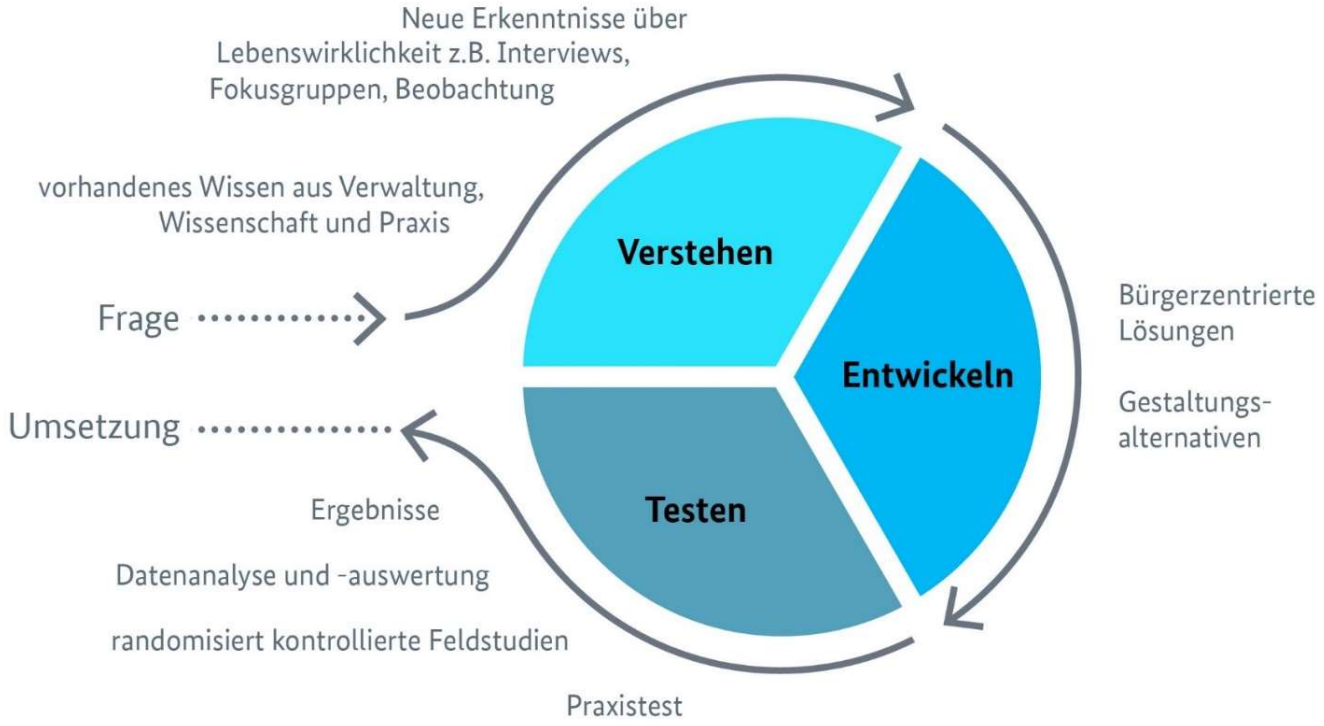
Bundesamt für Sicherheit in der Informationstechnik

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Überblick

- Im vorliegenden Zwischenbericht werden die wichtigsten Ergebnisse der ersten Phase des Projektes „Schutz von Online-Konten“ dargestellt.
- **Projektphase 1 – Verstehen**: In dieser Projektphase ging es darum, den Umgang der Bürgerinnen und Bürger mit Passwörtern besser zu verstehen.
- **Projektphase 2 – Entwickeln**: Auf der Basis der gewonnen Erkenntnisse sollen anschließend in einer zweiten Projektphase gemeinsam mit Bürgerinnen und Bürgern Lösungen entwickelt werden, die in ihrem Alltag und ihrer Lebensrealität anwendbar sind und funktionieren.
- **Projektphase 3 – Testen**: In einer dritten Projektphase sollen schließlich alternative Ausgestaltungen der entwickelten Lösungen in einem Feldexperiment hinsichtlich ihrer Wirksamkeit geprüft werden.

Projektphasen



Hintergrund

- Die zahlreichen Hacks von Online-Konten in der Vergangenheit sowie auch Studien zur Verwendung von Passwörtern verdeutlichen, dass viele Bürgerinnen und Bürger, von einem objektiven technischen Standpunkt betrachtet, ihre Online-Konten nur unzureichend schützen[*1].
- Diese Diskrepanz zwischen dem verfügbaren Wissen, wie Online-Konten durch starke Passwörter, Mehrfach-Authentisierungen[*2] oder durch die Verwendung von Passwortmanagern geschützt werden können und dem tatsächlichen Sicherheitsverhalten der Bürgerinnen und Bürger ist auffällig und erklärungsbedürftig.
- In diesem Projekt sollen Maßnahmen entwickelt und getestet werden, die Bürgerinnen und Bürger in der Breite dabei unterstützen, ihre Online-Konten wirksamer zu schützen.

[*1] siehe Literaturliste

[*2] Unter „Authentisierung“ wird verstanden, dass sich ein Nutzer gegenüber einem IT-System, zum Beispiel durch ein Passwort, ausweist. Die Überprüfung der Richtigkeit des Nachweises, zum Beispiel des Passworts, durch das IT-System wird dagegen als „Authentifizierung“ bezeichnet.

Zentrale Fragestellungen

- Wie gehen Bürgerinnen und Bürger beim Schutz ihrer Online-Konten genau vor?
- Worin liegen Hindernisse für den Schutz von Online-Konten (z.B. Bedienbarkeit, Aufwand, Vielzahl von Passwörtern, Misstrauen gegenüber technischen Lösungen)?
- Was denken Bürgerinnen und Bürger über verschiedene Sicherheits-verfahren (Passwörter, Passwortsafes und Passwortmanager, Zwei- oder Mehrfaktor-Authentisierungen mit Kombinationen aus Wissen, Besitz und Biometrie)?
- Welche Informationen und Hilfen wünschen sich Bürgerinnen und Bürger, um den Umgang mit Passwörtern einfacher und sicherer zu machen?
- Über welche Kommunikationswege möchten sie informiert werden?

Methoden

Gruppendiskussionen und Online-Befragung

- Zur Beantwortung der aufgeworfenen Fragen wurden in einer ersten Projektphase qualitative und quantitative Methoden kombiniert.
- Zuerst wurden Gruppendiskussionen durchgeführt, um ein tieferes Verständnis der Motivstruktur und Ziele der Bürgerinnen und Bürger im Umgang mit Passwörtern und anderer Sicherheitsverfahren zu erlangen.
- Danach wurde eine repräsentative quantitative Online-Befragung durchgeführt, um die Ergebnisse der qualitativen Phase an einer größeren Stichprobe zu validieren.
- Die Ergebnisse der Gruppendiskussionen und der Online-Befragung werden integriert dargestellt, da sich die Befunde gegenseitig ergänzen und die qualitativen Befunde auch zur Veranschaulichung und Vertiefung der quantitativen Ergebnisse dienen. Es wird durch „Online-Befragung“ oder „Gruppendiskussion“ gekennzeichnet, worauf sich die Ergebnisse beziehen.

Methode qualitativ: Gruppendiskussionen

- 10 Gruppendiskussionen mit jeweils 10 Teilnehmern (16.08. – 22.08.2019)
- Dauer: jeweils 90 Minuten; Ort: Berlin
- Homogene Gruppen, getrennt nach Geschlecht und fünf Altersgruppen

Alter	Geschlecht	
14-17	n=10 weiblich	n=10 männlich
18-29	n=10 weiblich	n=10 männlich
30-49	n=10 weiblich	n=10 männlich
50-64	n=10 weiblich	n=10 männlich
65 und älter	n=10 weiblich	n=10 männlich

Methode quantitativ: Online-Befragung

Merkmalsrepräsentative Befragung der deutschen Internetbevölkerung:

- Stichprobengröße: N=995
- Alter: 16 Jahre und älter
- Kreuzquoten: Geschlecht und Alter
- Randquoten: Bildung und Region
- Befragungsdauer: Median = 8 Minuten
- Durchführungszeitraum: 26.10. - 3.11.2019

Merkmalsrepräsentative Stichprobe der deutschen Bevölkerung, die das Internet nutzt

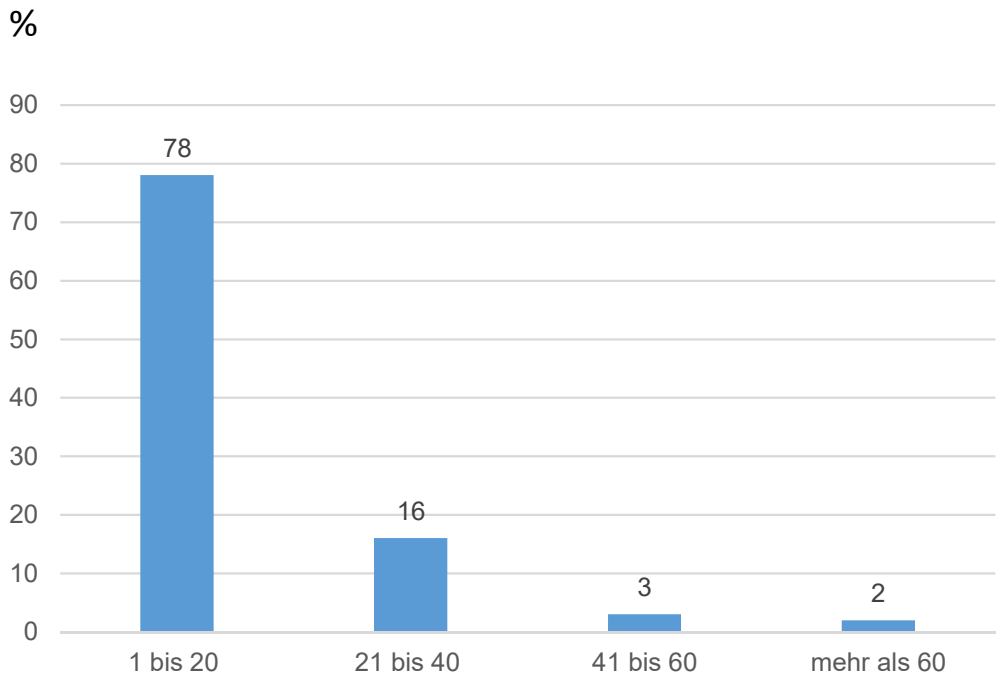
Alter/Geschlecht	männlich	weiblich
16-29	11%	11%
30-39	7%	7%
40-49	12%	10%
50-59	11%	10%
60+	12%	10%

Bildung	%
Kein oder Haupt- bzw. Volksschulabschluss	31
Weiterführende Schule: Realschule/POS	31
(Fach-)Abitur/Fach- bzw. Hochschulabschluss	38

Region	
Baden-Württemberg	14%
Bayern	16%
Berlin	3%
Brandenburg	3%
Bremen	1%
Hamburg	2%
Hessen	7%
Mecklenburg-Vorpommern	2%
Niedersachsen	10%
Nordrhein-Westfalen	23%
Rheinland-Pfalz	5%
Saarland	1%
Sachsen	5%
Sachsen-Anhalt	5%
Schleswig-Holstein	3%
Thüringen	3%

Ergebnisse

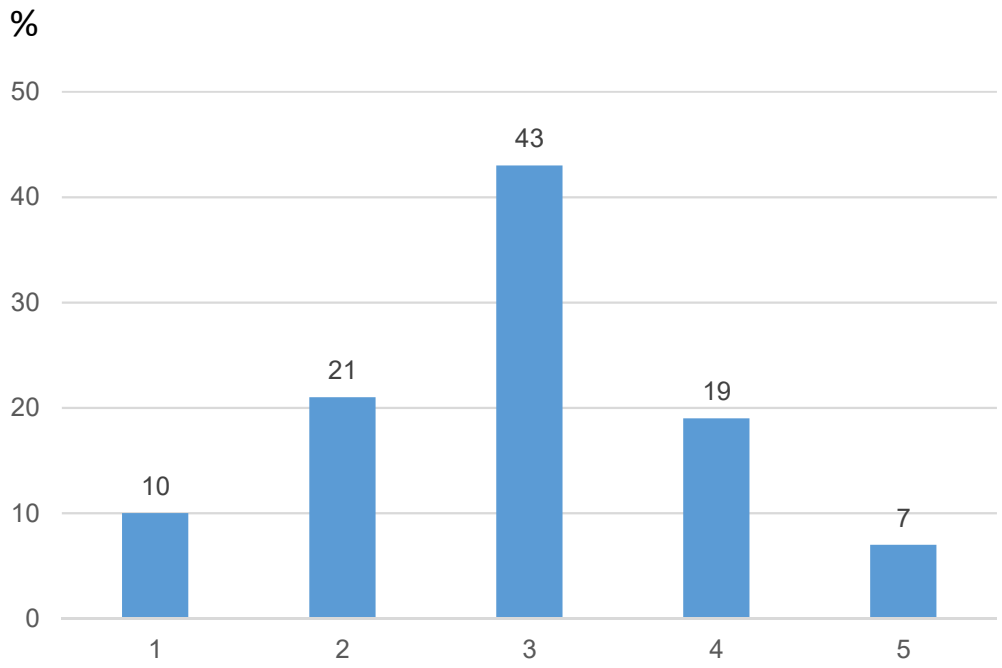
Knapp vier Fünftel der Befragten geben an, 1 bis 20 Online-Konten zu haben.



Wie viele Online-Konten (E-Mail, Online-Banking, Online-Händler, Soziale Medien etc.) haben Sie insgesamt, die durch ein Passwort geschützt sind?

Basis: Online-Befragung, alle Befragten

Im Durchschnitt wird die Gefahr, dass Datendiebe an Passwörter gelangen könnten, als „mittelhoch“ eingeschätzt.

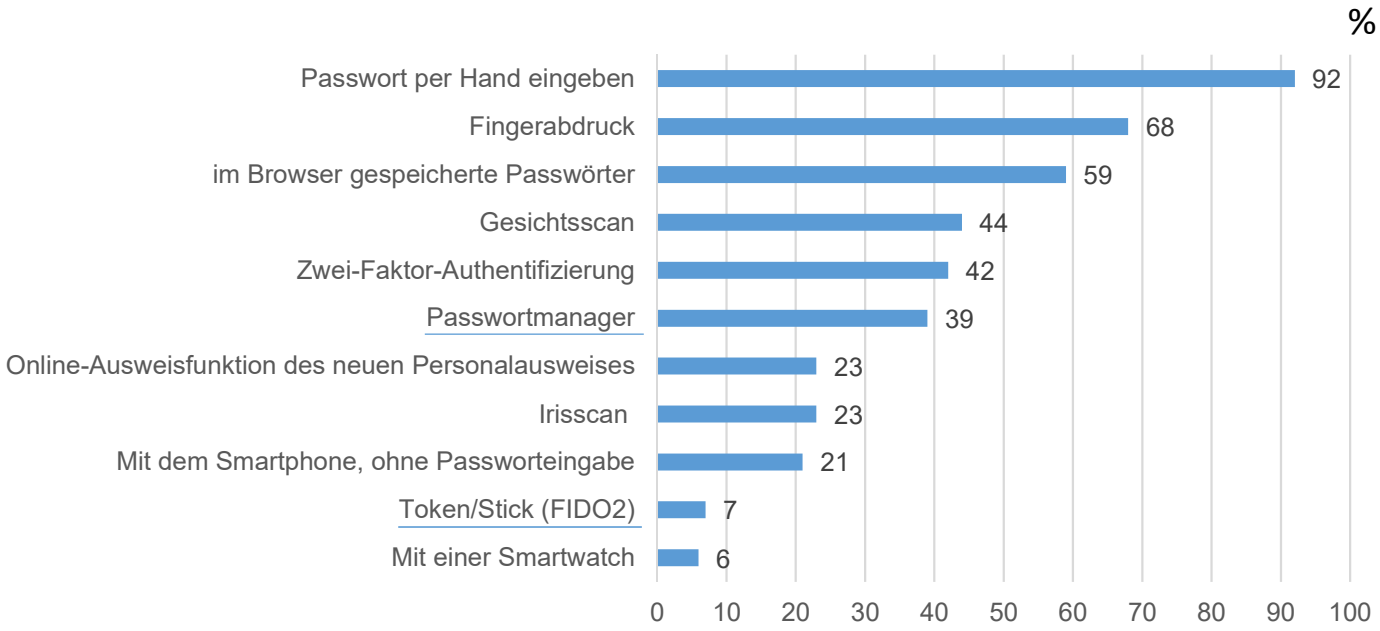


Mittelwert = 2,9

Wie hoch schätzen Sie die Gefahr ein, dass Datendiebe an Ihre Passwörter gelangen könnten, mit denen Sie Ihre Online-Konten schützen? (1 = sehr gering, 5 = sehr hoch)

Basis: Online-Befragung, alle Befragten

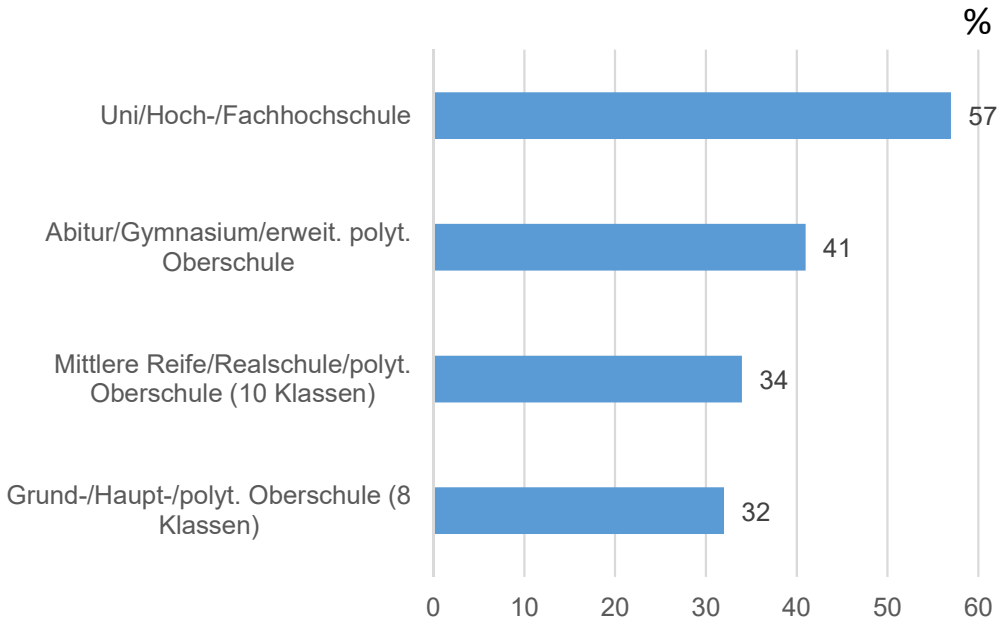
Rund 40% der Bürger kennen Passwortmanager. FIDO2 ist bisher kaum bekannt.



Welche der folgenden Möglichkeiten **kennen** Sie, um sich bei einem Online-Konto anzumelden? Mehrfachnennungen sind möglich.

Basis: Online-Befragung, alle Befragten

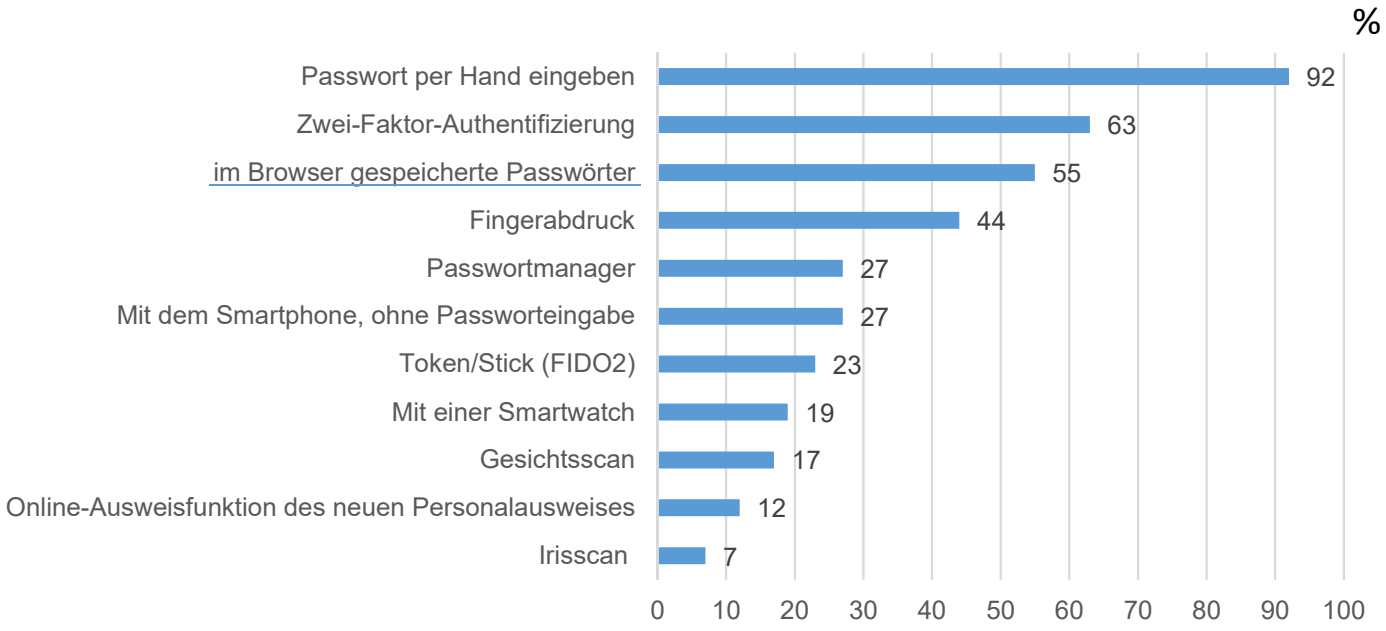
Die formal höher Gebildeten kennen häufiger die Möglichkeit von Passwortmanagern.



Anteil der Befragten in den Bildungsgruppen, die die Möglichkeit kennen, sich mit einem Passwortmanager bei einem Online-Konto anzumelden

Basis: Online-Befragung, alle Befragten

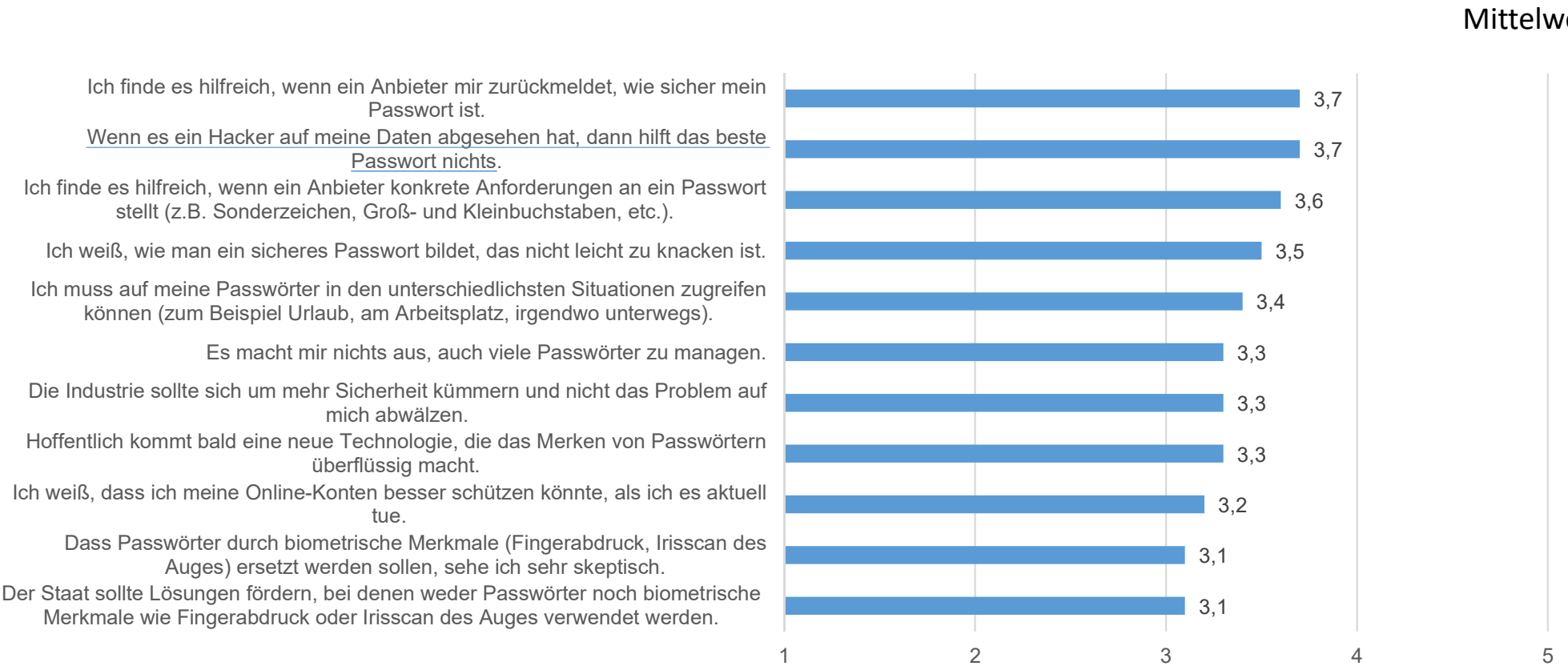
Mehr als die Hälfte der Befragten, die wissen, dass man Passwörter im Browser speichern kann, nutzen diese Möglichkeit.



Welche der folgenden Möglichkeiten **nutzen** Sie, um sich bei einem Online-Konto anzumelden? Mehrfachnennungen sind möglich.

Basis: Online-Befragung, alle Befragten, die angaben, dass sie die jeweilige Möglichkeit kennen (siehe Seite 14).

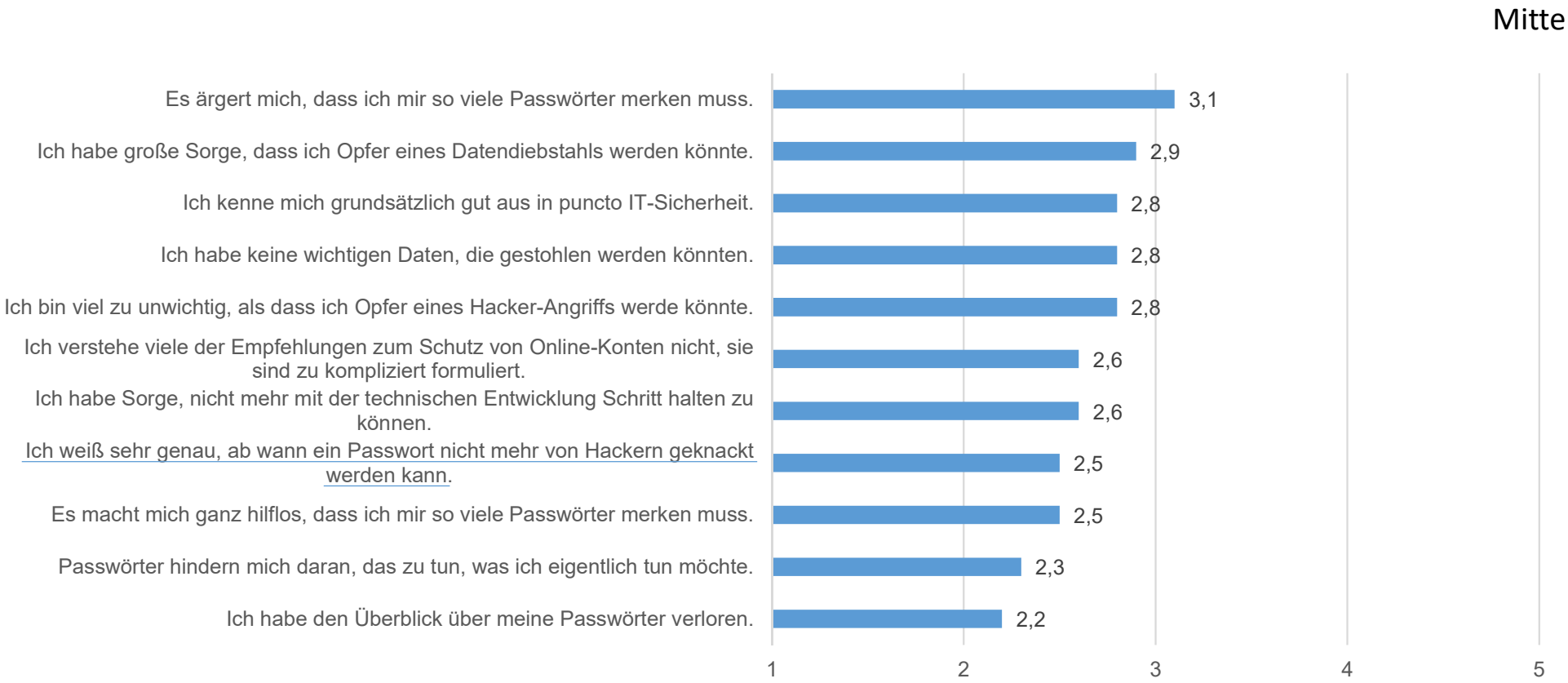
Die Befragten glauben eher nicht, dass sie sich durch Passwörter wirksam vor Hackern schützen können.



Wie sehr stimmen Sie den unteren Aussagen zu? (1 = stimme überhaut nicht zu, 5 = stimme voll und ganz zu)

Basis: Online-Befragung, alle Befragten

Die Befragten wissen eher nicht, ab wann ein Passwort nicht mehr von Hackern geknackt werden kann.



Wie sehr stimmen Sie den unteren Aussagen zu? (1 = stimme überhaut nicht zu, 5 = stimme voll und ganz zu)

Basis: Online-Befragung, alle Befragten

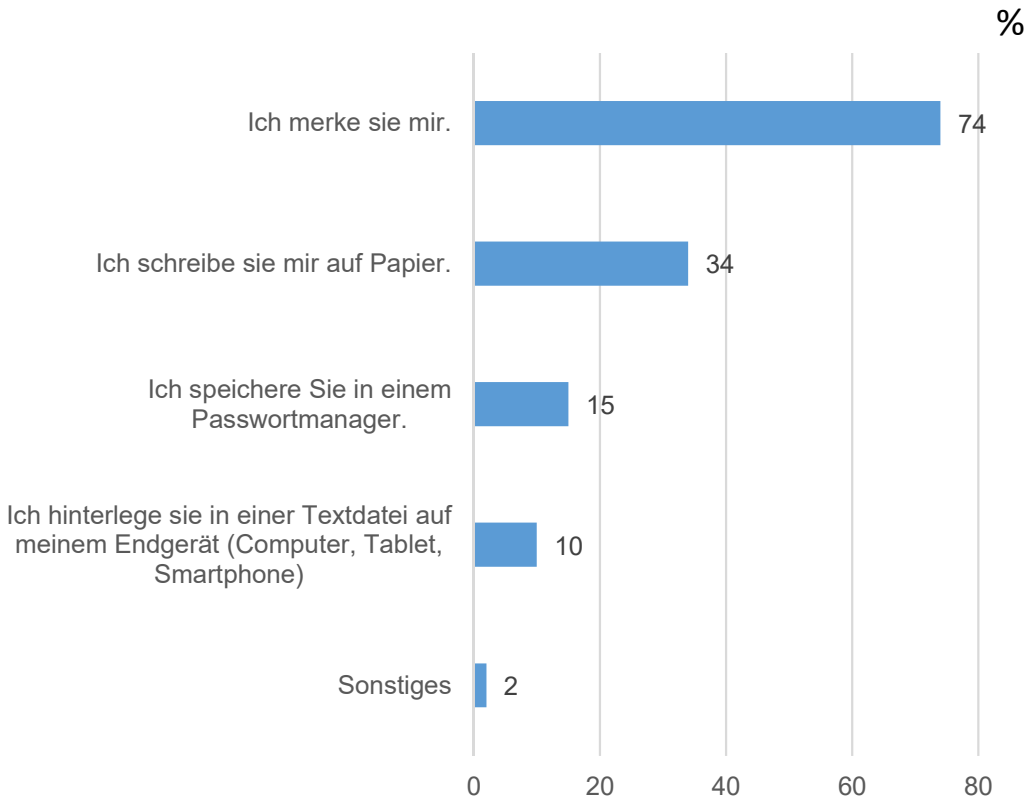
Zeit für die Passwortbildung und die Notwendigkeit, sich viele Passwörter zu merken, stehen im Alltag einem sicheren Passwortverhalten entgegen.

Hauptgründe
Zeit und Aufwand für sichere Passwörter
Sehr viele Passwörter müssen gemerkt werden
Faulheit/Bequemlichkeit
Komplexität

Was hält Sie ganz konkret im Alltag ab, Ihre Online-Konten möglichst optimal zu schützen?

Basis: Online-Befragung, alle Befragten, die mit 4 oder 5 auf folgende Frage geantwortet haben: „Ich weiß, dass ich meine Online-Konten besser schützen könnte, als ich es aktuell tue.“ (1 = stimme überhaut nicht zu, 5 = stimme voll und ganz zu (n=406))

Am häufigsten merken sich die Befragten ihre Passwörter im Gedächtnis.



Wo genau bewahren Sie die Passwörter für Ihre Online-Konten auf?
Mehrfachnennungen sind möglich.

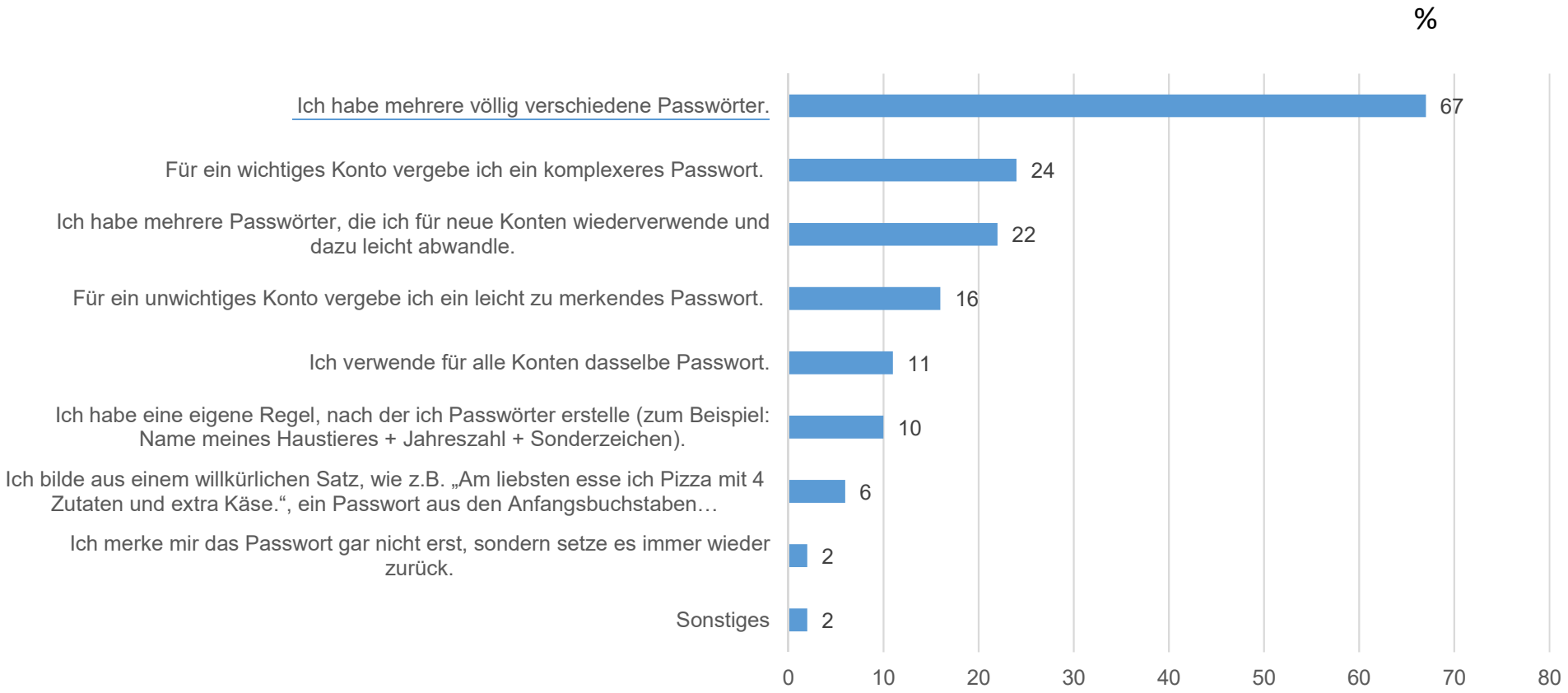
Basis: Online-Befragung, alle Befragten

Da sich die Teilnehmerinnen und Teilnehmer der Gruppen viele Passwörter merken müssen, stoßen sie an Grenzen der Merkfähigkeit.

- Aufgrund der Vielzahl der Online-Konten, die Teilnehmerinnen und Teilnehmer durch Passwörter schützen müssen, befinden sie sich aktuell in einer Situation der kognitiven Überforderung.
- Die kognitive Überforderung besteht in der begrenzten Merkfähigkeit; dies betrifft alle Altersgruppe.
- Die Generierung eines sicheren Passwortes wird nicht als Hauptbarriere gesehen, sondern die Anforderung ein eigenes sicheres Passwort für sehr viele Accounts (30-50) zu verwenden.
- Ferner wird die Passworteingabe als Hindernis angesehen, schnell ans (Handlungs-)Ziel zu kommen. „Es muss schnell gehen“.
- Passwörter werden in unterschiedlichen Kontexten (zu Hause, im Urlaub, am Arbeitsplatz etc.) abgefragt; das erschwert den Umgang.

Basis: Gruppendiskussion

Zwei Drittel der Befragten geben an, dass sie völlig verschiedene Passwörter vergeben.



Welche der unten aufgeführten Möglichkeiten nutzen Sie bei der Vergabe eines Passwortes? Mehrfachnennungen sind möglich.

Basis: Online-Befragung, alle Befragten

Strategien der Passwortnutzung I

- Über alle Altersgruppen hinweg versuchen die Teilnehmer, die Passwörter im Gedächtnis zu behalten oder schreiben sie sich auf Papier auf.
- Die Teilnehmer greifen auf die Möglichkeit des Zurücksetzens von Passwörtern zurück; dies wird als sichere und bequeme Methode gesehen, um sich die Passwörter nicht aufschreiben zu müssen.
- Es werden häufig einzelne „Master-Passwörter“ gebildet, die über die Accounts variiert werden, oder es werden nur wenige Passwörter für mehrere verschiedene Accounts verwendet.

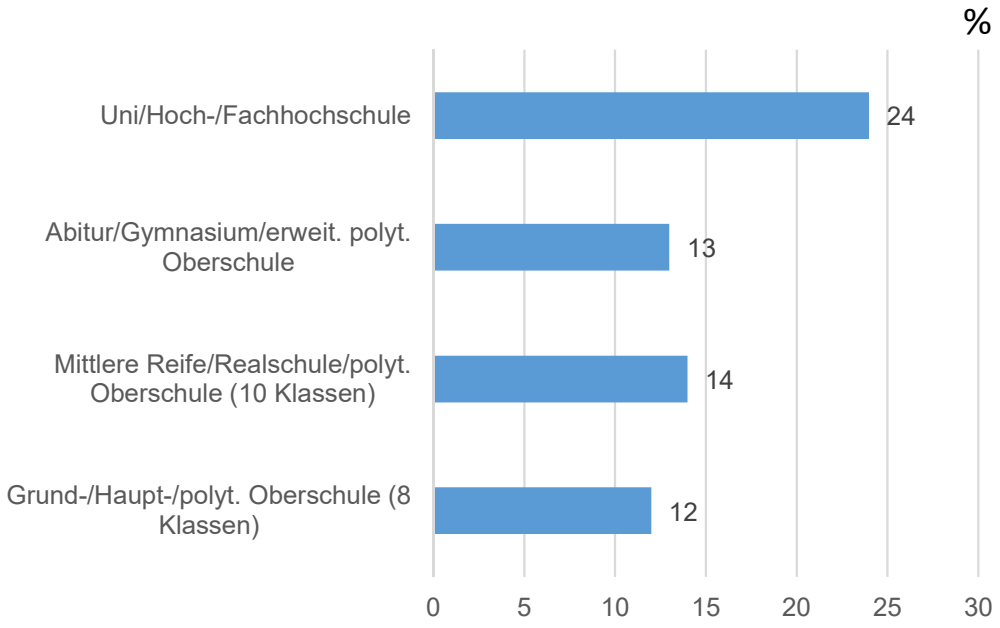
Basis: Gruppendiskussion

Strategien der Passwortnutzung II

- Die Teilnehmer der Gruppendiskussionen haben individuelle Algorithmen entwickelt, wie sie leichter Passwörter bilden und sich merken können: z.B. Name Haustier + Sonderzeichen + vierstellige Zahl + Ausrufezeichen. Zum Teil wandeln die Teilnehmer auch nur einzelne Elemente ihrer individuellen Algorithmen ab, um einen Bezug zu einem spezifischen Konto herzustellen, den sie sich gut merken können.
- Um der Überforderung Herr zu werden, nehmen die Teilnehmer eine Risikoabwägung vor; sie unterscheiden subjektiv, was wichtige und unwichtige Accounts sind; für „unwichtige“ Accounts werden einfache Passwörter oder bereits verwendete Passwörter vergeben.

Basis: Gruppendiskussion

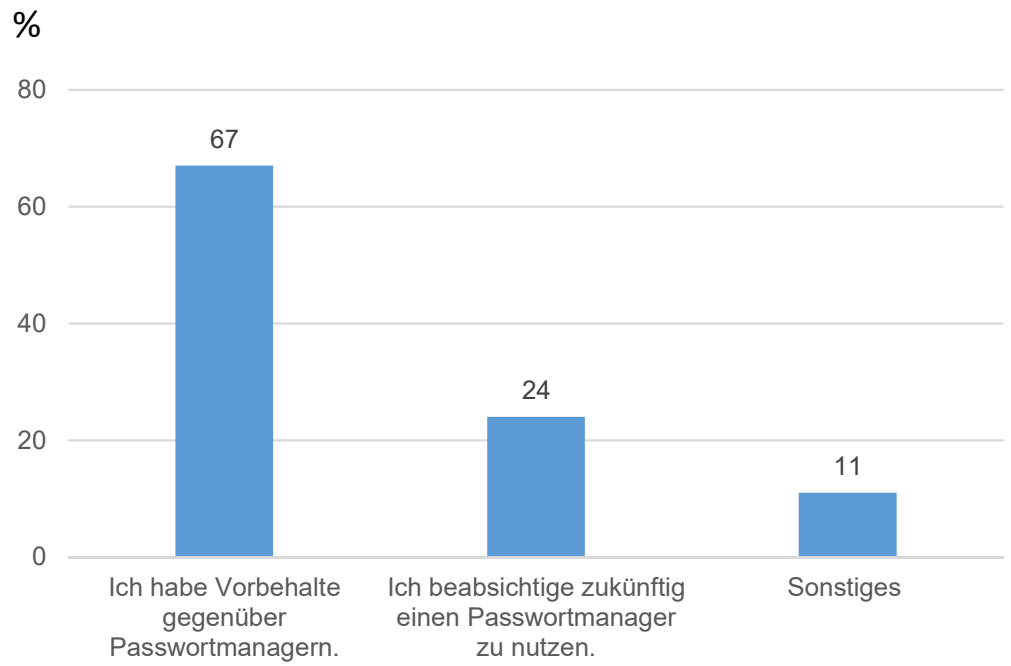
Die formal höher Gebildeten speichern häufiger ihre Passwörter im Passwortmanager als die formal geringer Gebildeten.



Anteil der Befragten in den Bildungsgruppen, die angaben, dass sie ihre Passwörter in einem Passwortmanager aufbewahren

Basis: Online-Betragung, alle Befragten

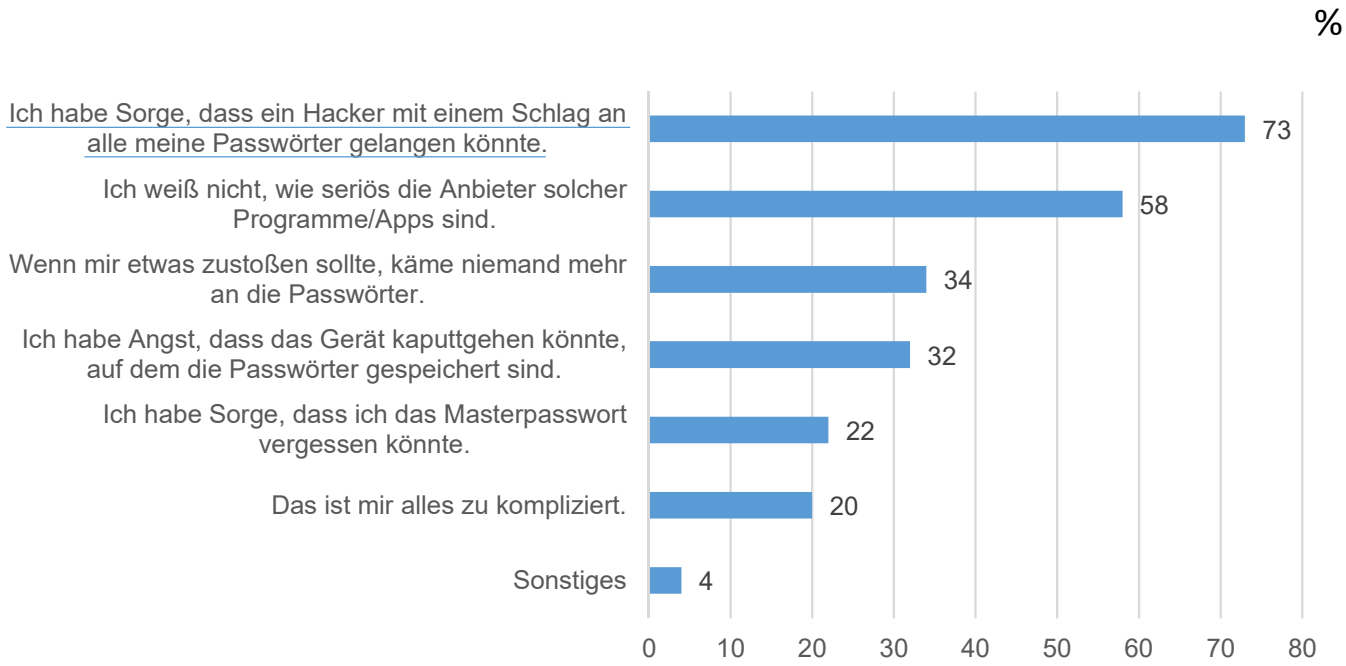
Bei denjenigen, die Passwortmanager kennen, sind Vorbehalte der Hauptgrund für die Nichtnutzung eines Passwortmanagers.



Warum nutzen Sie keinen Passwortmanager?

Basis: Online-Befragung, alle Befragten, die angaben, dass sie Passwortmanager kennen, aber nicht nutzen. (n=285)

Im Vordergrund steht dabei die Sorge, dass ein Hacker an alle Passwörter auf einmal gelangen könnte.



Welche Vorbehalte haben sie gegenüber Passwortmanagern?

Basis: Online-Befragung, alle Befragten, die angaben, dass sie Vorbehalte gegenüber Passwortmanagern haben. (n=192)

Die Teilnehmerinnen und Teilnehmer der Gruppendiskussionen sind misstrauisch gegenüber Passwortmanagern.

- Die Verwendung von Passwort-Safes oder Passwortmanagern stößt auf Skepsis; die Teilnehmer haben Sorge, dass potentielle Angreifer bei einem „Einbruch“ auf dem Rechner mit einem Schlag alle Passwörter stehlen könnten.
- Auch weiß man nicht, wie seriös der Anbieter des Passwortmanagers ist. „Fühlt sich doof an, wenn man das aus der Hand gibt, als hätte ein Fremder den eigenen Schlüsselbund.“ Oder: „Irgendwo im Internet alle meine Passwörter. Das ist doch total unsicher.“
- Auch könnte das Gerät mit den darauf gespeicherten Passwörtern kaputt gehen.
- Im Falle eines Unfalls oder Todes haben Angehörige keinen Zugang zu den Passwörtern.

Basis: Gruppendiskussion

Für am wahrscheinlichsten halten es die Befragten, dass Hacker über Datendiebstähle bei Unternehmen an ihre Passwörter gelangen könnten.

Mittelwerte

2,5	3,0	3,1	3,3
Ein Hacker hat sich über Ihre **Lebensgewohnheiten** und Ihre Freunde erkundigt. Dabei hat er erfahren, dass Ihr Hund Struppi heißt und Sie 1980 geboren wurden. Danach prüft er, ob er mit dem Passwort „Struppi1980“ in Ihr E-Mail-Konto gelangt.	Ein Hacker hat es auf ein wichtiges Konto von Ihnen abgesehen. Er versucht sich bei diesem Konto anzumelden und probiert automatisiert mit einem Computerprogramm **alle möglichen Buchstaben- und Zahlenkombinationen** aus, in der Hoffnung so Ihr Passwort zu erraten.	Ein Hacker schickt Ihnen eine **E-Mail**, in der Sie aufgefordert werden, Ihr Online-Konto zu aktualisieren, da es ansonsten gesperrt wird. In der E-Mail befindet sich ein Link, den Sie **anklicken** und folgen sollen.	Ein Hacker hat sich **verschlüsselte Passwortlisten** im sogenannten Darknet besorgt, die bei einem Datendiebstahl von einem großen Unternehmen erbeutet worden, bei dem auch Sie Kunde sind. Mit einem Computerprogramm versucht er nun diese Passwörter zu entschlüsseln, unter denen sich auch Ihres befindet.

Für wie wahrscheinlich halten Sie es, dass Hacker Sie so angreifen, wie unten beschrieben, um an Ihre Passwörter zu gelangen? (1 = überhaut nicht wahrscheinlich, 5 = sehr wahrscheinlich)

Basis: Online-Befragung, alle Befragten

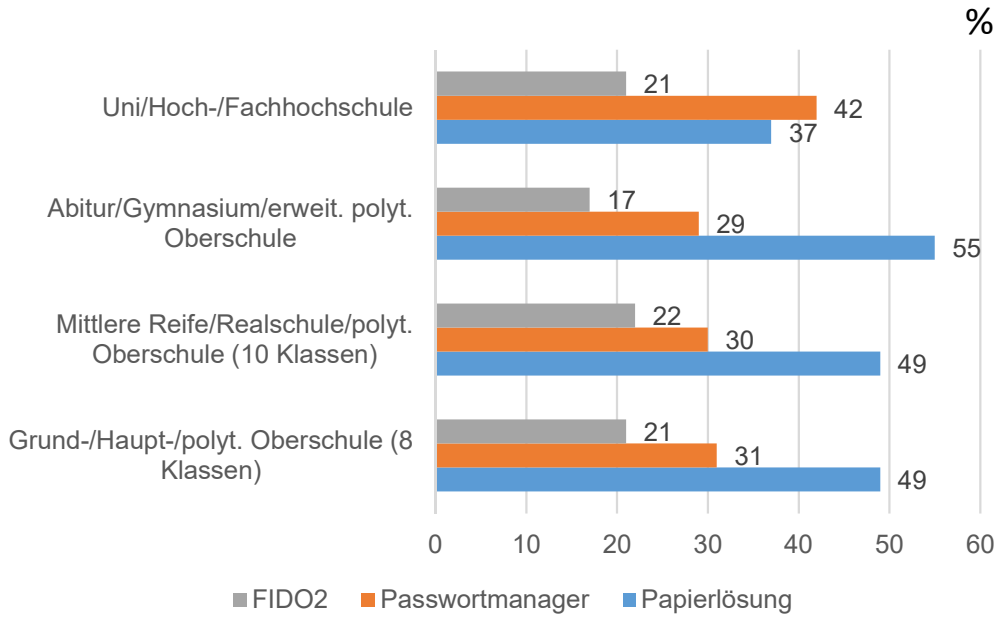
Fast die Hälfte der Befragten würden am liebsten eine sichere Papierlösung für die Verwaltung ihrer Passwörter nutzen.

Papierlösung	Passwortmanager	FIDO2
Sie bilden Passwörter, die aus **zwei Teilen** bestehen. Der erste Teil ist bei jedem Konto **immer gleich**. Diesen Teil behalten Sie ausschließlich im Gedächtnis. Der zweite Teil **unterscheidet sich für jedes Konto**. Als Merkhilfe legen Sie hierfür eine Liste **auf Papier** an. Wenn Sie sich bei einem Konto anmelden, müssen Sie **beide Teile zusammen als ein Passwort eingeben.** Sollte die Liste in fremde Hände gelangen, kann sich niemand damit bei einem Konto anmelden, da er nicht den ersten Teil des Passworts kennt.	Sie verwenden einen **Passwortmanager**. Dieser generiert automatisch sichere Passwörter für Ihre verschiedenen Konten. Diese werden in einer App verschlüsselt auf Ihrem Gerät gespeichert. Sie müssen sich bei einer Anmeldung **nur ein sicheres Passwort** für den Passwortmanager **merken**. Der Passwortmanager meldet sich automatisch bei einem Konto an und prüft gleichzeitig die Identität der Webseite. Dadurch wird die Eingabe von Passwörtern auf gefälschten Webseiten verhindert.	Sie melden sich **ohne Passwort** bei einem Online-Konto an. Der Nachweis Ihrer Identität erfolgt direkt über eine speziell **gesicherte Hardware** im Gerät, das Sie nutzen (Computer, Smartphone) und das Sie für eine Anmeldung autorisiert haben. Da **keine Passwörter mehr** verwendet werden, können diese auch nicht gestohlen werden.
48%	32%	20%

Unten sind drei Möglichkeiten aufgeführt, wie man seine Online-Konten sicherer machen kann. Welche davon würden Sie am ehesten nutzen?

Basis: Online-Befragung, alle Befragten

Im Gegensatz zu den anderen Bildungsgruppen würde diejenige mit der höchsten Bildung am ehesten einen Passwortmanager nutzen.



Unten sind drei Möglichkeiten aufgeführt, wie man seine Online-Konten sicherer machen kann. Welche davon würden Sie am ehesten nutzen?

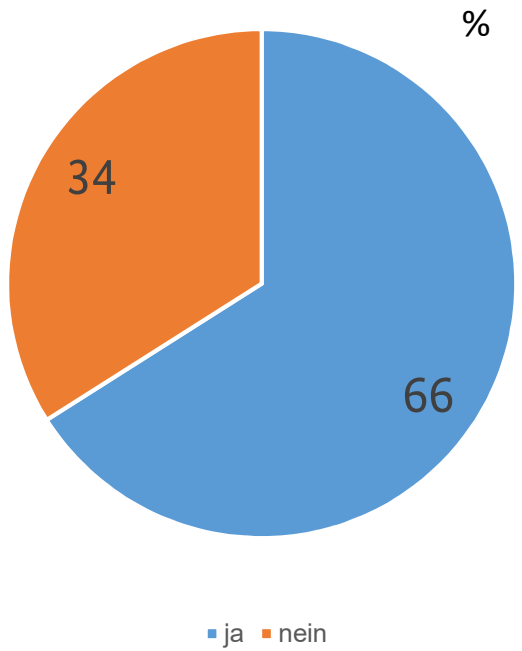
Basis: Online-Befragung, alle Befragten

Die Teilnehmerinnen und Teilnehmer der Gruppendiskussionen erhoffen sich von biometrischen Verfahren eine Erleichterung.

- Die Teilnehmerinnen und Teilnehmer stehen biometrischen Verfahren grundsätzlich aufgeschlossen gegenüber. Sie erhoffen sich dadurch eine Erleichterung beim Management ihrer vielen Online-Konten. „Biometrie ist die Zukunft.“
- Besonders bei Älteren besteht aber auch die Befürchtung, dass durch biometrische Verfahren, die in Zwei- oder Mehrfach-Authentisierungen eingesetzt werden, die Prozesse komplexer und damit aufwendiger werden.
- Es besteht viel Verwirrung, was die einzelnen Sicherheitsverfahren (TAN, Passwort, Code etc.) und die dafür verwendeten Begriffe genau bedeuten; ebenfalls darüber, dass die gleichen Sicherheitsverfahren mit synonymen Begriffen belegt sind.

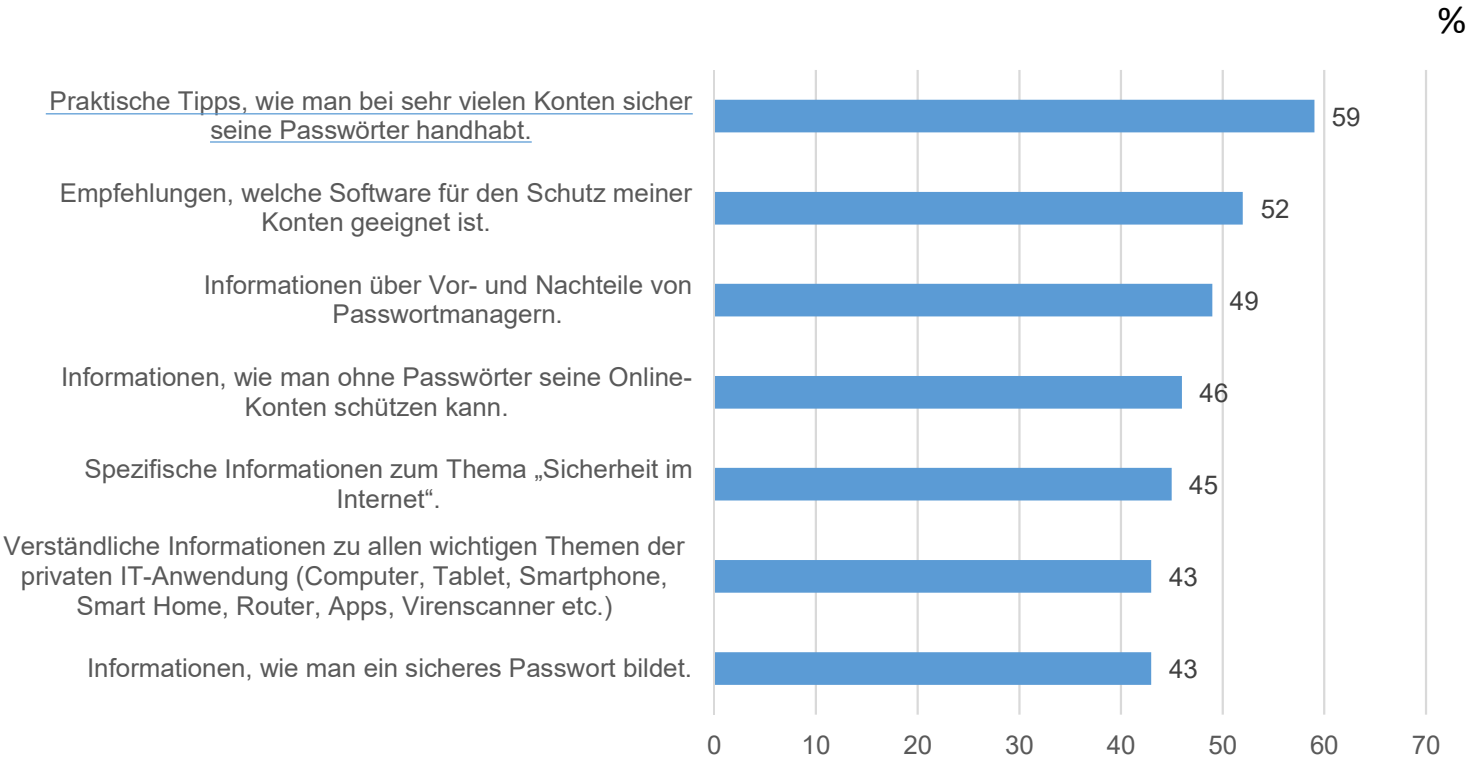
Basis: Gruppendiskussion

Zwei Drittel der Befragten wünschen sich mehr Informationen, wie man sich vor Datendiebstahl schützen kann.



Wünschen Sie sich mehr Informationen, wie Sie sich vor Datendiebstahl schützen können?
Basis: Online-Befragung, alle Befragten

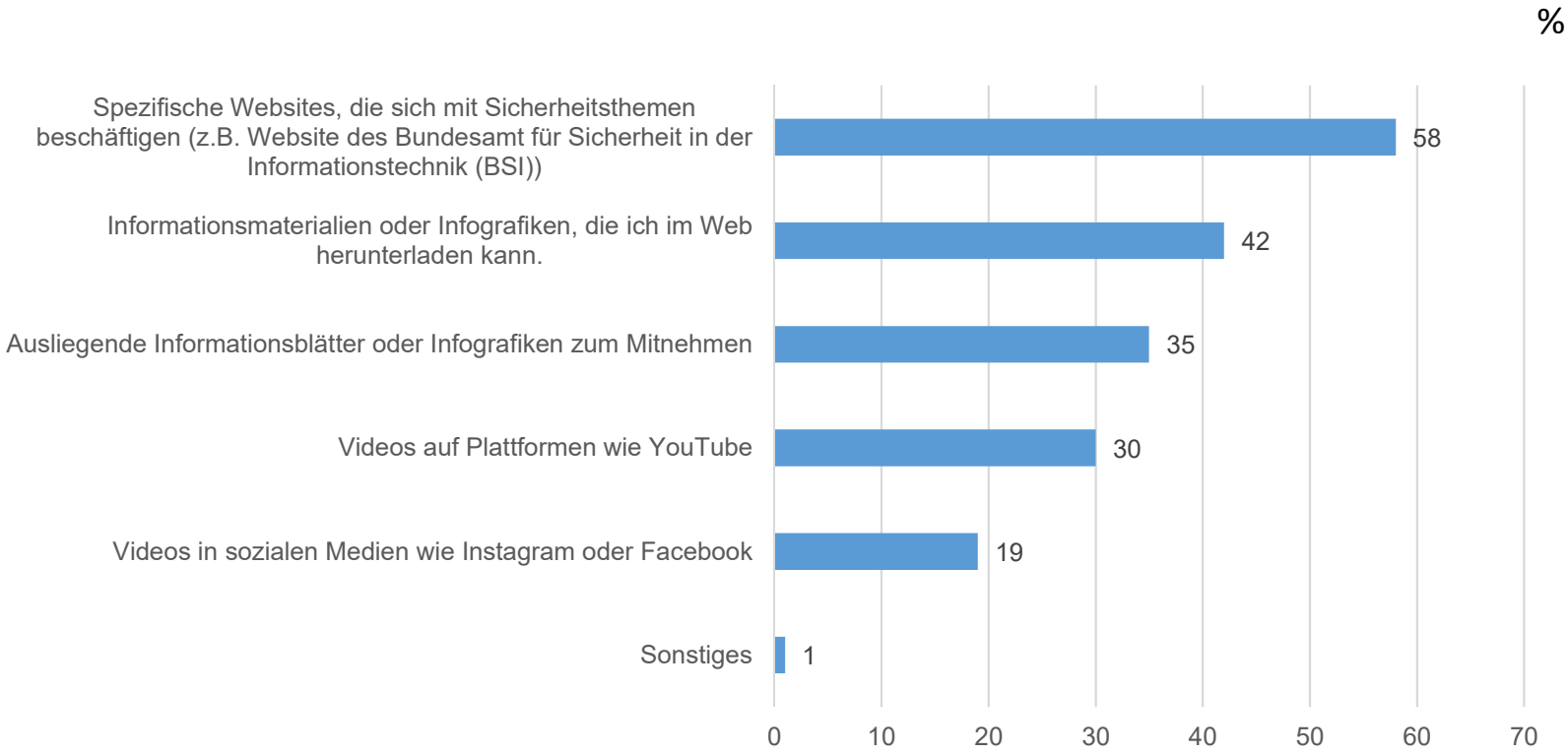
Die Befragten wünschen sich am häufigsten praktische Tipps, wie man viele Online-Konten handhabt.



Welche Informationen wünschen Sie sich? Mehrfachnennungen sind möglich.

Basis: Online-Befragung, alle Befragten, die sich mehr Informationen wünschen. (n=659)

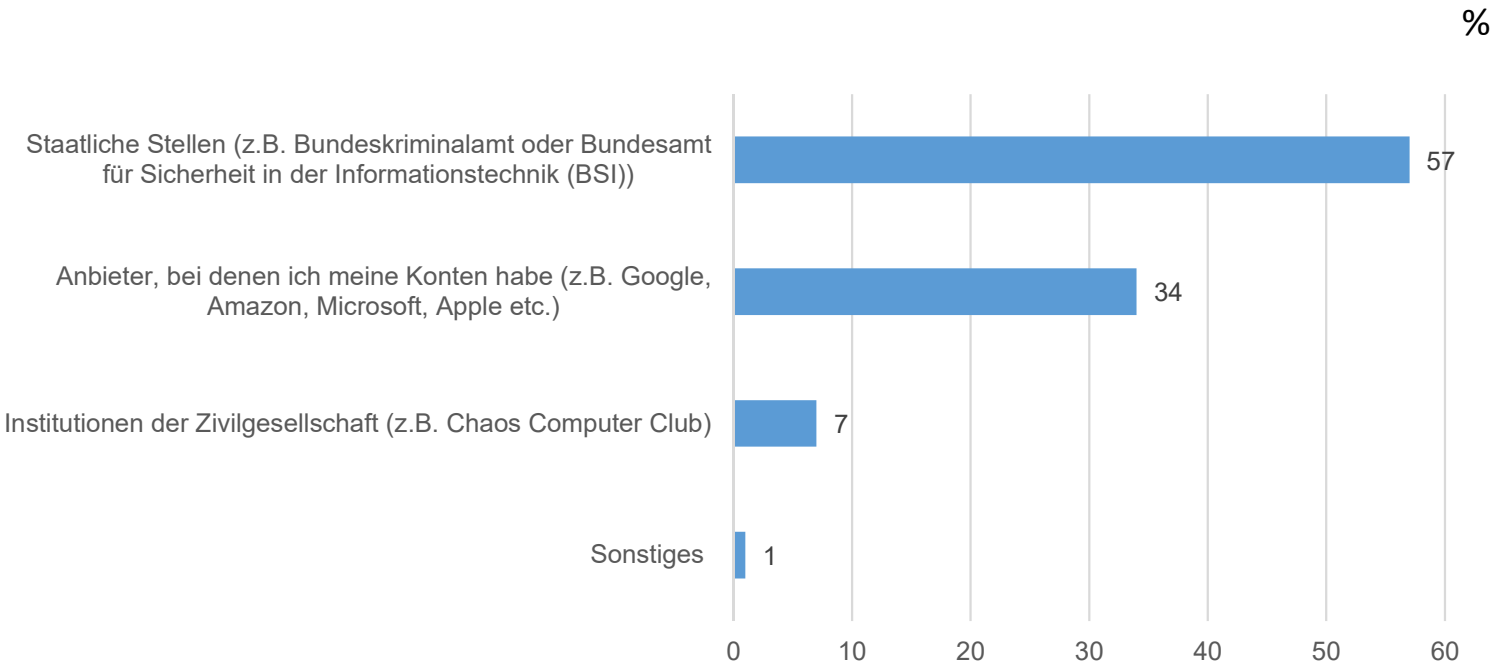
Am häufigsten wünschen sich die Befragten Informationen auf Fachwebsites zu Sicherheitsthemen.



Über welche Kommunikationswege möchten Sie informiert werden? Mehrfachnennungen sind möglich.

Basis: Online-Befragung, alle Befragten, die sich mehr Informationen wünschen. (n=659)

Informationen sollten am ehesten von staatlichen Stellen zur Verfügung gestellt werden.



Von wem wünschen sie sich diese Information am meisten?

Basis: Online-Befragung, alle Befragten, die sich mehr Informationen wünschen. (n=659)

Zusammenfassung der Ergebnisse

Hauptproblem ist die Handhabung vieler Passwörter

- Die Generierung eines sicheren Passwortes wird nicht als Hauptbarriere gesehen, sondern die Anforderung, jeweils ein eigenes sicheres Passwort für sehr viele Online-Konten zu verwenden.
- Über alle Altersgruppen hinweg versuchen die Bürgerinnen und Bürger, sich die Passwörter zu merken oder sie schreiben sie sich auf Papier auf.
- Um Passwörter in verschiedenen Situationen schnell abrufen zu können, werden wegen der begrenzten Gedächtniskapazität anstatt komplexer Passwörter einfach zu merkende Passwörter vergeben.
- Ferner wird die Passworteingabe als Hindernis angesehen, schnell ans (Handlungs-)Ziel zu kommen. „Es muss schnell gehen“.

Misstrauen gegenüber Passwortmanagern

- Die Verwendung von Passwort-Safes oder Passwortmanagern stößt bei vielen auf Skepsis; die Bürgerinnen und Bürger haben Sorge, dass potentielle Angreifer bei einem „Einbruch“ auf dem Rechner oder Smartphone mit einem Schlag alle Passwörter stehlen könnten.
- Im Gegensatz zu den anderen Gruppen sind Personen mit formal höherer Bildung Passwortmanagern gegenüber am aufgeschlossensten; sie sehen hier eine effiziente Lösung für ihr Problem, viele Online-Konten managen zu müssen.

Zusammenfassung der wichtigsten Gründe für die Verwendung leicht zu merkender Passwörter

„Ich habe mehr als fünfzig Accounts. Wie soll ich mir da alle Passwörter merken.“

Begrenzte Merkfähigkeit

„Ich vertraue auf Produkte, Provider und Infos und werde dann doch gehackt.“

Misstrauen in Software

Passwort-verhalten

Angst vor Passwort-diebstahl

„Bei mir liegen die Passwörter in einem Safe.“

Geringe Selbstwirksamkeits-erwartung

„Ein Hacker ist weit voraus.“

Wunsch nach praktischen Lösungen

- Da einerseits das Bedrohungserleben, Opfer eines Datendiebstahls zu werden, nicht stark ausgeprägt ist und anderseits die Überzeugung besteht, dass ein Hacker, falls er es darauf anlegen würde, ohnehin alle Online-Konten hacken könnte, ist für die Bürgerinnen und Bürger in ihrem Alltag Handhabbarkeit wichtiger als Sicherheit.
- Folglich wünschen sich die Bürgerinnen und Bürger am häufigsten praktische Tipps, wie man viele Online-Konten und Passwörter sicher handhaben kann. Diese Informationen sollten auf spezifischen Websites von staatlichen Anbietern zur Verfügung gestellt werden, die Experten für Sicherheitsthemen sind (z.B. BSI).

Literatur 1

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and informatics, 34(7), 1038-1058.

Becker, I., Parkin, S., & Sasse, M. A. (2018). The rewards and costs of stronger passwords in a university. Linking password lifetime to strength. Proceedings of the 27th USENIX security symposium.

Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In Proc. IEEE symposium on security and privacy (S&P). IEEE Computer Society, Washington, DC, USA, 2012, pp. 538–552.

DSiN Sicherheitsindex 2019. Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage der Verbraucher in Deutschland. Berlin.

DIVSI (2018). DIVSI U25-Studie Euphorie war gestern. Die „Generation Internet“ zwischen Glück und Abhängigkeit. Hamburg.

Fahl, S., Harbach, M., Acar, Y., & Smith, M. (2013). On the ecological validity of a password study. In Proc. ninth symposium on usable privacy and security (SOUPS). ACM, New York, NY, USA.

Gehringer, E.F. (2002). Choosing passwords: Security and human factors. Technology and society. International symposium.

Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password authentication from a human factors perspective: Results of a survey among end-users. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 53(6), 459–463.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 383–392). New York: ACM.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security. 10.1016/j.cose.2015.07.002.

Literatur 2

Parkin, S., Driss, S., Krol, K., & Sasse, M. A. (2016). Assessing the User Experience of Password Reset Policies in a University. In: Technology and Practice of Passwords. PASSWORDS 2015. (pp. pp. 21-38). Springer: Cham.

Reuter, C., Kaufhold, M.-A., & Klös, J. (2017). Benutzbare Sicherheit: Usability, Safety and Security bei Passwörtern. In: Burghaedt, M, Wimmer, R., Wolff, C., & Wormser-Hacker, C. (Hrsg.). Mensch und Computer 2017 – Workshopband, 10. – 13. September 2017, Regensburg.

Rin, C., Summers, K., Rhodes, E., Virothaisakun, J., & Chisnell, D. (2015). Password creation strategies across high- and low-literacy web users, Proceedings of the 78th ASIS&T Annual meeting.

Sasse, M. A., & Smith, M. (2016). The Security-Usability Tradeoff Myth. IEEE Security and Privacy , 14 (5) pp. 11-13.

Schmitt, H., Nehren, P., Iacono, L.L., & Gorski, P.L. (2017). Usable Security und Privacy by Design. entwickler.press.

Shay, R., Bauer, L., Christin, N., Cranor, F. L., Forget, A., Komanduri, S., Mazurek, M. L., Melicher, M., Segreti, M. S., & B. Ur, A. (2015). A spoonful of sugar? The impact of guidance and feedback on password-creation behavior. In Proc. 33rd annual ACM conference on human factors in computing systems (CHI). ACM, New York, NY, USA, 2015, pp. 2903–2912.

Stobert, E. (2014). The agony of passwords: Can we learn from user coping strategies? In CHI'14 Extended Abstracts on Human Factors in Computing Systems (pp. 975–980). New York: ACM.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). «I added '!' at the end to make it secure»: Observing password creation in the lab. Symposium on usable privacy and security (SOUPS), 2015, July 22–24, 2015, Ottawa, Canada.

Yan, J., Blackwell, R., Anderson, R. J., & A. Grant (2004). Password memorability and security: empirical results. IEEE security & privacy, 2(5): 25–31, 2004.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2013). Password advice shouldn't be boring: Visualizing password guessing attacks. In Proc. eCRS, 2013.