# AXA Cyber-sorgen-monitor 2025

## Studienbericht

Mai 2025

OTOMO

# IMPRESSUM

AXA Cybersorgenmonitor, Mai 2025

Auftrag: AXA Schweiz

Ausführung: Sotomo, Dolderstrasse 24, 8032 Zürich.

Projektteam: Emma Croci, Elia Heer, Michael Hermann

# AXA Cyber-sorgenmonitor 2025

## 1.1 ZU DIESER STUDIE

Kaum ein Bereich unseres Lebens bleibt heute vom Internet unberührt. Die digitale Transformation hat unseren Alltag grundlegend verändert und in vielerlei Hinsicht vereinfacht. Gleichzeitig bringt sie jedoch immer wieder neue Risiken mit sich – sowohl auf gesellschaftlicher als auch auf persönlicher Ebene. Wie besorgt blickt die Schweizer Bevölkerung auf diese Herausforderungen im Netz? Welche Themen werden als besonders risikobehaftet wahrgenommen? Fühlen sich die Menschen ausreichend informiert darüber, wie sie im Falle eines Cyberdelikts am besten reagieren sollten? Und wie schwierig empfinden es Eltern, ihre Kinder vor den negativen Seiten des Internets zu schützen? Diese und weitere Fragen hat Sotomo für den ersten Cybersorgenmonitor im Auftrag der AXA untersucht.

Die Studie gliedert sich in drei Teile. Der erste Teil analysiert, welche digitalen Herausforderungen die Bevölkerung als besonders relevant einstuft, aber auch wie die Bevölkerung selbst mit dem Internet umgeht. Der zweite Teil ist fokussiert auf zwei Arten von Cyberdelikten – Cyberbetrug und Cyberbelästigung – und untersucht deren Verbreitung sowie die Auswirkungen auf die Betroffenen. Der dritte Teil beleuchtet die Wahrnehmung der Chancen und Risiken der Internetnutzung durch Kinder

und zeigt auf, wie sicher sich Eltern im Umgang mit diesem Thema fühlen und wo Massnahmen gesetzt werden.

## 1.2 WICHTIGSTE ERGEBNISSE IN KÜRZE

Schweizer Bevölkerung sorgt sich um die Sicherheit im digitalen Raum

Ein grosser Teil der Schweizer Bevölkerung sorgt sich um Cyberkriminalität und die Sicherheit im Netz (Abb. 1). 78 Prozent schätzen die Herausforderung für die Schweiz beim Thema digitale Sicherheit und Cyberkriminalität als erheblich ein. Damit bereitet Cyberkriminalität den Schweizer:innen ebenso häufig Sorgen wie beispielsweise der Wohnungsmarkt. Besonders starkes Kopfzerbrechen bereiten der Bevölkerung Cyberangriffe auf kritische Infrastrukturen (47%), Cyberbetrüge (44%) sowie eine Beeinflussung der öffentlichen Meinung durch Fake-Profile oder Desinformation (44%)(Abb. 3).

Verbreiteter Wunsch nach weniger Zeit an den privaten digitalen Geräten

Mehr als zwei Drittel der Befragten (71%) stufen den allgemeinen Umgang der Bevölkerung mit dem Internet als zu risikoreich ein. Gleichzeitig bewerten über die Hälfte der Befragten ihren eigenen Umgang als angemessen (55%) oder sogar als (eher) zu vorsichtig (27%) (Abb. 7). Doch viele haben den Eindruck, das Smartphone würde Überhand über das eigene Leben gewinnen. Fast die Hälfte der Befragten (46%) gibt an, sie würde eigentlich gerne weniger Zeit an privaten digitalen Geräten verbringen (Abb. 12). Angesichts der Herausforderung zunehmender Bildschirmzeit, des Suchtpotenzials mancher Apps sowie datenschutzrechtlicher Bedenken wird immer wieder ein Verbot der Social-Media-App TikTok diskutiert. Ein solches Verbot stösst in der Bevölkerung auf Zuspruch, fast die Hälfte der Befragten befürwortet ein Tiktok-Verbot (48%) (Abb. 14).

## Ein Achtel hat in den letzten fünf Jahren Geld bei einem Cyberbetrug verloren

Rund zwölf Prozent haben in den letzten fünf Jahren einen Cyberbetrug mit finanziellen Folgen erlebt (Abb. 19). Davon erlitten zwei Drittel (8%) einen Verlust von weniger als 1000 Franken und ein Drittel (4%) einen hohen finanziellen Verlust von über 1000 Franken. Viele der Betroffenen hat der Betrug emotional belastet – besonders bei einem hohen finanziellen Verlust. Von den Opfern eines Betrugs mit mehr als 1000 Franken Schaden berichten 76 Prozent von einer hohen oder eher hohen emotionalen Belastung als Folge (Abb. 21).

## Selbst schwere Fälle von Cyberbelästigungen werden kaum der Polizei angezeigt

14 Prozent der Bevölkerung sind schon einmal im digitalen Raum belästigt worden. Das heisst, sie haben auf einer Online-Plattform bereits gezielte Beleidigungen, Belästigungen oder Bedrängungen erlebt. Dazu gehören beispielsweise Cybermobbing, Hassrede oder sexuelle Belästigung (Abb. 26). Gut die Hälfte von ihnen berichtet davon, dass sie dies emotional belastet hat (Abb. 29). Doch selbst von den Personen, die Opfer einer emotional belastenden Cyberbelästigung geworden sind haben nur 23 Prozent den Vorfall der Polizei gemeldet (Abb. 30).

## Klare Mehrheiten für Handyverbot an Schulen und Verbot von Social Media für Kinder unter 16

In der Bevölkerung gibt es einen weit verbreiteten Wunsch, Kinder besser vor den Risiken privater digitaler Geräte zu schützen. Als grösste Herausforderung wird hierbei, sowohl von Eltern als auch von der allgemeinen Bevölkerung, Cybermobbing genannt (Abb. 33). Mögliche Regelungen wie ein generelles Handyverbot an Schulen befürworten 81 Prozent der Befragten und 80 Prozent sprechen sich dafür aus, Social-Media-Plattformen für Kinder unter 16 Jahren zu verbieten (Abb. 36).

## Die digitale Sicherheit von Kindern überfordert viele Eltern

38 Prozent der Eltern von Kindern zwischen 6 und 17 Jahren fühlen sich klar oder eher nicht in der Lage, ihre Kinder ausrei-

chend vor Cyberrisiken zu schützen (Abb. 38). 51 Prozent fällt es schwer, Massnahmen zur sicheren Nutzung des Internets (z.B. ein Verbot gewisser Online-Plattformen) bei ihren Kindern umzusetzen. Ausserdem berichten 52 Prozent der Befragten mit Kindern, es gebe bei ihnen zuhause Konflikte über die Dauer der Bildschirmzeit (Abb. 40). Dies zeigt, dass Eltern beim Schutz ihrer Kinder im digitalen Raum nicht nur Massnahmen ergreifen, sondern dabei auch an Grenzen stossen.

# Herausforderungen in der digitalen Welt

Die digitale Welt ist ein fester Bestandteil unseres alltäglichen Lebens. Die Möglichkeiten, die sich durch den digitalen Wandel bieten, sind jedoch noch neu und entwickeln sich stetig weiter – ebenso wie die damit verbundenen Risiken. Dieses Kapitel untersucht, wie die Bevölkerung auf Herausforderungen im Netz blickt und welchen Stellenwert sie diesen für sich selbst und für die Schweiz beimisst. Zusätzlich wird untersucht, welchen Aktivitäten Befragte im Internet nachgehen und wie sie ihre eigene Bildschirmzeit wahrnehmen.

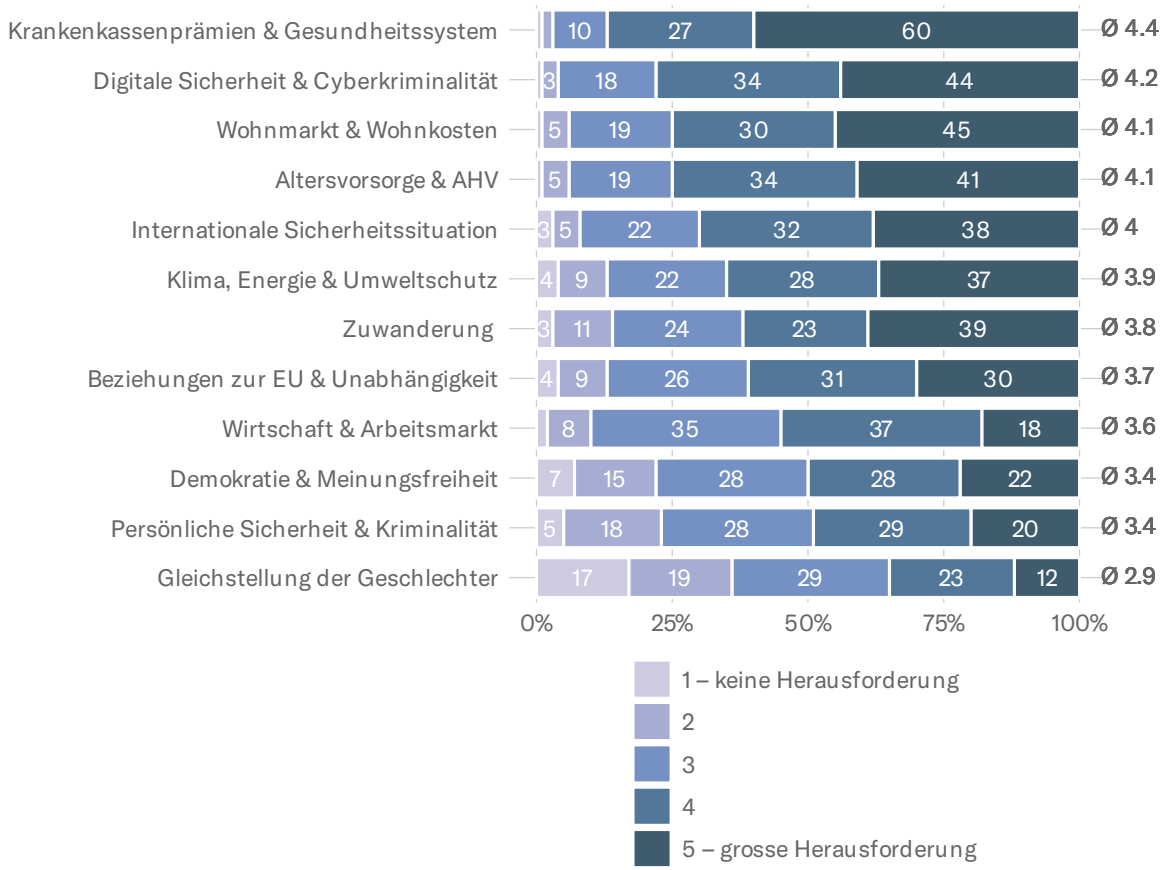
## 2.1 CYBERDELIKTE ALS UNIVERSELLE HERAUSFORDERUNG

Eine Fülle an Tätigkeiten kann heute online erledigt werden. Neben neuen Errungenschaften und Möglichkeiten bringt die digitale Transformation auch erhebliche Herausforderungen mit sich – ein Aspekt, den die Bevölkerung deutlich wahrnimmt (Abb. 1). Konkret sind rund drei Viertel der Befragten der Meinung, dass Themen rund um Cybersicherheit und Cyberkriminalität eine erhebliche Herausforderung darstellen, sprich

eine 4 oder 5 auf einer Skala von 1 (keine Herausforderung) bis 5 (grosse Herausforderung) sind. Cyberkriminalität wird also beinahe einhellig als erhebliche Herausforderung für die Schweiz eingestuft – lediglich Schwierigkeiten im Gesundheitssystem werden von einem höheren Anteil der Befragten als eine erhebliche Herausforderung wahrgenommen.

Herausforderungen für die Schweiz (Abb. 1)

«Wie gross schätzen Sie die Herausforderungen für die Schweiz bei den folgenden Themen ein?»

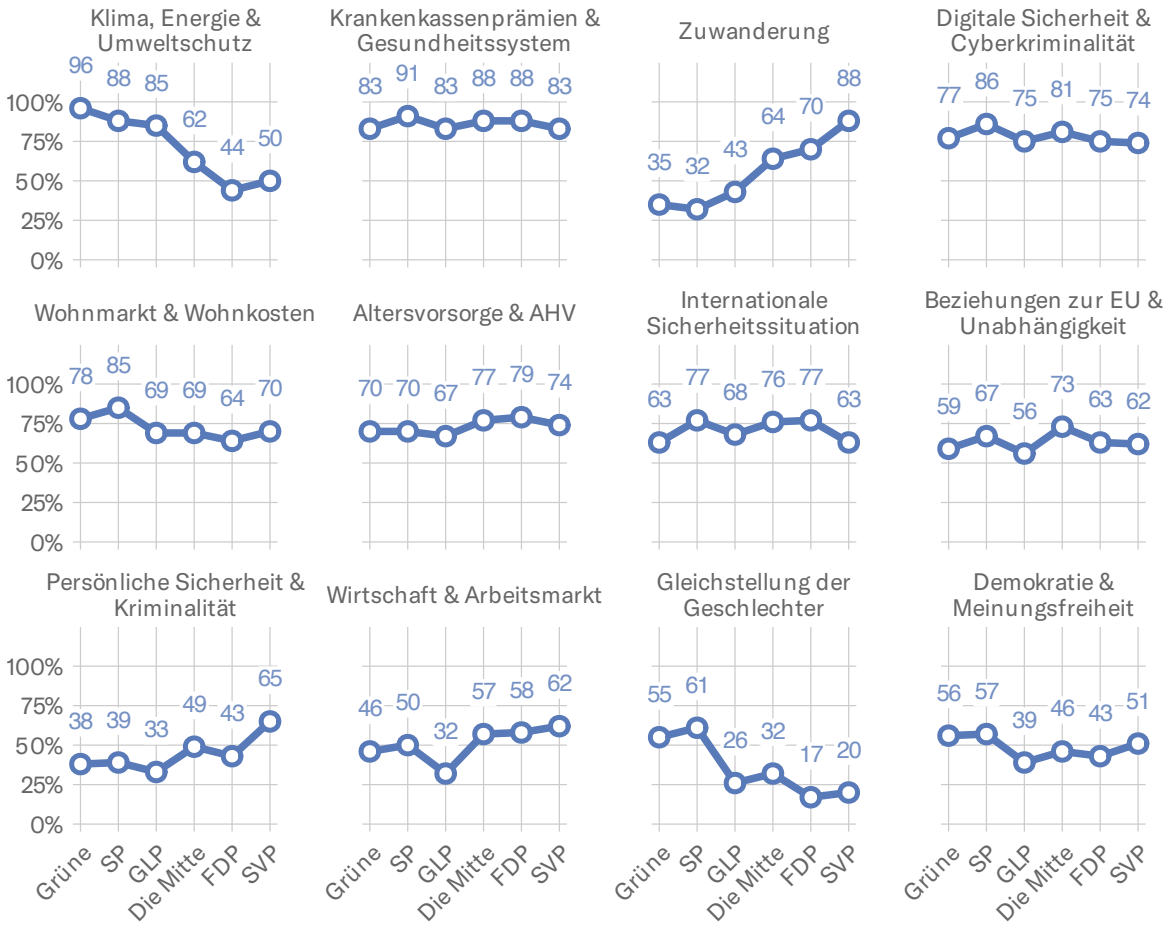



Ein Grund, weshalb der Bereich «Cyberkriminalität und Digitale Sicherheit» so weit vorne rangiert, dürfte sein, dass dieser von der breiten Bevölkerung – unabhängig von der politischen Einstellung – als Herausforderung angesehen wird. Das Thema wird nicht einseitig von einer Partei politisiert, sondern vielmehr verbindet die geteilte Sorge die politischen Lager, wie die Abbildung 2 verdeutlicht. So findet über alle Parteigrenzen hinweg ei-

ne grosse Mehrheit der Befragten, dass digitale Sicherheit eine Herausforderung für die Schweiz ist.

Herausforderungen für die Schweiz – nach Partei (Abb. 2)

«Wie gross schätzen Sie die Herausforderungen für die Schweiz bei den folgenden Themen ein? – Nur 4 und 5 auf einer Skala von 1 bis 5 zusammengefasst aufgeschlüsselt.»

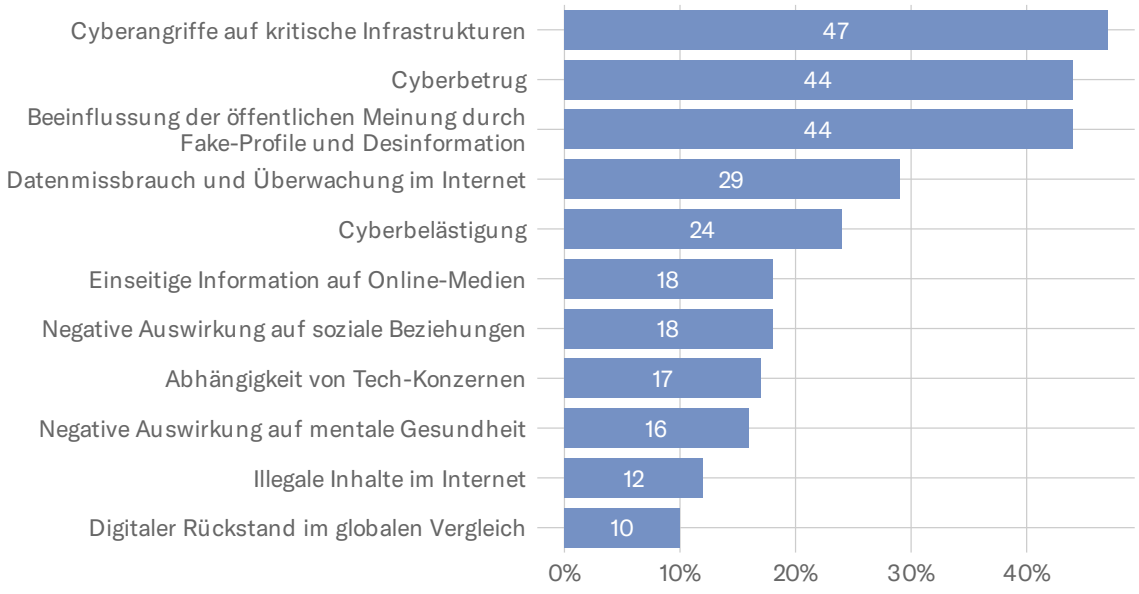



Im Vergleich dazu zeigen sich bei der Problemstellung von anderen Themenbereichen klar die Parteilinien. Grüne schätzen Klimaschutz deutlich häufiger als erhebliche Herausforderung ein als die Anhängerschaft der SVP (Grüne 96%; SVP 50%). Ein ähnliches aber umgekehrtes Bild zeigt sich auch bei der Zuwanderung. Bei Cyberkriminalität sind Parteiunterschiede hingegen kaum erkennbar: sowohl Grüne als auch SVP nehmen diesen Themenbereich ähnlich häufig als grosse Herausforderung wahr (Grüne 77%; SVP 74%).

Abbildung 3 gibt Aufschluss darüber, welche Aspekte der digitalen Welt die Bevölkerung besonders beschäftigt. Am meisten Menschen sorgen sich vor Cyberangriffen auf kritische Infrastrukturen (47%), Cyberbetrug (44%) und der Beeinflussung der öffentlichen Meinung durch Desinformation oder Fake-Profile (44%).

Herausforderungen in der digitalen Welt (Abb. 3)

«Was sind Ihrer Meinung nach in der Schweiz aktuell die grössten Herausforderungen im Zusammenhang mit der digitalen Welt und dem Internet?» – Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.



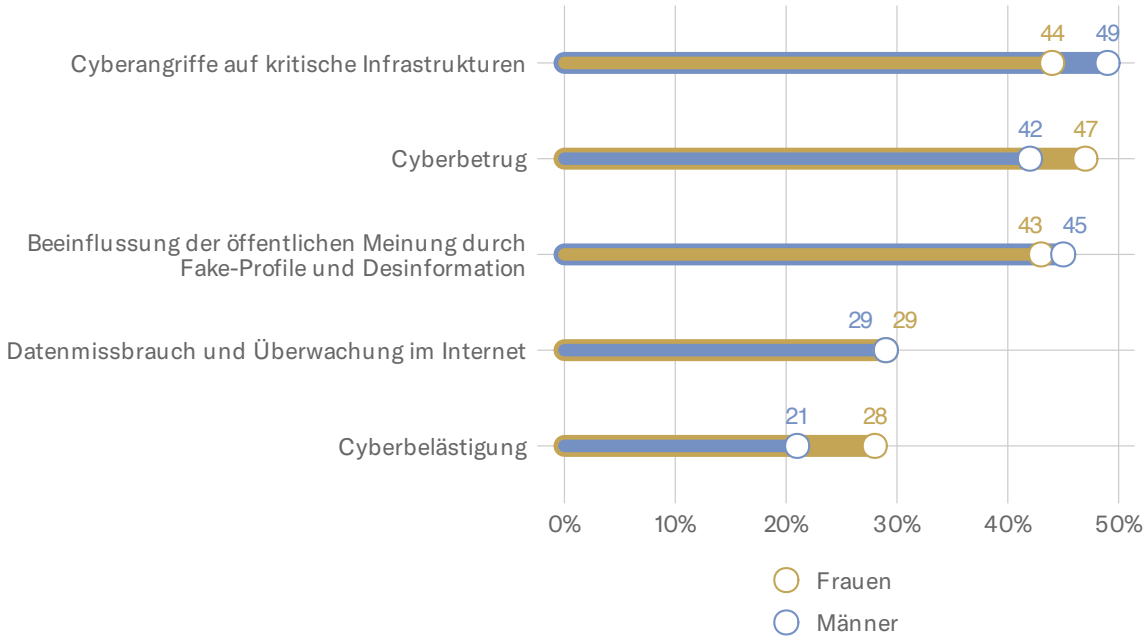
# Die meisten Menschen in der Schweiz sehen Cyberkriminalität als erhebliche Herausforderung.

Die meistgenannten Herausforderungen im Zusammenhang mit Cyberkriminalität betreffen damit sowohl Einzelpersonen als auch die Gesellschaft als Ganzes. Während Angriffe auf kritische Infrastrukturen und manipulative Desinformation primär den gesamtgesellschaftlichen Rahmen betreffen, stehen mit Cyberbetrug und Überwachung im Internet auch individuelle Risiken im Fokus der Sorgen der Schweizer Bevölkerung. Weniger Sorgen bereiten den Befragten hingegen die negativen Auswirkungen der Nutzung digitaler Geräte auf das Sozialleben (18%) oder die technologische Abhängigkeit von ausländischen Techkonzernen (17%). Auch die negativen Auswirkungen digitaler Geräte auf die mentale Gesundheit besorgen nur einen geringen Anteil (16%).

Die Einschätzungen zu digitalen Risiken variiert je nach Bevölkerungsgruppe. Abbildung 4 zeigt, dass sich Frauen im Vergleich zu Männern etwas häufiger um Cyberrisiken sorgen, die Einzelpersonen direkt betreffen. Auffällig ist insbesondere die verbreitetere Besorgnis bezüglich Cyberbelästigung: 28 Prozent der Frauen sehen hierin eine der grössten Herausforderungen, im Vergleich zu 21 Prozent der Männer. Männer schätzen hingegen Cyberangriffe auf kritische Infrastrukturen etwas häufiger als grösste Herausforderung ein als Frauen (Männer 49%; Frauen 44%).

Herausforderungen in der digitalen Welt – nach Geschlecht (Abb. 4)

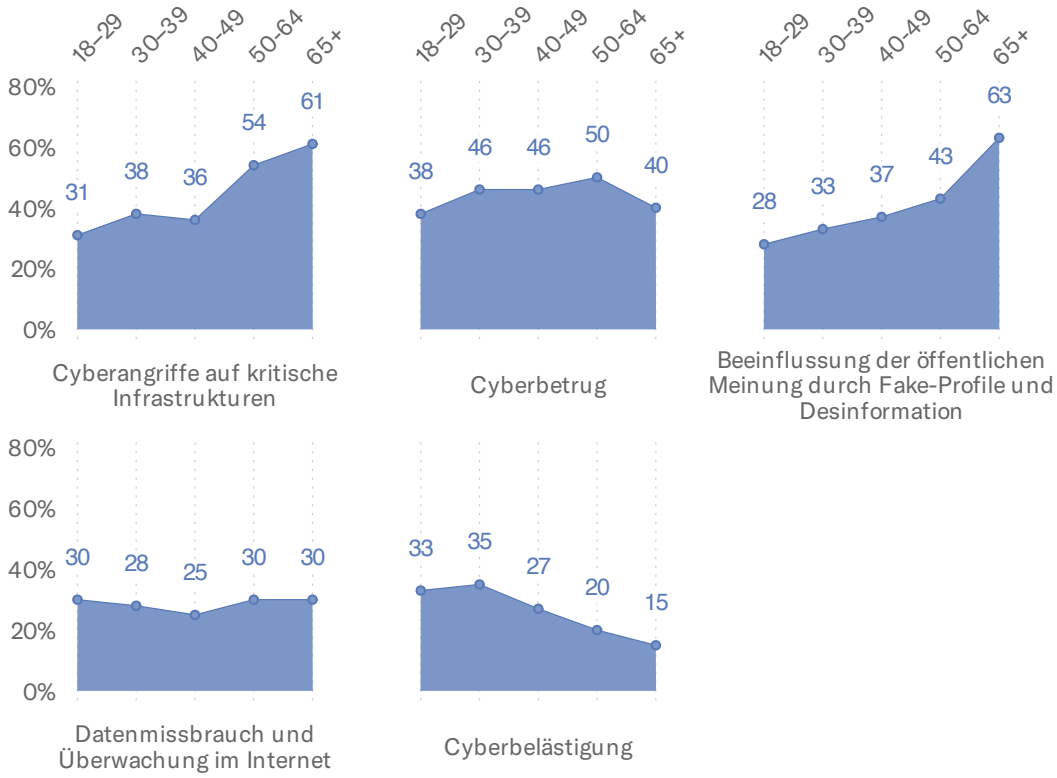
«Was sind Ihrer Meinung nach in der Schweiz aktuell die grössten Herausforderungen im Zusammenhang mit der digitalen Welt und dem Internet?» – Abgebildet sind nur die fünf meistgenannten Herausforderungen. Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.




Auch zwischen den Altersgruppen zeigen sich deutliche Unterschiede: jüngere Generationen (18–29 Jahre) schätzen vergleichsweise weniger Themen als grosse Herausforderungen ein. Unter den 18–29-Jährigen beschäftigen die Themen Cyberbetrug (38%) sowie Cyberbelästigung (33%) besonders. Nur 30–39-Jährige nehmen Cyberbelästigung noch etwas häufiger als eine der grössten Herausforderungen wahr (35%). Ältere Personen sind dagegen häufiger besorgt über Cyberangriffe auf kritische Infrastrukturen (61%) sowie die Beeinflussung der öffentlichen Meinung durch Fake-Profile und Desinformation (63%) (Abb. 5).

Herausforderungen in der digitalen Welt – nach Alter (Abb. 5)

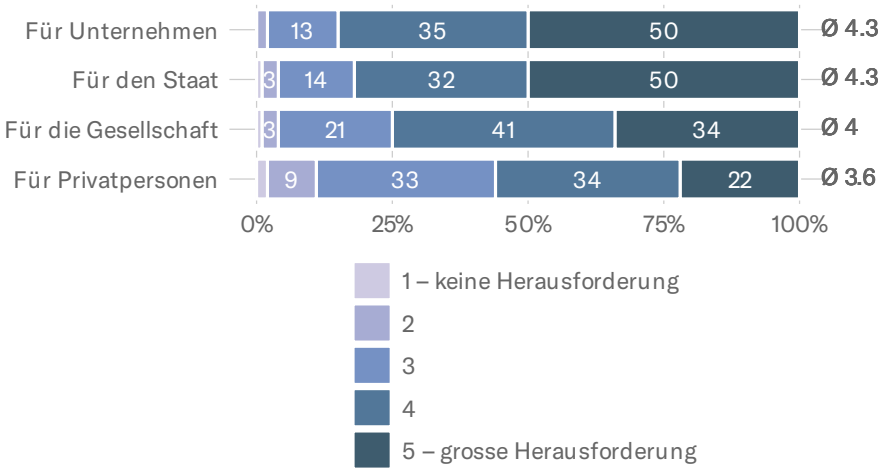
«Was sind Ihrer Meinung nach in der Schweiz aktuell die grössten Herausforderungen im Zusammenhang mit der digitalen Welt und dem Internet?» – Abgebildet sind nur die fünf meistgenannten Herausforderungen. Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.




Die Bevölkerung schätzt die Herausforderungen von Cyberdelikten für Unternehmen als besonders hoch ein (Abb. 6). 85 Prozent schätzen die Herausforderung als 4 oder 5 auf einer Skala von 1 (keine Herausforderung) bis 5 (grosse Herausforderung) ein. Auch für den Staat wird die Herausforderung als gross angesehen (82%). Drei Viertel schätzen die Herausforderung für die gesamte Gesellschaft als erheblich ein. Für Privatpersonen wird das Thema etwas weniger oft als problematisch eingestuft. Trotzdem sieht gut die Hälfte der Befragten Cyberdelikte als bedeutende Herausforderung für Individuen (56%).

Herausforderung Cyberdelikte für verschiedene Akteure (Abb. 6)

«Wie hoch schätzen Sie die Herausforderung von Cyberdelikten für die folgenden Akteure ein?»

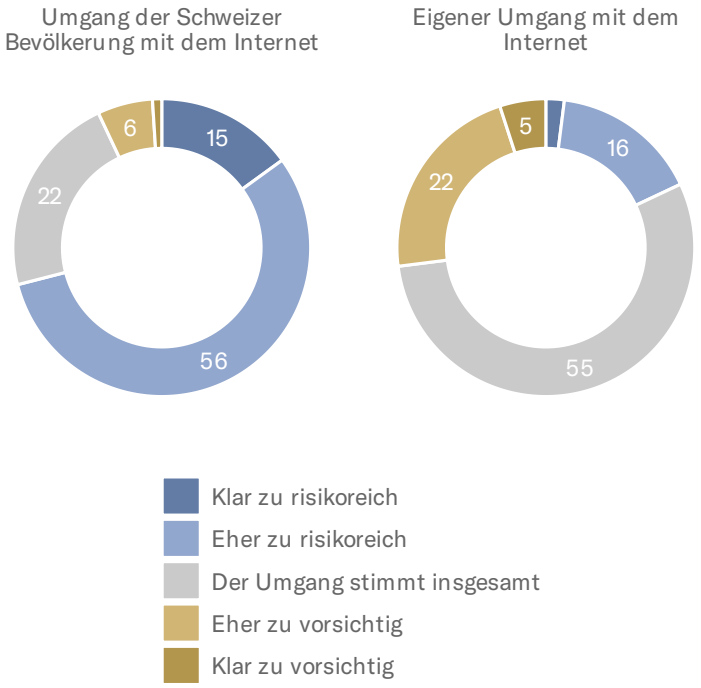



Angesichts der starken Wahrnehmung von Herausforderungen in der digitalen Welt, stellt sich die Frage, wie sicher die Schweizer Bevölkerung ihren eigenen Internetumgang einschätzt (Abb. 7). Interessanterweise schätzen die Befragten ihr eigenes Verhalten im Netz mehrheitlich als sicher ein, während sie umgekehrt dem Rest der Bevölkerung einen zu risikofreudigen Umgang attestieren. Rund die Hälfte der Befragten (55%) sind der Ansicht, dass sie selbst einen angemessenen Umgang mit Online-Risiken in Bezug auf den Schutz vor Cyberdelikten pflegen. 18 Prozent schätzen den eigenen Umgang als klar oder eher zu risikoreich ein. 27 Prozent finden, sie seien zu vorsichtig im Internet unterwegs.

# 71 Prozent attestieren der Bevölkerung einen leichtsinnigen Umgang mit dem Internet.

Online-Sicherheitseinschätzung - Einschätzung der Bevölkerung und Selbsteinschätzung (Abb. 7)

«Wie schätzen Sie insgesamt das Verhalten der Schweizer Bevölkerung bei ihren Online-Aktivitäten ein, in Bezug auf den Schutz vor Cyberdelikten?»

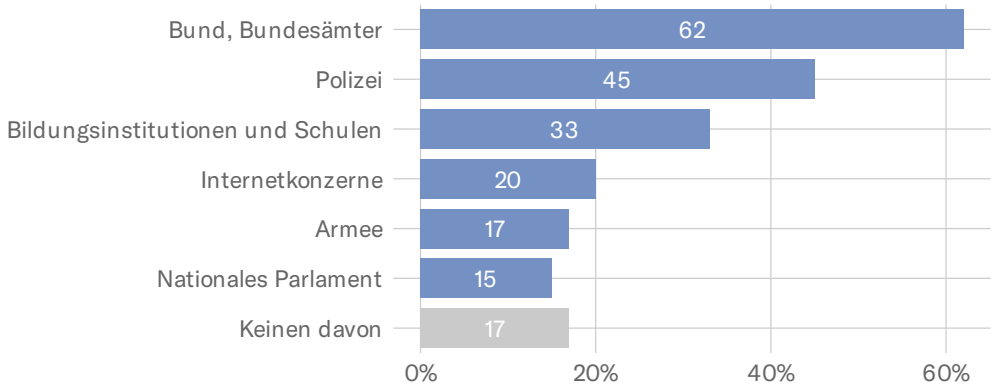



Gleichzeitig glauben 71 Prozent, dass die Schweizer Bevölkerung insgesamt klar oder eher zu leichtsinnig mit Cybergefahren umgeht. Das Vertrauen der Schweizer Bevölkerung in ihre Mitbürgerinnen und Mitbürger ist bei diesem Thema also eher gering.

Dafür ist das Vertrauen in den Bund und in die zuständigen Bundesämter, wie das Bundesamt für Cybersicherheit, hoch (Abb. 8). Zwei Drittel trauen dem Bund zu, den Schutz der Bevölkerung vor Cyberdelikten zu verbessern.

Vertrauen in Akteure für Cyberschutz (Abb. 8)

«Welchen Akteuren trauen Sie zu, den Schutz der Schweizer Bevölkerung vor Cyberdelikten zu verbessern?» – Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.




Am anderen Ende des Vertrauensspektrums steht das nationale Parlament. Nur 15 Prozent trauen National- und Ständerat zu, den Schutz vor Cyberdelikten zu verbessern. Erstaunlicherweise glaubt ein Sechstel der Befragten, dass der Schutz vor Cyberdelikten von keinem der genannten Akteure verbessert werden kann (17%).

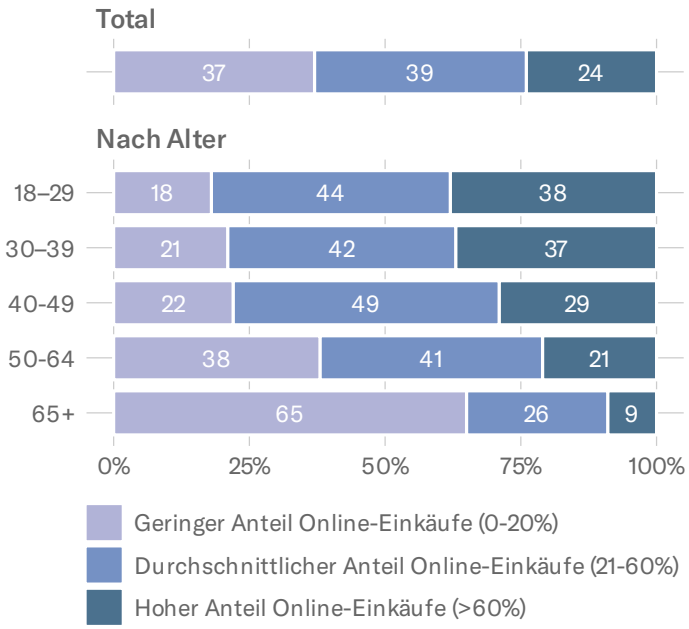
## 2.2 DIE SCHWEIZER BEVÖLKERUNG: VERNETZT UND (ZU) VIEL ONLINE

Mehr und mehr alltägliche Tätigkeiten können mittlerweile problemlos über das Internet erledigt werden – und das nutzt die Schweizer Bevölkerung. So zeigt zum Beispiel die Abbildung 9, dass ein Viertel aller Befragten über 60 Prozent ihrer Non-Food-Einkäufe online einkauft. Jüngere Personen kaufen tendenziell noch häufiger über Websites ein als ältere. Über die Hälfte der Personen im Alter zwischen 50 und 64 Jahren tätigt mehr als 20 Prozent ihrer Non-Food-Einkäufe online. Ab dem Rentenalter nimmt dieser Anteil jedoch stark ab. Rund zwei Drittel der über 64-Jährigen kauft nur einen geringen Anteil ihrer Anschaffungen online ein. Dies könnte daran liegen, dass im Alter viele Personen bereits ihre gefestigten Gewohnheiten haben, die sie

nur ungern ändern. Die jüngeren Generationen sind bereits mit der Möglichkeit von Online-Shopping aufgewachsen, wohingegen für ältere Generationen, dies eher eine neuere Möglichkeit des Einkaufens darstellt.

Online-Einkaufsanteil (Abb. 9)

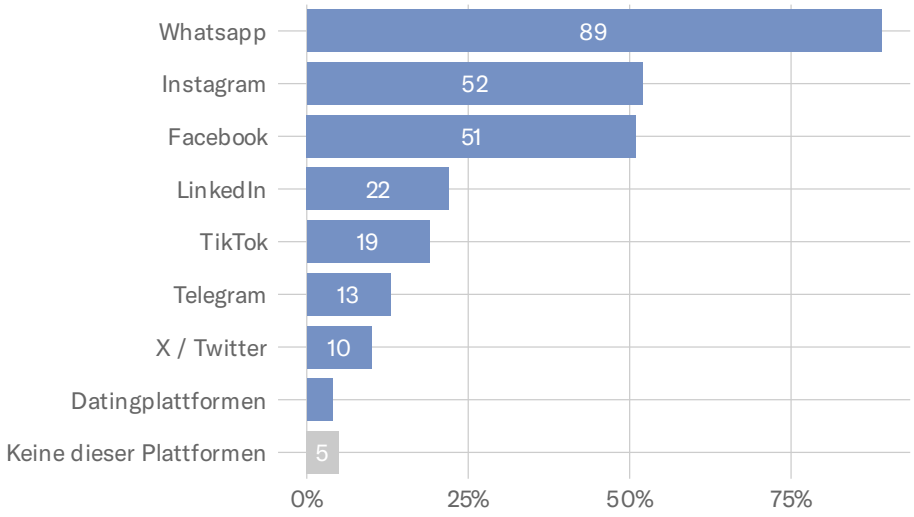
«Was schätzen Sie, wie gross ist ungefähr der Anteil an Einkäufen (Kleider, Elektronik, Hobbyprodukte, etc.), den Sie online tätigen?» (Anteil ohne Lebensmitteleinkäufe angeben)




Auch sozialer Kontakt findet heute vermehrt online statt. Die am häufigsten genutzte Social-Media-Applikation der Schweizer Bevölkerung ist mit Abstand der Messengerdienst Whatsapp. Rund 90 Prozent benutzen Whatsapp mindestens einmal pro Woche. Das von den Befragten am zweithäufigsten genutzte Soziale Medium ist Instagram, jedoch mit einem nennenswerten Abstand zu Whatsapp: Nur knapp die Hälfte nutzen diese App mindestens einmal in der Woche. Dies gilt auch für Facebook. Die restlichen Sozialen Medien werden jeweils nur von einem Fünftel verwendet. Ein kleiner Anteil von fünf Prozent gibt zudem an, keine dieser Sozialen Medien zu nutzen.

Nutzung sozialer Medien (Abb. 10)

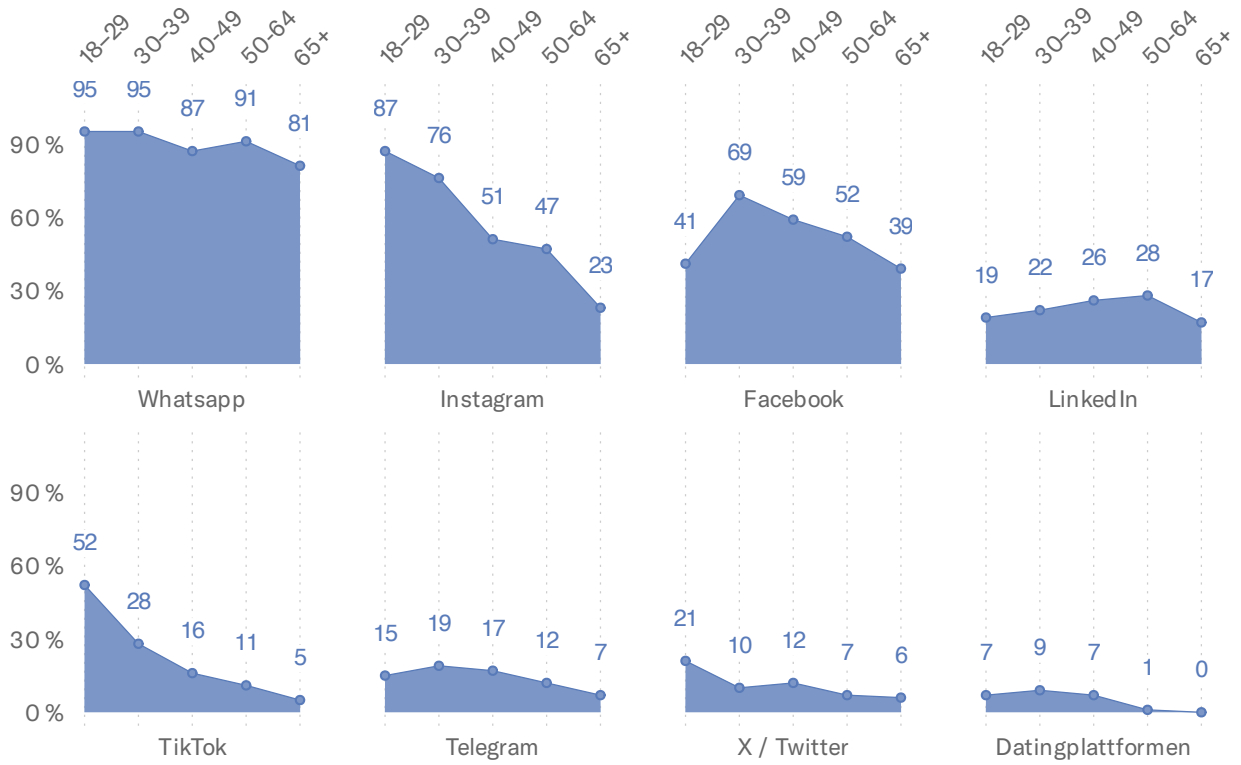
«Welche der folgenden Sozialen Medien nutzen Sie selbst mindestens einmal pro Woche?»




Ein genauerer Blick auf die Nutzung von Sozialen Medien nach Alter zeigt, dass WhatsApp auch die einzige Applikation ist, die von allen Altersgruppen gleichstark verwendet wird (Abb. 11). Bei steigendem Alter werden die verschiedenen Sozialen Medien sichtlich weniger genutzt: Personen über 65 Jahren nutzen kaum Instagram, Facebook und Co. Instagram wird vor allem von den jüngeren Altersgruppen genutzt (87% der 18-29-jährigen; 76% der 30-39-jährigen). Auch Tiktok wird von über der Hälfte der 18-29-Jährigen genutzt, hingegen kaum oder nur selten von Befragten über 50 Jahren. Es zeigen sich also jeweils Nischennutzungen von bestimmten Alterskategorien. Jüngere Generationen benutzen neuere Soziale Medien, wie Instagram und Tiktok häufiger. Hingegen ist Facebook, das bereits 2004 gegründet wurde, mit 69 Prozent am stärksten unter 30-39-Jährigen verbreitet.

Nutzung sozialer Medien – nach Alter (Abb. 11)

«Welche der folgenden Sozialen Medien nutzen Sie selbst mindestens einmal pro Woche?»



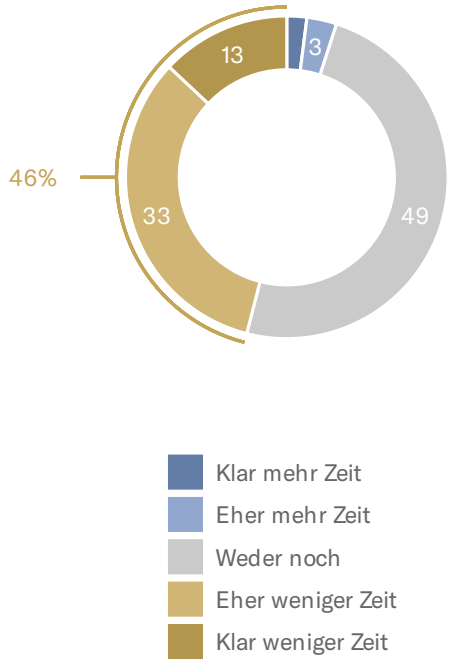

Die Schweizer Bevölkerung ist vernetzt und bewegt sich generell oft im Netz. Ob Nachrichten verschicken oder einkaufen, fast alles kann heute online erledigt werden und die Ergebnisse zeigen: viele tun dies auch. Im Zusammenhang mit einer Verlagerung von alltäglichen Handlungen ins Internet, stellt sich jedoch die Frage, wie die Menschen selbst das Dauer-Online-Sein wahrnehmen. Die Möglichkeiten, mit denen man am Handy und Co. Zeit verbringen kann, sind endlos. Doch nicht alle empfinden die damit verbrachte Zeit als ideal.

# Schweizer:innen wollen weniger Zeit an digitalen Geräten verbringen.

Die Abbildung 12 zeigt, dass rund die Hälfte der Befragten (49%) mit ihrer aktuellen Bildschirmzeit zufrieden ist. Hingegen finden 46 Prozent der Befragten, dass sie lieber weniger Zeit auf ihren digitalen Geräten verbringen möchten. Umgekehrt gibt kaum jemand an, er oder sie wünschte sich, mehr Zeit an digitalen Geräten verbringen zu können.

Bildschirmzeit (Abb. 12)

«Würden Sie gerne mehr oder weniger Zeit an Ihren privaten digitalen Geräten verbringen?»

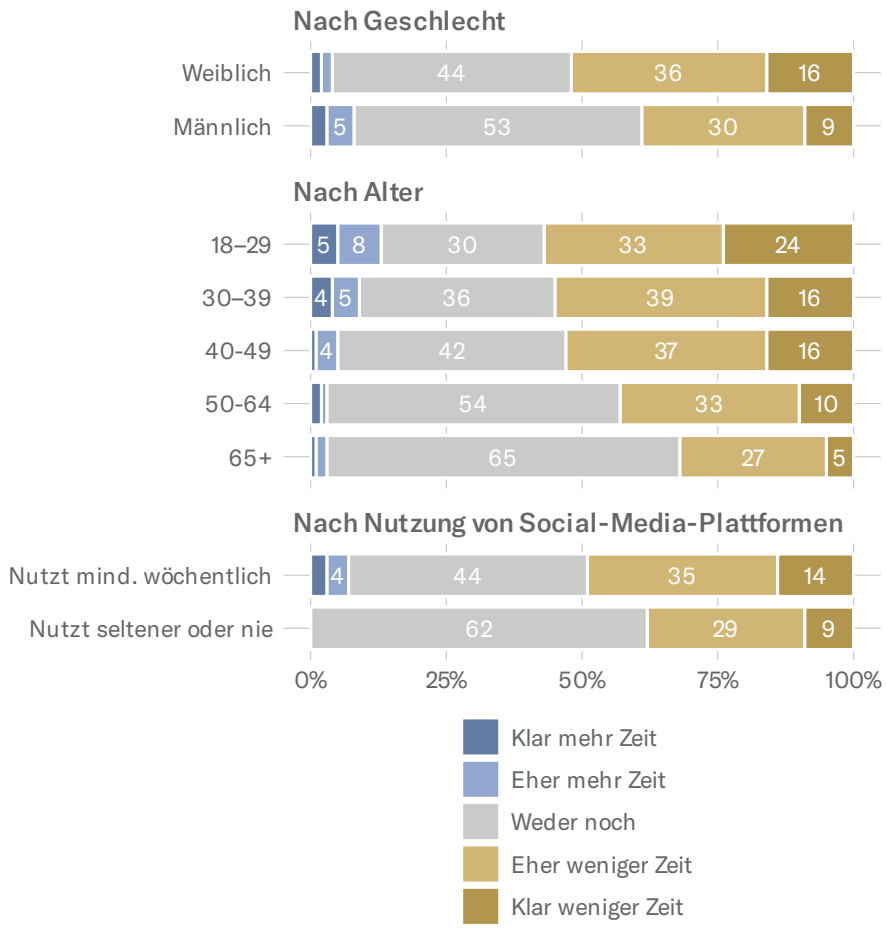



Dass beinahe die Hälfte angibt, lieber weniger Zeit an digitalen Geräten verbringen zu wollen, zeigt deutlich: Für einen beträchtlichen Teil der Bevölkerung nehmen digitale Geräte einen zu grossen Raum im Alltag ein.

Wie Abbildung 13 zeigt, wollen insbesondere viele jüngere Menschen weniger Zeit an ihren digitalen Geräten verbringen. Über die Hälfte der 18-29-Jährigen äussert diesen Wunsch. Hingegen sind fast zwei Drittel der über 65-Jährigen zufrieden mit ihrer jetzigen Nutzungszeit. Diese Ergebnisse geben wieder, dass Jüngere zwar das Internet stärker nutzen (vgl. Abb. 11), aber einem Teil von ihnen dies auch zu viel wird.

Bildschirmzeit (Abb. 13)

«Würden Sie gerne mehr oder weniger Zeit an Ihren privaten digitalen Geräten verbringen?»




Zudem zeigt sich ein klarer Geschlechtergraben: 52 Prozent der Frauen würden gerne weniger Zeit an ihren privaten digitalen Geräten verbringen, verglichen mit 39 Prozent der Männer. Bei Befragten, die mindestens einmal in der Woche Soziale Medien nutzen, ist der Anteil, der gerne weniger Zeit am Bildschirm verbringen würde, deutlich höher als bei Personen, die selten Sozia-

le Medien nutzen (49% der regelmässigen Nutzenden von Sozialen Medien; 38% der seltenen Nutzenden von Sozialen Medien). Wer sich also viel im Netz bewegt, nimmt dies nicht immer positiv wahr.

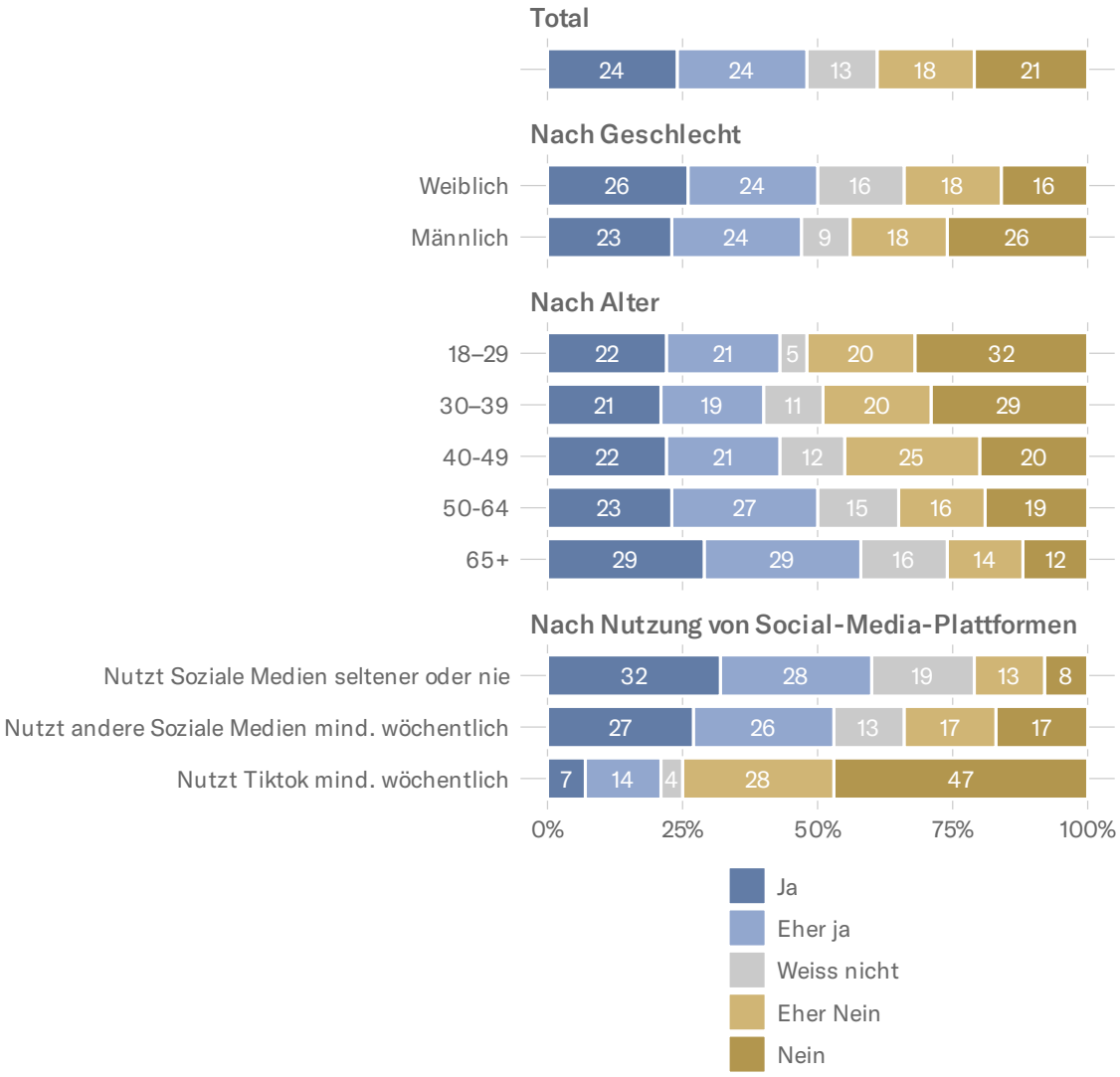
Dieses Problem dürfte in Zukunft eher noch zunehmen. Denn die heutigen jungen Generationen sind mit digitalen Geräten aufgewachsen und haben diese fest in ihren Alltag integriert. Wenn sie älter werden und ihre Nutzungsgewohnheiten beibehalten, wird allein durch den demografischen Effekt der Anteil jener Menschen steigen, die viel Zeit online verbringen – und damit möglicherweise auch der Anteil jener, die sich wünschen, sie könnten ihre private Bildschirmzeit reduzieren.

Hinsichtlich der steigenden Bildschirmzeit und dem Suchtpotenzial von manchen Apps, als auch aus Bedenken zur Datensicherheit wird in der Öffentlichkeit oft ein Verbot oder eine Regulierung der Plattform «TikTok» diskutiert.[1] Auf Geräten der Mitarbeitenden der EU-Kommission ist Tiktok aus Datenschutzgründen bereits verboten.[2] Zudem wird Tiktok dafür kritisiert ein sehr hohes Suchtpotenzial zu haben, vor allem bei Jugendlichen und Kindern. Sowohl die Algorithmen als auch das endlose Scrollen durch Kurzvideos, machen das Ansehen fesselnd und fördern einen Automatismus, dem man sich nur schwer entziehen kann.[3] Wie die Schweizer Bevölkerung zu einem allgemeinen Tiktok-Verbot steht, ist auf der Abbildung 14 ersichtlich. Ungefähr die Hälfte befürwortet ein allgemeines Tiktok-Verbot (48%). Unter den jüngeren Befragten, die Tiktok tendenziell öfters benutzen (siehe Abb. 11), sind die Hälfte gegen ein Tiktok-Verbot. Die Haltung zu einem Tiktok-Verbot variiert stark je nach Bevölkerungsgruppe.

[1] Radio SRF 1 2025: Braucht es in der Schweiz Regeln für Facebook, Tiktok und co.
[2] NZZ 2023: Spionageverdacht bei Tiktok
[3] SRF 2024: Gefangen in der Endlosschlaufe: Smartphone-Sucht bei Jugendlichen

Zustimmung zu einem TikTok-Verbot in der Schweiz (Abb. 14)

«Befürworten Sie ein generelles Verbot von TikTok in der Schweiz?»




Ein ähnliches Bild zeigt sich auch bei Personen, die Tiktok generell nutzen. Ein Fünftel (21%) dieser Befragten befürwortet ein Tiktok-Verbot, eine klare Mehrheit ist eher dagegen (75%). Wer hingegen andere oder keine Soziale Medien benutzt, spricht sich eher für eine Regulierung aus (53% bzw. 60%). Dass Tiktok-Nutzende sich weniger für ein Tiktok-Verbot aussprechen erstaunt nicht, jedoch verweist es darauf, dass die Nutzenden trotz den öffentlich bekannten Risiken der App, diese gerne nutzen und nicht davon absehen wollen.

Zusammengefasst zeigen die Ergebnisse, dass bedeutende Herausforderungen in der digitalen Welt existieren, darüber ist sich die Mehrheit der Schweizer Bevölkerung einig (Abb. 3). Die aufgeschlüsselten Ergebnisse zeigen: Den eigenen Umgang mit dem Internet schätzen die Befragten aber generell als angemessen ein und fühlen sich beim Surfen auch wohl. Jedoch gibt es auch klare Unterschiede zwischen der eigenen Wahrnehmung und der Einschätzung der Bevölkerung insgesamt: Hier findet die Mehrheit, dass Schweizer und Schweizerinnen sich weniger risikofreudig im Netz bewegen sollten (Abb. 7). Wie stark jedoch individuelle Sorgen um Cyberkriminalität und die eigene Sicherheit sind, bleibt eine offene Frage, die im nächsten Kapitel erläutert wird.

# Cyberbetrug und Cyberbelästigung

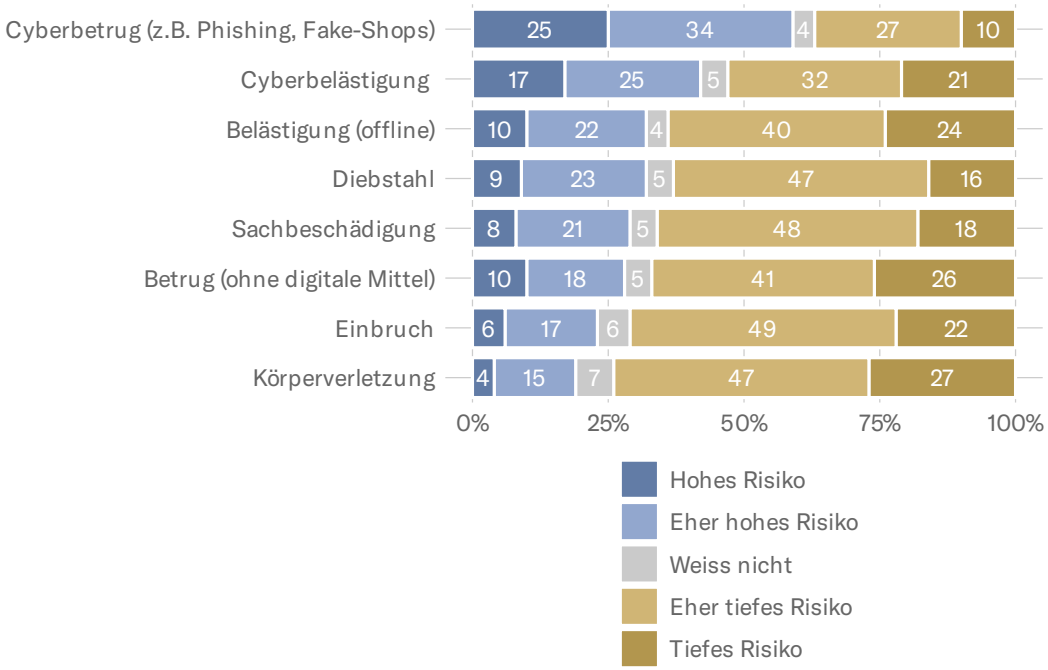
In diesem Kapitel wird die Herausforderung der Cyberkriminalität mit Schwerpunkt auf zwei Arten von Straftaten beleuchtet: Cyberbetrug und Cyberbelästigung. Das Kapitel zeigt auf, wie besorgt die Bevölkerung über diese Delikte ist, wie häufig Personen in der Schweiz schätzungsweise davon betroffen sind und wie belastend sie für die Opfer sein können.

## 3.1 VERBREITETE SORGE VOR CYBERDELIKTEN

Die Schweizer Bevölkerung schätzt das Risiko, Opfer von online begangenen Delikten zu werden, deutlich höher ein als bei vergleichbaren Delikten in der physischen Welt. Besonders gross ist die Sorge vor Cyberbetrug, beispielsweise durch Phishing oder Fake-Shops: 59 Prozent schätzen das Risiko, dass sie in den nächsten Jahren davon betroffen sein werden, als hoch oder eher hoch ein (Abb. 15). Bei Betrug ohne digitale Mittel sind es hingegen nur 28 Prozent. Ein ähnliches Bild zeigt sich bei Belästigungen: 42 Prozent schätzen das Risiko einer Cyberbelästigung als hoch oder eher hoch ein. Bei Belästigungen «offline» sind es hingegen weniger mit 32 Prozent.

Einschätzung des Risikos von div. Delikten persönlich betroffen zu sein (Abb. 15)

«Wie hoch schätzen Sie das Risiko ein, dass Sie persönlich von den folgenden Delikten in den nächsten drei Jahren betroffen sein werden?» – Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.




Ein Vergleich mit der polizeilichen Kriminalstatistik zeigt: die Bevölkerung schätzt die Risiken von Cyberbetrug im Vergleich mit Betrug ohne digitale Mittel realistisch ein. Digitale Betrugsfälle kommen tatsächlich deutlich häufiger vor als Betrugsfälle ohne Verwendung von digitalen Mitteln. So sind gemäss Kriminalstatistik letztes Jahr 80 Prozent aller angezeigten Betrugsfälle online begangen worden[4].

Etwas anders sieht es bei Belästigungen aus. Bei Strafbeständen wie Beschimpfung, Verleumdung, übler Nachrede oder Drohung überwiegen weiterhin klar die angezeigten Vergehen, die nicht im digitalen Raum verübt wurden [5]. Gerade bei Cyberbelästigungen muss jedoch von einer hohen Dunkelziffer ausgegangen werden, da längstens nicht alle Fälle der Polizei gemeldet werden.

[4] BFS 2025: Polizeiliche Kriminalstatistik, Jahresbericht 2024

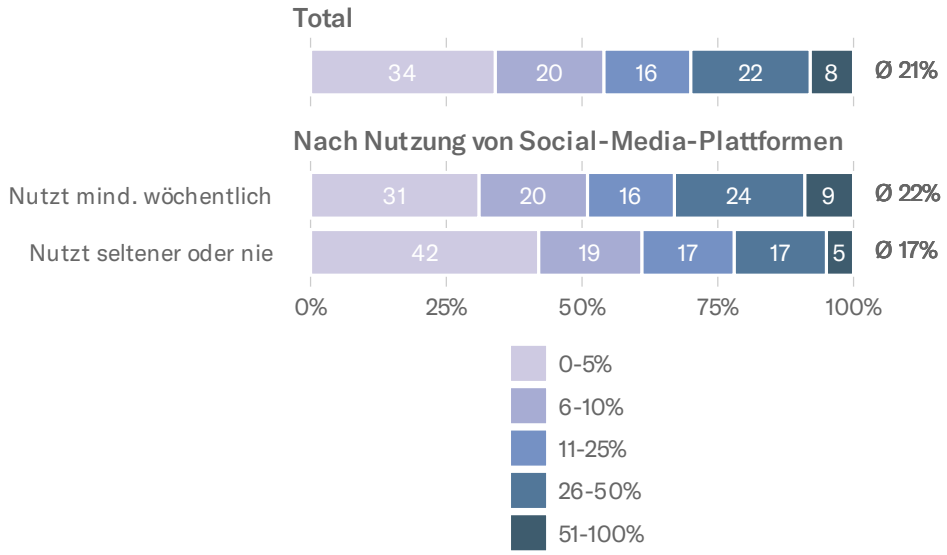
[5] BFS 2025: Polizeiliche Kriminalstatistik, Jahresbericht 2024; BFS 2025: Strafgesetzbuch (StGB): Straftaten und beschuldigte Personen

# Risiken von Cyberbetrug und -belästigung wird klar höher eingeschätzt als von ähnlichen Delikten «offline».

Abbildung 16 zeigt genauer, wie hoch die Bevölkerung die Wahrscheinlichkeit einschätzt, dass sie selbst in den nächsten fünf Jahren im digitalen Raum belästigt werden. Ein Drittel schätzt die Wahrscheinlichkeit auf über 25 Prozent. Interessant ist, dass fast jede zehnte Person, die regelmässig Social Media (Facebook, Instagram, X / Twitter, TikTok, etc.) nutzt, die Wahrscheinlichkeit einer Cyberbelästigung auf über 50 Prozent schätzt – und trotzdem weiterhin regelmässig eine oder mehrere dieser Social-Media-Plattformen nutzt. Dies, obwohl vermutlich ein grosser Teil der Fälle von Cyberbelästigung auf diesen Plattformen stattfindet. Diese Personen nehmen ihrer eigenen Einschätzung nach ein erhöhtes Risiko in Kauf, Opfer von Cybermobbing zu werden, um weiterhin auf Social Media aktiv sein zu können.

Einschätzung der Wahrscheinlichkeit einer Cyberbelästigung (Abb. 16)

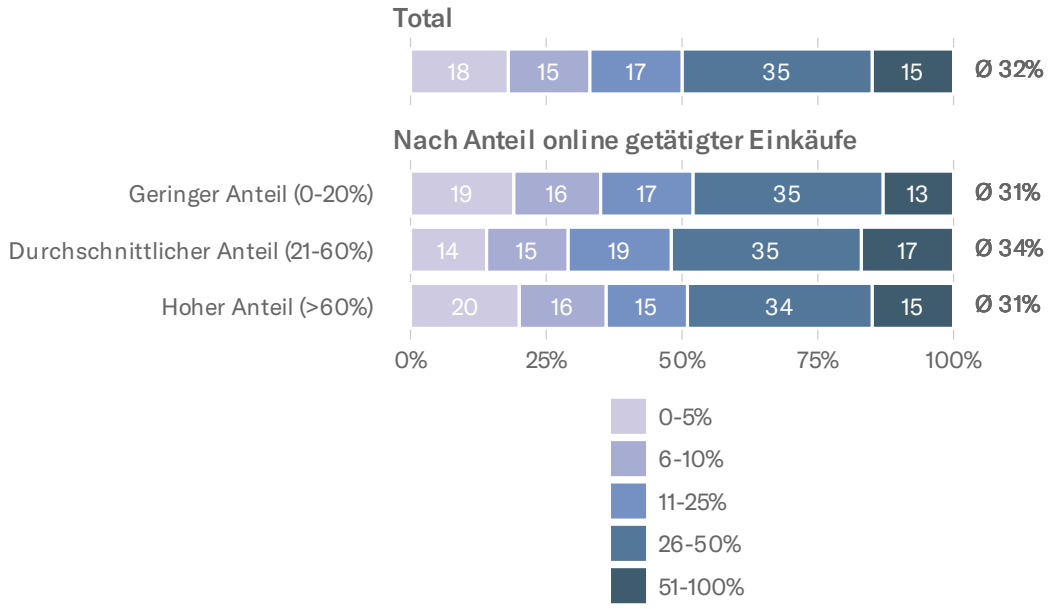
«Für wie wahrscheinlich halten Sie es, dass Sie in den nächsten fünf Jahren von Cyberbelästigung betroffen sein werden?» – Offene Frage. Antwortklassen wurde nach Dateneinsicht durch Autor:innen definiert.




Das Risiko, persönlich von einem Cyberbetrug betroffen zu sein, schätzen Befragte höher ein als bei einer Cyberbelästigung (vgl. Abb. 17 & 16). Im Schnitt wird die Wahrscheinlichkeit, in den nächsten fünf Jahren Opfer eines Cyberbetrugs zu werden, auf 32 Prozent eingeschätzt.

Einschätzung der Wahrscheinlichkeit eines Cyberbetrugs (Abb. 17)

«Für wie wahrscheinlich halten Sie es, dass Sie in den nächsten fünf Jahren von einem Cyberbetrug betroffen sein werden?» – Offene Frage. Antwortklassen wurde nach Dateneinsicht durch Autor:innen definiert.




Bemerkenswert ist, dass es kaum einen Unterschied in der Risikowahrnehmung gibt zwischen Personen, die viel online einkaufen, und solchen, die lieber im stationären Handel einkaufen – obwohl laut Kriminalstatistik viele Betrugsfälle in Online-Shops und auf Kleinanzeigenplattformen stattfinden[6]. Rund die Hälfte der Personen, die einen hohen Anteil ihrer Einkäufe online tätigen, schätzt das Risiko, online betrogen zu werden, auf über 25 Prozent ein. Sie gehen dieses hohe Risiko ein, um weiterhin online einkaufen zu können.

## 3.2 EMOTIONALE BELASTUNG BEI OPFERN VON CYBERBETRUG

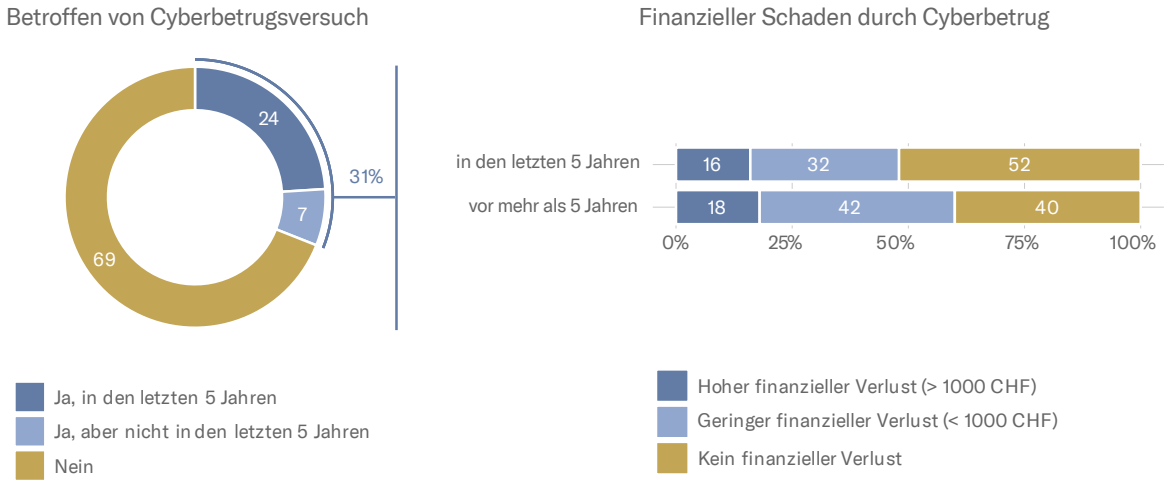
Drei von zehn erwachsenen Personen in der Schweiz haben schon einmal einen Cyberbetrugsversuch erlebt (Abb. 18). Bei knapp einem Viertel der Befragten fand der Cyberbetrugsversuch in den letzten fünf Jahren statt, bei sieben Prozent liegt

[6] BFS 2025: Polizeiliche Kriminalstatistik, Jahresbericht 2024

dieser bereits länger zurück. Cyberbetrug zählt gemäss geltender Rechtslage zu den klassischen Betrugsdelikten und setzt damit einen finanziellen Schaden beim Opfer voraus.[7] Fehlt ein solcher Vermögensverlust, wird der Vorfall juristisch nicht als Cyberbetrug eingestuft. Deshalb wird in diesem Bericht zwischen Cyberbetrugsversuchen ohne finanziellen Schaden und Cyberbetrug mit finanziellem Schaden unterschieden. Der Abbildung 18 lässt sich also entnehmen, dass knapp 15 Prozent der Befragten schon einmal einen tatsächlichen Cyberbetrug erlebt haben.

Betroffene von Cyberbetrugsversuch (Abb. 18)

«Haben Sie selbst bereits einen Cyberbetrug erlebt?»



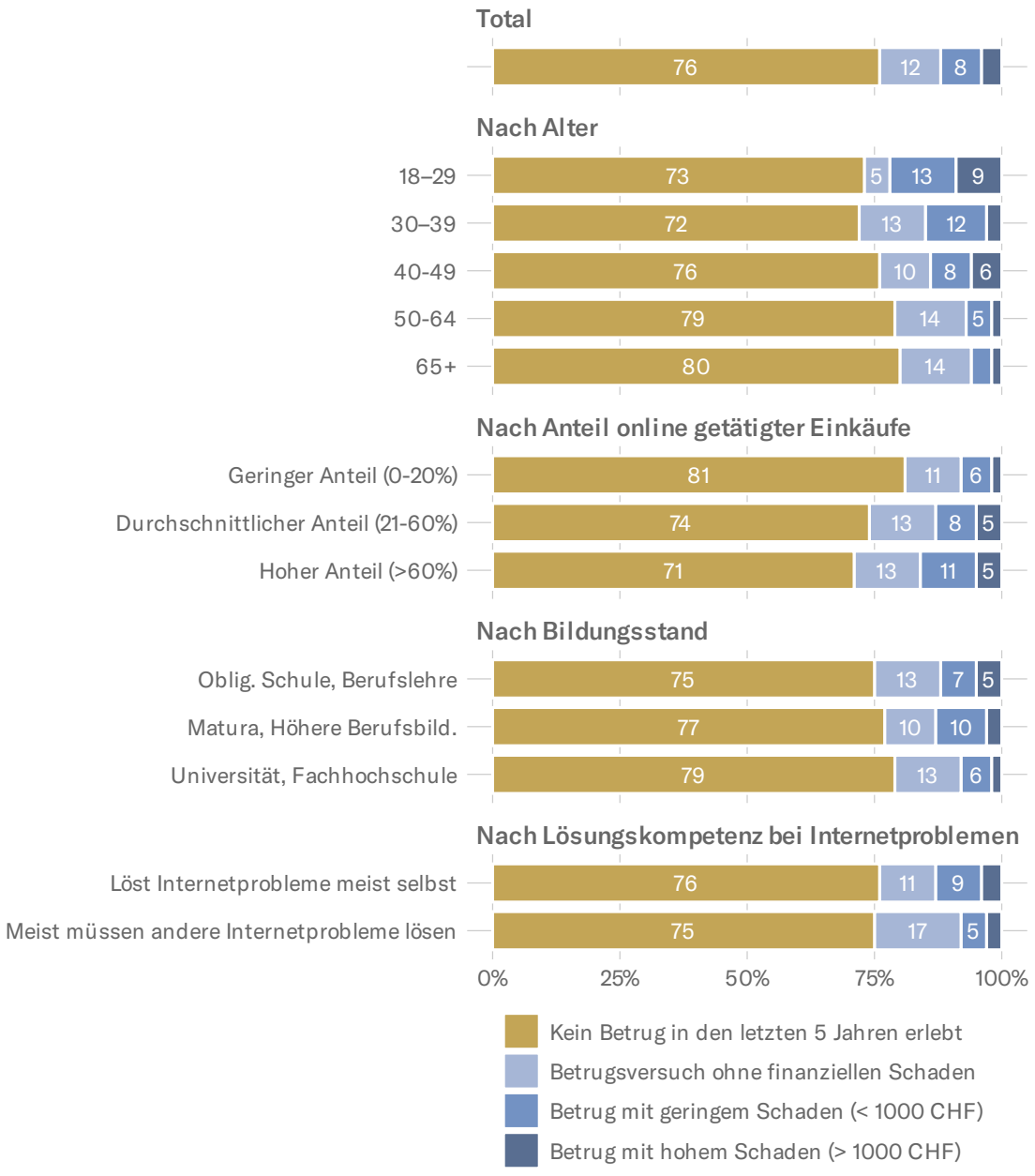

Nach obiger Definition wurden in den letzten fünf Jahren knapp zwölf Prozent der Befragten Opfer eines Cyberbetrugs mit finanziellem Verlust (Abb. 19). Wiederum zwölf Prozent der Befragten geben an, in den letzten fünf Jahren einen Cyberbetrugsversuch ohne finanzielle Folgen erlebt zu haben. Wie Abbildung 19 zeigt, sind Personen, die das Internet häufiger benutzen – Jüngere und Personen, die einen hohen Anteil ihrer Einkäufe online

[7] Schweizerische Kirminalprävention 2025: Betrug

tätigen – etwas häufiger bereits Opfer von einem Cyberbetrug geworden.

Finanzieller Schaden durch Cyberbetrug (Abb. 19)

«Haben Sie selbst bereits einen Cyberbetrug erlebt?» / «Haben Sie durch den Cyberbetrug einen finanziellen Schaden erlitten?» – nur Cyberbetrüge in den letzten 5 Jahren




Doch die Unterschiede zwischen den Bevölkerungsgruppen sind geringfügig. So sind aus allen Bildungsschichten ungefähr ähnlich viele Personen bereits Opfer geworden. Zudem fallen Personen, die sich im digitalen Raum gut auskennen, ebenso

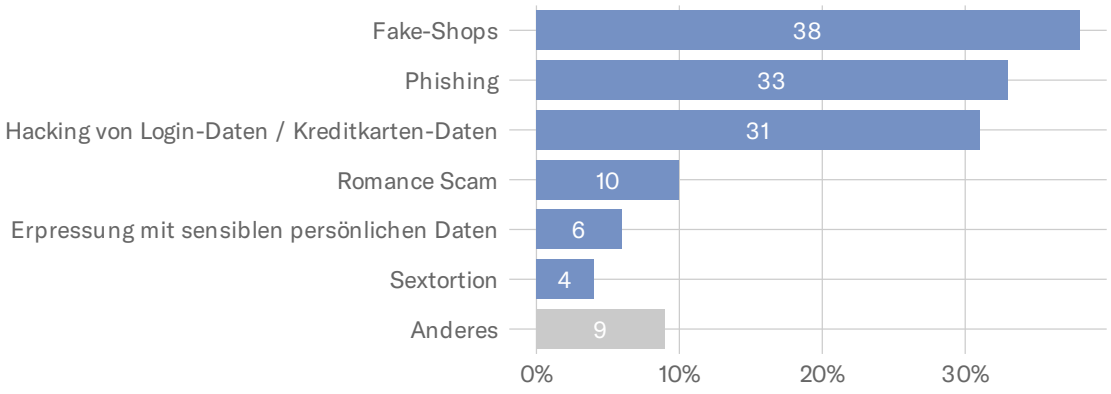
häufig Betrügern zum Opfer, wie Personen, welche mit dem Internet weniger bewandert sind. Konkret sind Personen, welche angeben, dass sie technische Probleme bei der Internetnutzung (z.B. Verbindungsprobleme, Software-Absturz) immer oder meistens selbst lösen können, ähnlich häufig bereits Opfer von Cyberbetrug geworden, wie Personen, welche angeben, dass sie für technische Probleme meistens Hilfe beiziehen. Damit kann gesagt werden: es gibt offenbar keinen klaren Opfer-Typus, also keine eindeutige Personengruppe, aus der die meisten Opfer von Cyberbetrug stammen.

# Es gibt keinen klaren Opfertypus für Cyberbetrug.

Abbildung 20 veranschaulicht, welche Arten von Cyberbetrug am häufigsten vorkommen. Die meisten Betroffenen (38%) haben schon Betrugsfälle via betrügerischer Internetshops, bei denen beispielsweise die Lieferung von bereits bezahlten Waren ausblieb, erlebt.

Erfahrungen mit Cyberbetrug (Abb. 20)

«Von welchen der folgenden Formen des Cyberbetrugs waren Sie selbst bereits betroffen?» – Nur Personen, die schon einmal Cyberbetrug erlebt haben (N=252). Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.



Drei von zehn waren bereits Opfer von Phishing also betrügerischen E-Mails, SMS oder Anrufen, die sie dazu verleitet haben, sensible Informationen wie Passwörter oder Bankdaten auf gefälschten Webseiten preiszugeben. 31 Prozent berichten, dass ihre Login- oder Kreditkartendaten gehackt wurden. Seltener sind Romance Scams (Online-Liebesbetrug für finanzielle Vorteile; 10%), Erpressung mit sensiblen und persönlichen Daten (6%) oder Sextortion (Erpressung mit Veröffentlichung von intimen Bildern; 4%). Auch wenn diese Betrugsformen weniger häufig auftreten, sind in absoluten Zahlen immer noch eine beträchtliche Anzahl von Menschen betroffen.

Opfer eines Betruges zu werden, kann für die Betroffenen eine hohe emotionale Belastung darstellen. Zu den negativen Gefühlen, die sich aus dem finanziellen Verlust und dem verletzten Sicherheitsgefühl ergeben können, dürfte häufig auch ein Gefühl der Scham hinzukommen, etwa darüber, auf die Betrugsmasche hereingefallen zu sein – obwohl es grundsätzlich alle treffen kann, wie Abbildung 19 zeigt.

Besonders hoch ist die emotionale Belastung, wenn die Betroffenen einen gewichtigen finanziellen Schaden erleiden (Abb. 21). 76 Prozent der Opfer eines Cyberbetrugs, mit einem persönlichen Verlust von mehr als CHF 1000, berichten von einer hohen oder eher hohen emotionalen Belastung als Folge des Betrugs. Von den Personen, die einen geringen erlitten, geben rund die Hälfte an, emotional darunter gelitten zu haben.

Emotionale Belastung von Opfern von Cyberbetrug (Abb. 21)

«Wie war die emotionale Belastung für Sie persönlich, als Sie von einem Cyberbetrug betroffen waren? (Falls Sie mehrere Cyberbetrüge erlebt haben, antworten Sie für den schwersten Fall)» – Nur Personen, die schon einmal Cyberbetrug erlebt haben (N=253)

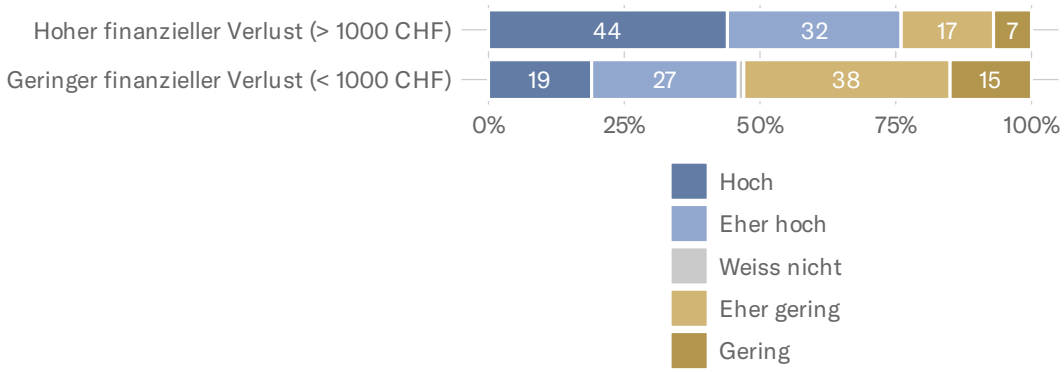
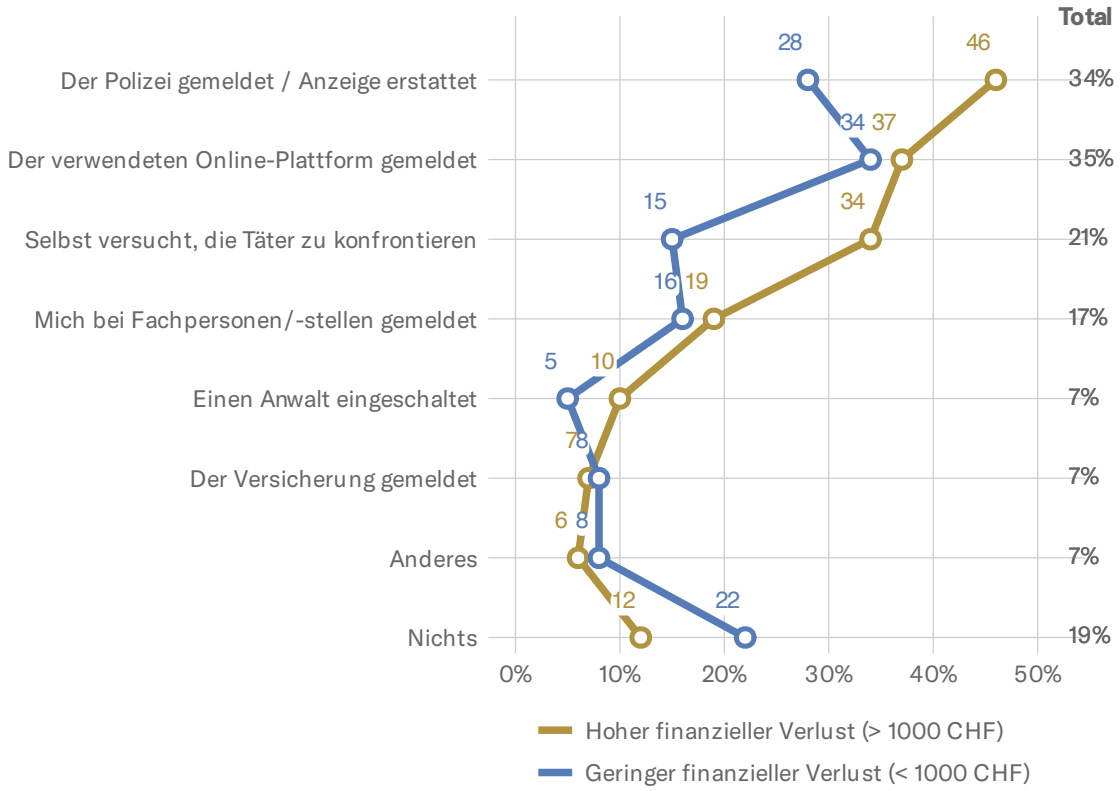



Abbildung 22 zeigt, wie Betroffene nach einem Cyberbetrug reagiert haben. Besonders auffällig ist der geringe Anteil derjenigen, die den Betrug der Polizei gemeldet haben. Selbst unter den Personen, die einen hohen finanziellen Verlust erlitten, wandten sich weniger als die Hälfte (46%) an die Polizei. Bei einem geringeren finanziellen Schaden lag dieser Anteil sogar nur bei 28 Prozent.

Getroffene Massnahmen nach Cyberbetrug – nach Höhe des finanziellen Verlusts (Abb. 22)

«Was haben Sie gemacht, als Sie Opfer eines Cyberbetrugs geworden sind? (Wählen Sie alle zutreffenden Antworten an. Falls Sie mehrere Cyberbetrüge erlebt haben, antworten Sie für den schwersten Fall)» – Nur Personen, die schon einmal Cyberbetrug erlebt haben (N=253)




Ein möglicher Grund, wieso so wenige zur Polizei gehen, ist wohl die geringe Wahrscheinlichkeit, dass Tatverdächtige identifiziert werden. Gemäss der Kriminalstatistik konnten 2024 nur 14 Prozent der Straftaten aufgeklärt werden. Aufklärung bedeutet in diesem Zusammenhang, dass eine Person als mutmassliche Täterin oder Täter identifiziert werden konnte. Im Online-Raum erschwert oft die Anonymität der Nutzenden die Identifikation zusätzlich. Die Chancen sind also sehr gering, dass eine Aufklärung erfolgen kann und entsprechend unwahrscheinlich ist es, das verlorene Geld zurückzuerhalten. Zudem verweisen Fachleute häufig darauf, dass Scham, auf die Betrugsmasche hereingefallen zu sein auch ein Grund für die tiefe Anzeige-Quote sein dürfte.[8] Dennoch wäre es wichtig, versuchte oder tatsächliche Betrugsfälle der Polizei zu melden, damit

[8] NZZ 2023: Massive Dunkelziffer bei Cybercrime

diese Zusammenhänge mit anderen Fällen herstellen und allenfalls Ermittlungsansätze finden kann sowie die Bevölkerung vor neuen Betrugsmaschen warnen kann[9].

Gut ein Drittel der Betroffenen hat den Betrugsvorfall der entsprechenden Online-Plattform gemeldet, rund jede sechste Person hat sich an Fachstellen gewandt. 34 Prozent der Opfer, die einen hohen finanziellen Verlust erlitten, haben zudem selbst versucht, die Täterschaft zu konfrontieren. Kaum jemand hat einen Anwalt eingeschaltet oder den Betrug der Versicherung gemeldet.

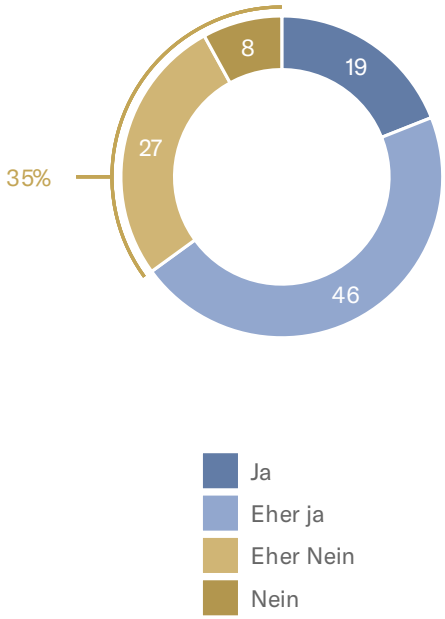
# Viele sind unsicher, wie sie im Falle eines Cyberbetrugs richtig reagieren sollen.

35 Prozent der Bevölkerung fühlt sich nicht ausreichend informiert darüber, wie sie bei einem Cyberbetrug am besten reagieren sollen (Abb. 23). Nur 19 Prozent sagen, sie wissen mit Sicherheit, wie zu reagieren sei.

[9] Schweizerische Kriminalprävention 2025: Was macht die Polizei bei Fällen von Internetbetrug?

Informationsstand bei Cyberbetrug (Abb. 23)

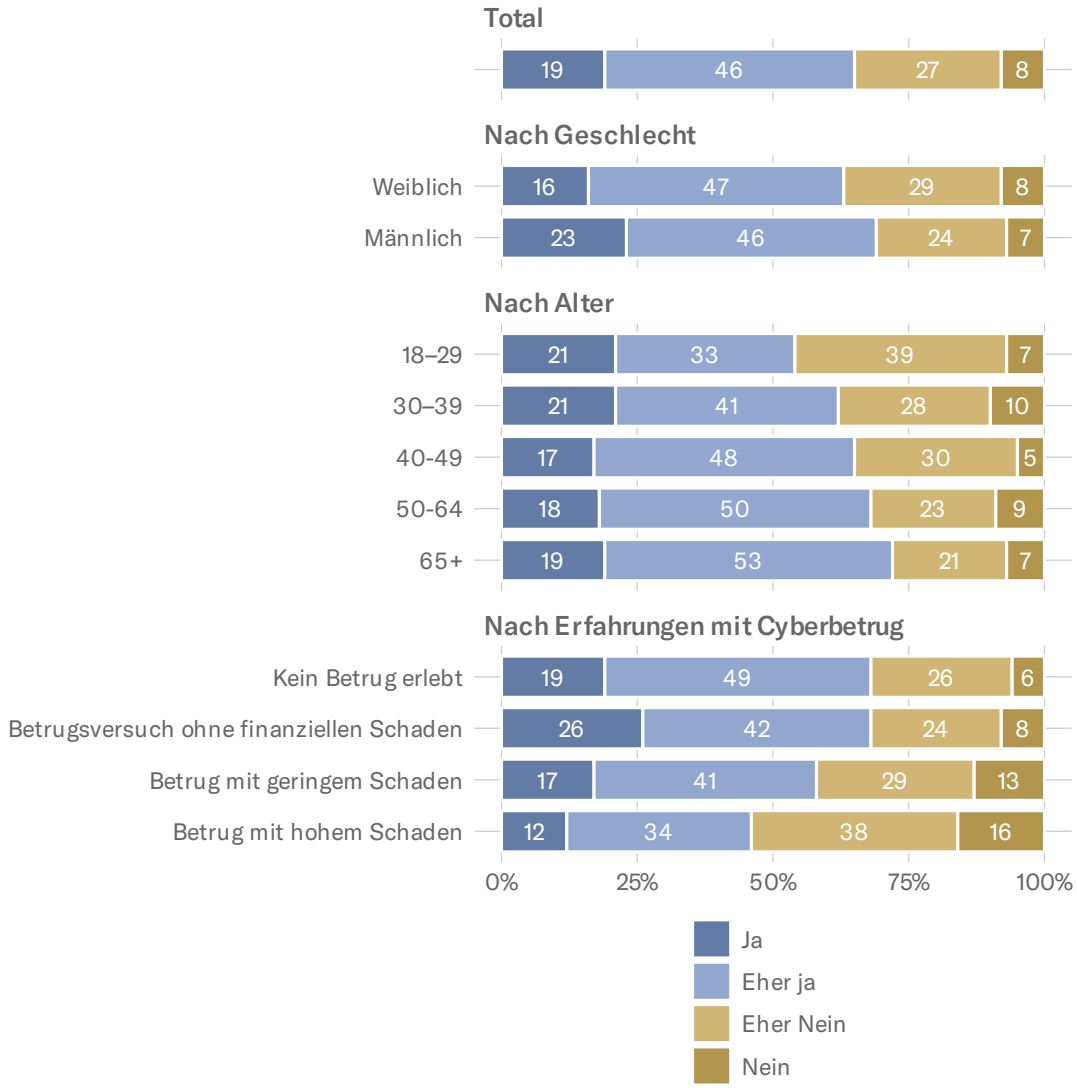
«Fühlen Sie sich genügend informiert darüber, wie Sie bei einem Cyberbetrug am besten reagieren?»




Interessanterweise fühlen sich Personen, die bereits einen finanziellen Schaden durch Cyberbetrug erlitten haben, tendenziell weniger gut informiert – obwohl sie eigentlich bereits Erfahrung im Umgang damit haben sollten (Abb. 24). Dies lässt darauf schliessen, dass viele erst im Nachhinein erkennen, dass sie nicht wirklich wussten, wie sie reagieren sollten.

Informationsstand bei Cyberbetrug (Abb. 24)

«Fühlen Sie sich genügend informiert darüber, wie Sie bei einem Cyberbetrug am besten reagieren?»




Zudem fühlen sich Frauen und jüngere Menschen weniger gut informiert darüber, wie sie bei einem Cyberbetrug handeln sollen. 37 Prozent der Frauen geben an, sich nicht genügend informiert zu fühlen, verglichen mit 31 Prozent der Männer. Besonders ausgeprägt ist diese Unsicherheit bei den 18- bis 29-Jährigen, von denen 46 Prozent angeben, nicht zu wissen, wie sie richtig handeln sollten. Zum Vergleich: In der Altersgruppe 65+ sind es nur 28 Prozent.

Ein beträchtlicher Teil der erwachsenen Bevölkerung in der Schweiz fühlt sich also unsicher und wünscht sich mehr In-

formationen darüber, wie im Falle eines Cyberbetrugs richtig vorzugehen ist.

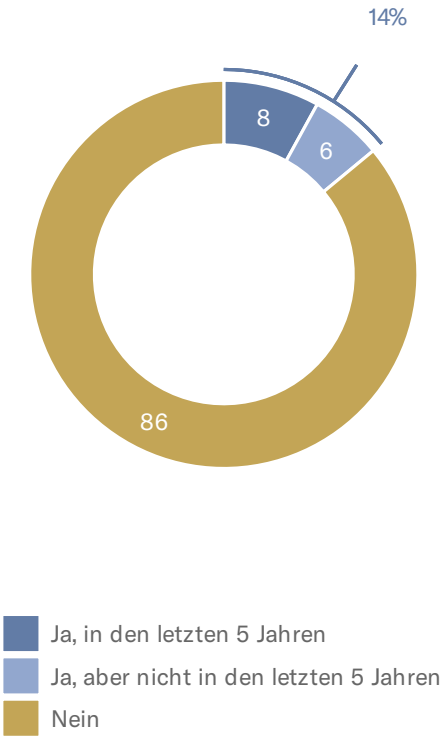
## 3.3 SELBST SCHWERE CYBERBELÄSTIGUNG WIRD KAUM ANGEZEIGT

Wie bei Betrug schätzen die Menschen in der Schweiz auch bei Belästigungen das Risiko selbst davon betroffen zu sein im digitalen Raum höher ein als «offline» (Abb. 15). Wie weiter oben beschrieben, lässt sich dieses Gefühl jedoch nicht durch die polizeiliche Kriminalstatistik erhärten. Die grosse Mehrheit der angezeigten Straftaten wie Verleumdung, Beschimpfung, üble Nachrede, Drohung oder Nötigung sind gemäss der Kriminalstatistik nicht im digitalen Raum begangen worden. Die polizeiliche Kriminalstatistik umfasst jedoch nur die angezeigten Delikte. Die Dunkelziffer dürfte gerade bei Cyberbelästigung beträchtlich sein.

Abbildung 25 gibt einen Hinweis darauf, wie verbreitet Cyberbelästigung tatsächlich ist. 14 Prozent der erwachsenen Schweizer Bevölkerung geben an, schon einmal selbst Cyberbelästigungen – sprich gezielte Beleidigung, Belästigung und Bedrängung auf einer Online-Plattform (z.B. Cybermobbing, Hassrede, sexuelle Belästigung) – erlebt zu haben. Bei rund acht Prozent geschah dies in den letzten fünf Jahren. Für sechs Prozent liegt die Belästigung bereits mehr als fünf Jahre zurück.

Opfer von Cyberbelästigungen (Abb. 25)

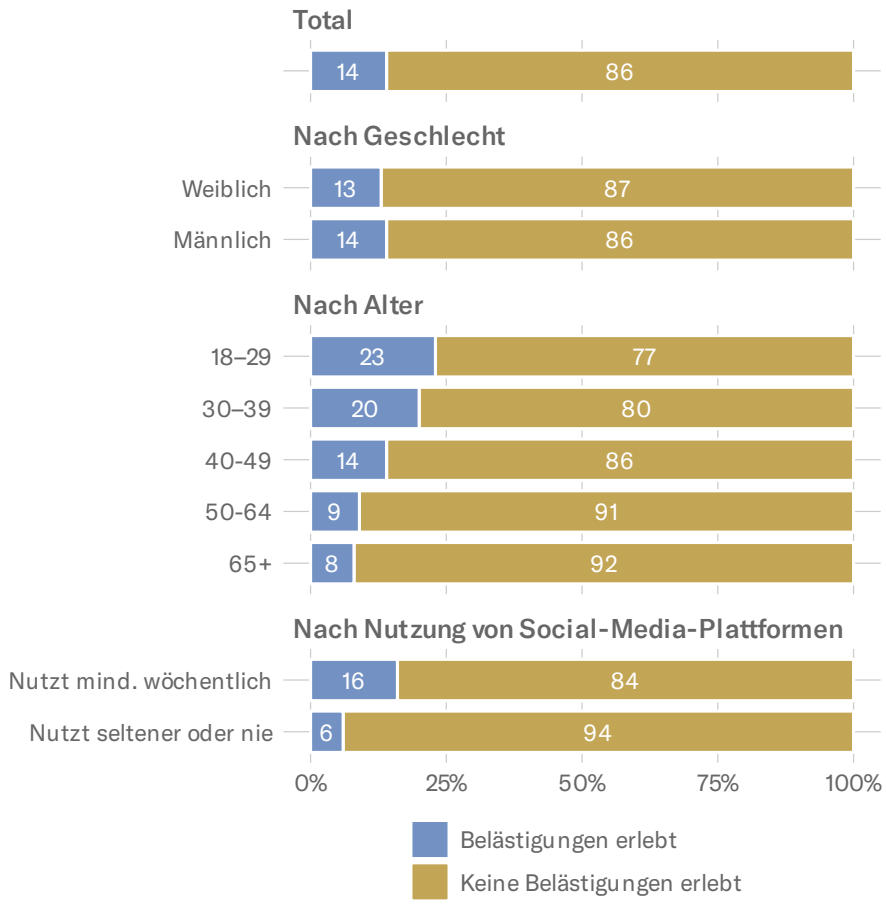
«Haben Sie selbst bereits Cyberbelästigungen erlebt? Cyberbelästigung bezeichnet die gezielte Beleidigung, Belästigung und Bedrängung von Personen auf Online-Plattformen. Dazu gehören unter anderem Cybermobbing, Hassrede, sexuelle Belästigung im Internet oder das ungewollte Veröffentlichen persönlicher Daten.»




Etwa gleich viele Männer (14%) wie Frauen (13%) geben an, schon Opfer von Cyberbelästigung geworden zu sein (Abb. 26). Jüngere Personen haben schon deutlich häufiger Erfahrungen mit Cyberbelästigungen machen müssen. Beinahe ein Viertel der 18-29-Jährigen (23%) gibt an, schon einmal online belästigt worden zu sein. Bei Personen über 50 sind es hingegen weniger als zehn Prozent.

Opfer von Cyberbelästigungen (Abb. 26)

«Haben Sie selbst bereits Cyberbelästigungen erlebt? Cyberbelästigung bezeichnet die gezielte Beleidigung, Belästigung und Bedrängung von Personen auf Online-Plattformen. Dazu gehören unter anderem Cybermobbing, Hassrede, sexuelle Belästigung im Internet oder das ungewollte Veröffentlichen persönlicher Daten.»



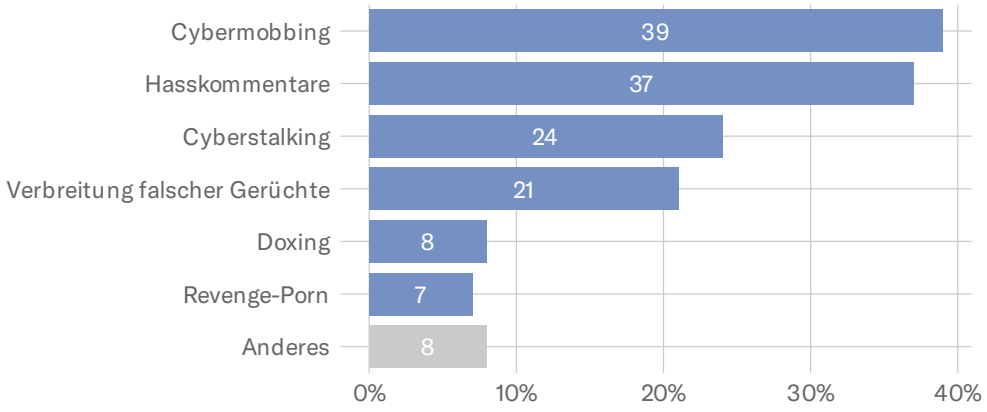

Von den Personen, die mindestens eine Social-Media-Plattform (Facebook, Twitter/X, Instagram, TikTok, linked.in) einmal pro Woche oder häufiger nutzt, geben 16 Prozent an, Erfahrungen mit Cyberbelästigung zu haben. Selbst bei Personen, die zum Zeitpunkt der Umfrage seltener als einmal pro Woche oder nie Social Media nutzten, waren sechs Prozent schon einmal betroffen.

Die am häufigsten erlebte Form von Cyberbelästigung ist Cybermobbing, also wiederholte Beleidigungen oder Belästigungen online (Abb. 27). 39 Prozent der Personen, die schon Cyberbelästigungen erlebt haben, sind schon Opfer von Cybermobbing geworden. 37 Prozent haben bereits Hasskommentare erhalten. 24 Prozent sind schon mit digitalen Mitteln ausspioniert wor-

den (Cyberstalking). Über 21 Prozent wurden falsche Gerüchte verbreitet. Weniger häufig sind Doxing (absichtliche Veröffentlichung sensibler persönlicher Daten wie Bilder, Wohndresse etc.; 8%) und Revenge Porn (ungewollte Veröffentlichung intimer Bilder/Videos; 7%).

Erlebte Formen von Cyberbelästigung (Abb. 27)

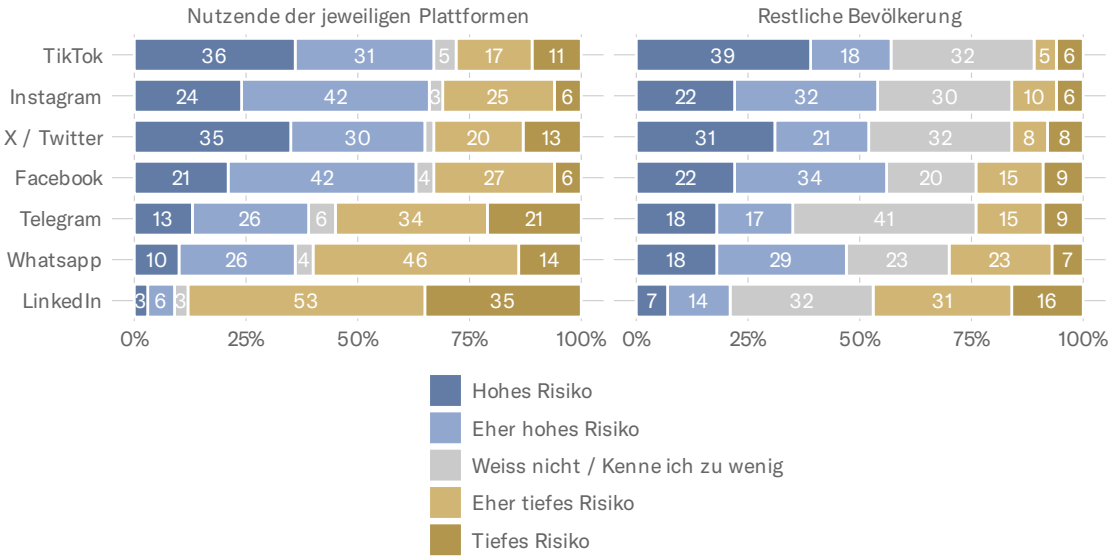
«Von welchen der folgenden Formen der Cyberbelästigung waren Sie bereits selbst betroffen?» – Nur Personen, die bereits von Cyberbelästigung betroffen waren(N=197). Die Labels auf der Abbildung sind gegenüber der Umfrage gekürzt.




Viele Cyberbelästigungen passieren auf Social-Media-Plattformen. Das Risiko variiert dabei je nach Plattformen. Abbildung 28 zeigt, wie die Bevölkerung das Risiko für Cyberbelästigungen auf den verschiedenen Plattformen einschätzt. Das Risiko wird bei TikTok am höchsten eingeschätzt – sowohl von TikTok-Nutzenden als auch von Nicht-Nutzenden. 67 Prozent der Personen, die mindestens einmal pro Woche TikTok benutzen schätzen das Risiko einer Cyberbelästigung als hoch oder eher hoch ein. Ähnlich sieht es bei den Plattformen Instagram (66%), X / Twitter (65%) und Facebook (63%) aus – wobei bei TikTok und X / Twitter jeweils der Anteil höher ist, die ein klar hohes Risiko sehen, verglichen mit den Personen, die das Risiko als eher hoch einschätzen.

Risiko für Belästigung auf versch. Plattformen – nach Nutzung der jeweiligen Plattformen (Abb. 28)

«Wie schätzen Sie das Risiko einer Cyberbelästigung für Nutzende auf folgenden Plattformen ein?» – Personen gelten als Nutzende, wenn sie mindestens einmal pro Woche auf der jeweiligen Plattform aktiv sind.

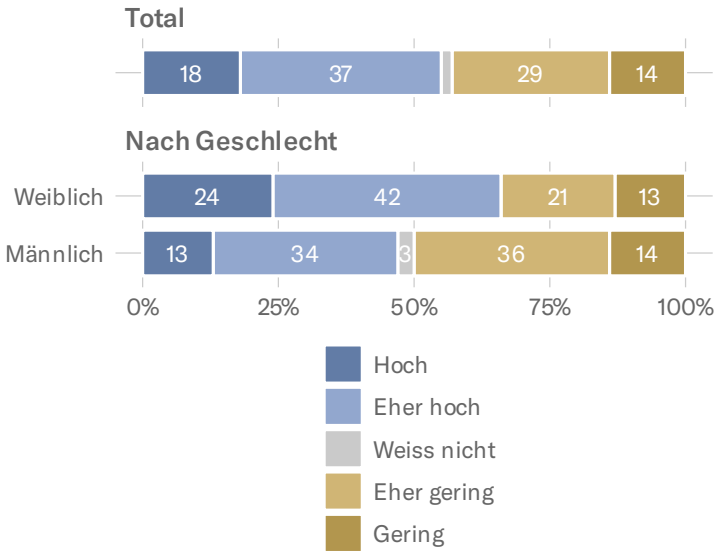



Bei den primär als Messengerdienste genutzten Plattformen Telegram und WhatsApp wird das Risiko niedriger eingeschätzt. 39 Prozent schätzen das Risiko bei Telegram als hoch oder eher hoch ein, 36 Prozent bei Whatsapp. Auch LinkedIn wird kaum als risikobehaftet wahrgenommen. Nur neun Prozent der Nutzenden stufen das Risiko einer Cyberbelästigung dort als hoch oder eher hoch ein.

Mehr als die Hälfte der Betroffenen (55%) gibt an, die Belästigung habe sie emotional stark oder eher stark belastet (Abb. 29). Besonders hoch ist die emotionale Belastung unter weiblichen Opfern. Zwei Drittel der betroffenen Frauen berichtet von einer hohen oder eher hohen Belastung. Bei den Männern empfinden knapp die Hälfte die emotionale Belastung als hoch. Frauen sind zwar nicht häufiger von Cyberbelästigung betroffen als Männer (Abb. 26), doch sie werden häufiger auf eine Art belästigt, die sie emotional belastet.

Emotionale Belastung durch Cyberbelästigung (Abb. 29)

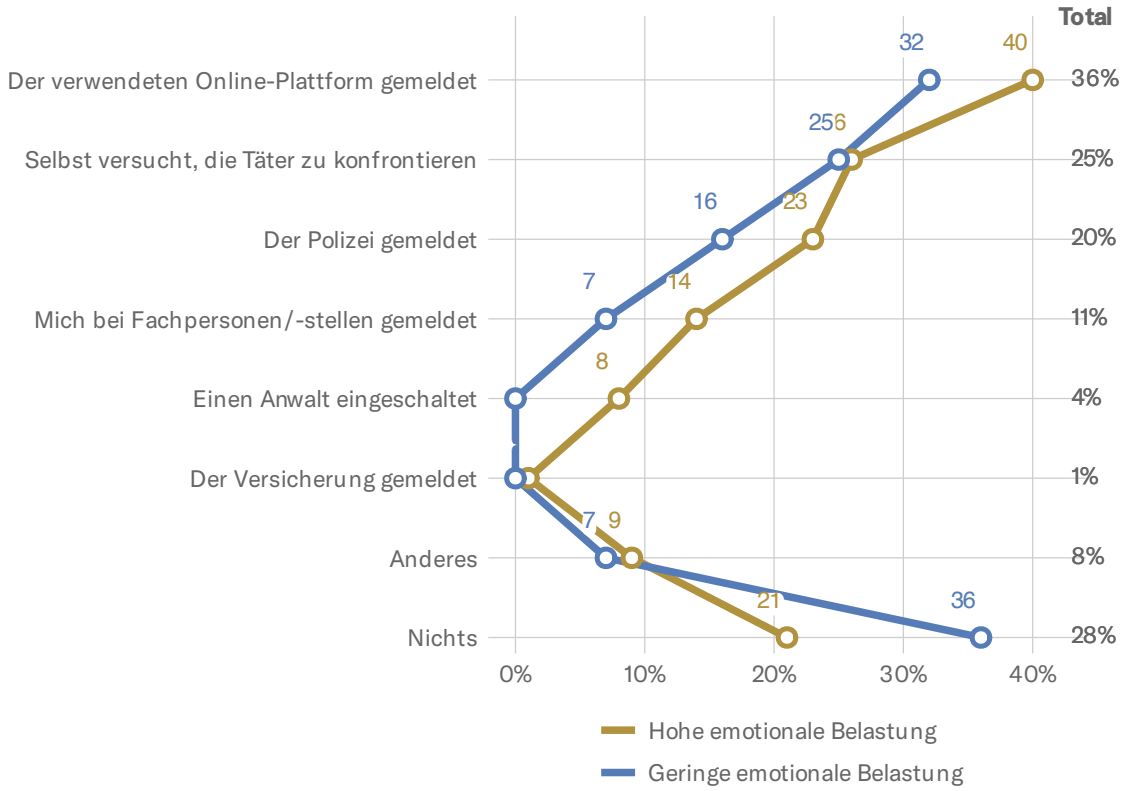
«Wie war die emotionale Belastung für Sie persönlich, als Sie von Cyberbelästigung betroffen waren? (Falls Sie mehrere Fälle von Cyberbelästigung erlebt haben, antworten Sie für den schwersten Fall)» – Nur Personen, die bereits von Cyberbelästigung betroffen waren (N=197)




Wie Abbildung 30 zeigt, melden selbst Opfer von schweren Cyberbelästigungen mit einer hohen emotionalen Belastung, die Belästigung nur selten der Polizei. 23 Prozent von Opfern mit einer hohen emotionalen Belastung haben die Belästigung der Polizei gemeldet – beinahe ebenso viele wie nichts gemacht haben (21%). Das deutet auf eine hohe Dunkelziffer in den offiziellen Deliktzahlen von Straftaten im Zusammenhang mit Cyberbelästigungen hin.

Getroffene Massnahmen nach Cyberbelästigung – nach emotionaler Belastung (Abb. 30)

«Was haben Sie gemacht, als Sie Ziel von Cyberbelästigung geworden sind? (Wählen Sie alle zutreffenden Antworten. Falls Sie mehrere Fälle von Cyberbelästigung erlebt haben, antworten Sie für den schwersten Fall)» – Nur Personen, die bereits von Cyberbelästigung betroffen waren (N=192)




40 Prozent, der Personen mit einer hohen emotionalen Belastung, haben die Belästigung der verwendeten Plattform gemeldet, 26 Prozent haben versucht, die Täterin oder den Täter selbst zu konfrontieren. Nur 14 Prozent hat sich bei Fachstellen gemeldet. Kaum jemand hat einen Anwalt eingeschaltet (8%) oder die Belästigung einer Versicherung[10] gemeldet (1%). Dies wohl primär aus dem Grund, dass bisher nur ein kleiner Anteil der Bevölkerung eine Versicherung für Cyberdelikte abgeschlossen hat.

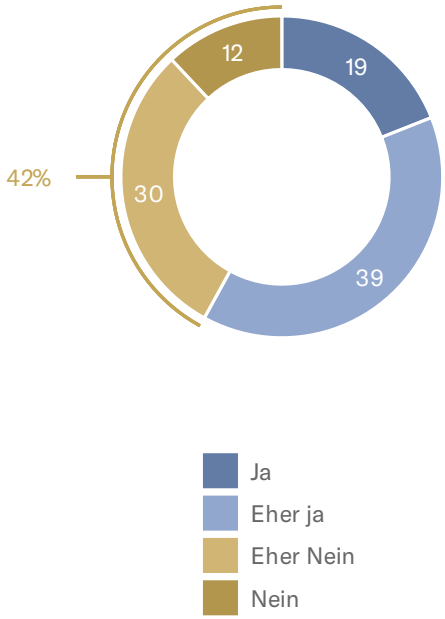
[10] Cyberversicherungen beinhalten oft einen Schutz bei Fällen von Cyberbelästigung. So kümmern sie sich beispielsweise um die Löschung von entsprechenden Inhalten oder übernehmen Anwalts- und Verfahrenskosten bei einem Rechtsfall und bieten psychologische Notfallbetreuung an.

# Hohe Dunkelziffer: Nur wenige melden Cyberbelästigungen der Polizei.

Dass nicht mehr Personen eine belastende Cyberbelästigung der Polizei melden, dürfte – wie bei Cyberbetrug – damit zusammenhängen, dass die Täterschaft sich hinter anonymen Online-Profilen verstecken kann, was eine Identifizierung dieser erschwert. Auch Schamgefühle dürften bei einigen eine Rolle spielen. Aber zumindest ein Teil der Zurückhaltung bei den getroffenen Massnahmen könnte auch dadurch erklärt werden, dass mehr als vier von zehn Personen (42%) sich nicht genügend informiert fühlen darüber, wie sie in einer solchen Situation am besten reagieren (Abb. 31). Nur rund eine von fünf Personen fühlt sich klar ausreichend informiert.

Informationsstand bei Cyberbelästigung (Abb. 31)

«Fühlen Sie sich genügend informiert darüber, wie Sie bei Cyberbelästigung am besten reagieren?»




Wie schon bei Cyberbetrug fühlt sich also auch bei Cyberbelästigungen ein beträchtlicher Teil der Bevölkerung unsicher, wie sie am besten reagieren sollten, wenn sie selbst zum Opfer werden.

Zusammengefasst kann gesagt werden, dass Cyberbelästigungen und Cyberbetrug die Bevölkerung in der Schweiz verunsichern. Ein erheblicher Teil schätzt das Risiko, in den nächsten Jahren selbst davon betroffen zu sein als hoch ein (Abb. 15) und viele wissen nicht genau, wie sie am besten reagieren sollten, falls sie selbst mal betroffen wären (Abb. 23 & Abb. 31). Gleichzeitig gibt es hierzulande bereits eine beträchtliche Zahl an Betroffenen – 14 Prozent wurden schon online belästigt (Abb. 25) und rund 15 Prozent haben schon einmal durch einen Cyberbetrug Geld verloren (Abb. 18). Die Betroffenen berichten oft von emotionaler Belastung (Abb. 21 & Abb. 29) – zur Polizei gehen aber nur wenige und so finden viele Vorfälle nie Eintrag in die offizielle Statistik. Die Ergebnisse dieses Kapitels deuten darauf hin, dass es in der Bevölkerung Bedarf nach mehr Informationen zu Risiken und Handlungsoptionen zum Thema Cyberdelikte gibt.

# Internetnutzung von Kindern

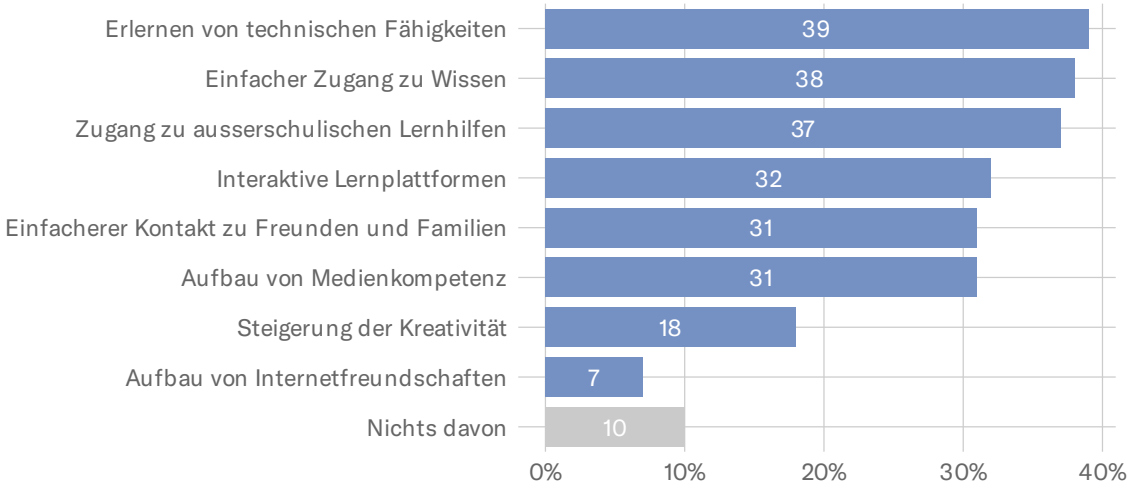
Die Schweizer Bevölkerung nimmt Gefahren im Internet deutlich wahr, fühlt sich aber in ihrem Umgang damit grundsätzlich sicher. Doch wie sieht es bei Kindern aus? Ab wann, wie und was sie im Internet konsumieren, sorgt immer wieder für Diskussionen. Dieses Kapitel beleuchtet die Einschätzungen der Bevölkerung – insbesondere von Eltern – zur Sicherheit von Kindern im Internet.

## 4.1 CYBERMOBBING ALS GRÖSSTES RISIKO FÜR KINDER

Wie bei Erwachsenen hat das Internet auch den Alltag von Kindern stark verändert und in einigen Bereichen vereinfacht. Besonders geschätzt werden von der Schweizer Bevölkerung in diesem Zusammenhang die vielfältigen Lerneffekte des Internets – etwa das Erlernen technischer Fähigkeiten (39 %), der einfache Zugang zu Wissen (38 %) sowie die mögliche Verwendung von Lernhilfen und -plattformen (37 % bzw. 32 %) (Abb. 32). Zudem erleichtert das Internet den sozialen Austausch mit Freunden und Familie. Immerhin 10 Prozent der Bevölkerung sieht jedoch keine der genannten Punkte als Vorteile einer Internetnutzung von Kindern.

Vorteile von Online-Plattformen für Kinder (Abb. 32)

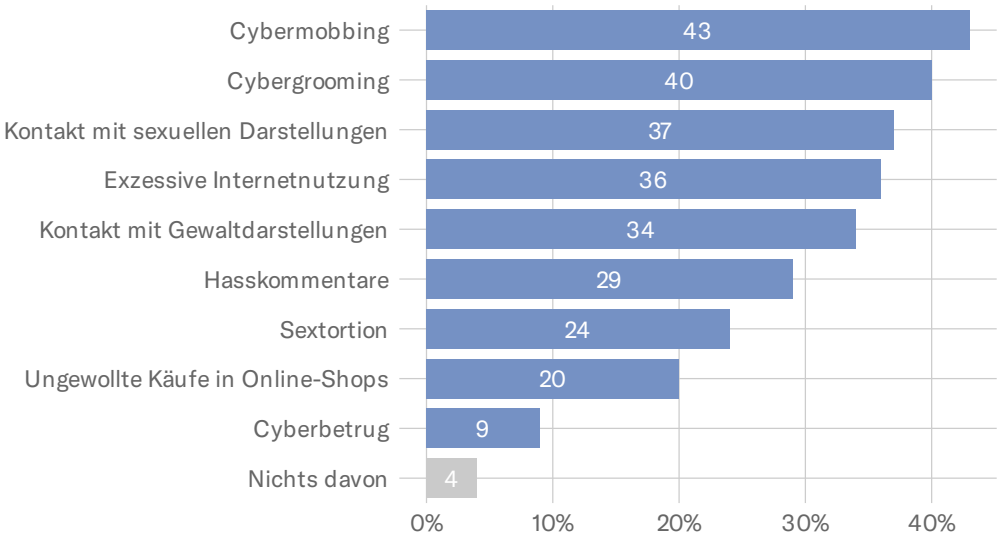
«Was sehen Sie als die grössten Vorteile für Kinder bei deren Nutzung von Online-Plattformen?»




Klar ist: die Nutzung des Internets bringt für Kinder auch gewisse Risiken mit sich. Besonders beim Thema Cybermobbing sorgen sich viele Personen (Abb. 33): Rund 43 Prozent der Befragten sehen darin eine der grössten Herausforderungen für Kinder im Internet. Auch Cybergrooming – die gezielte Manipulation von Kindern zu sexuellen Zwecken (40%) – sowie der Kontakt mit sexuellen Inhalten (37%) werden als Gefahren wahrgenommen. Ein weiterer bekannter Diskussionspunkt, die exzessive Nutzung von Internet bei Kindern, wird von über einem Drittel der Befragten als gewichtige Herausforderung angesehen.

Herausforderungen bei Online-Plattformen für Kinder (Abb. 33)

«Was sehen Sie als die grössten Herausforderungen für Kinder bei deren Nutzung von Online-Plattformen?»



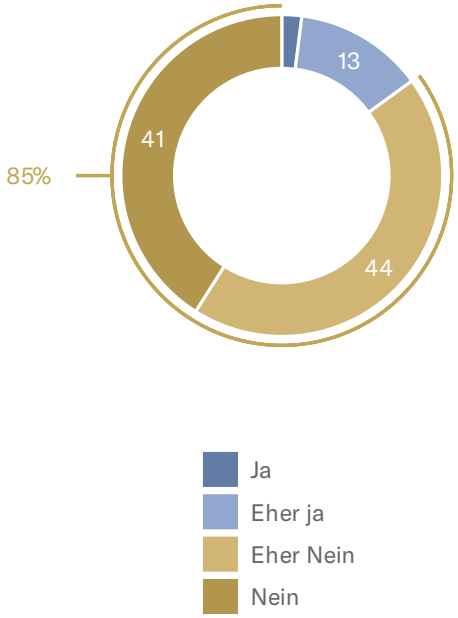

Es sind vor allem Belästigungsdelikte die als hohe Herausforderungen für Kinder im Internet wahrgenommen werden, die Gefahr von Cyberbetrug und ungewollten Einkäufen wird deutlich geringer eingeschätzt (9% und 20%).

# Eine Mehrheit glaubt Kinder sind zu wenig über Gefahren im Internet aufgeklärt.

Herausforderungen – auch ausserhalb vom Internet –gibt es für Kinder viele. Wenn eine angemessene Aufklärung über die Gefahren vorliegt, dann können diese auch vermindert werden. Doch die Abbildung 34 zeigt, dass eine deutliche Mehrheit (85%) glaubt, dass Kinder zu wenig über Sicherheitsrisiken auf Online-Plattformen informiert sind. Doch wenn das Wissen fehlt – wie kann ein sicherer Umgang mit dem Internet dennoch gefördert werden?

Informationsstand zu Online-Sicherheitsrisiken (Abb. 34)

«Sind Sie der Meinung, dass Kinder und Jugendliche heutzutage ausreichend über Sicherheitsrisiken auf Online-Plattformen informiert sind?»

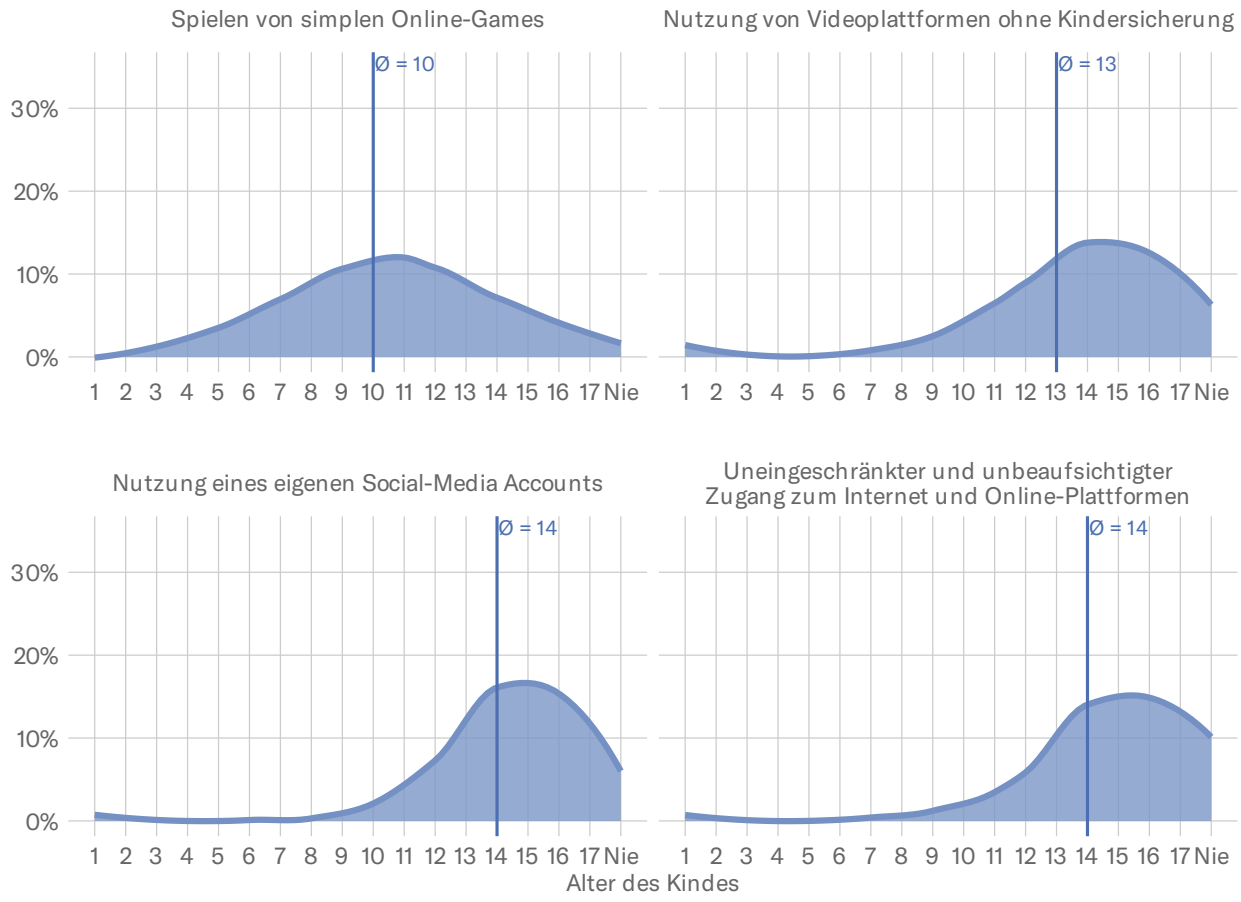



Eine mögliche Massnahme ist die Festlegung von Mindestalter-Grenzen. Abbildung 35 zeigt, dass Kinder – gemäss den Befragten – mit den meisten Online-Aktivitäten erst im Teenageralter beginnen sollten. Das Spielen von Online-Games wird mit einem durchschnittlich genannten Mindestalter von 10 Jahren am frühesten akzeptiert. Für andere Aktivitäten wie die Nutzung von Videoplattformen, eigene Social-Media-Accounts oder uneingeschränkten Internetzugang plädiert die Mehrheit sogar für ein Mindestalter von 14 Jahren oder höher. Ein kleiner Anteil der Befragten ist jeweils auch der Meinung, dass mit diesen Online-Aktivitäten im Kindesalter gar nicht begonnen werden sollte. Die Realität sieht aber anders aus: Bereits im Primarschulalter nutzen eine überwiegende Mehrheit der Kinder Soziale Medien oder Surfen auf Youtube.[11]

[11] ZHAW 2021: Ergebnisbericht zur MIKE-Studie 2021

Angemessens Alter für verschiedene Internetaktivitäten (Abb. 35)

«Ab welchem Alter halten Sie es für angemessen, dass Kinder mit den folgenden Aktivitäten beginnen?»

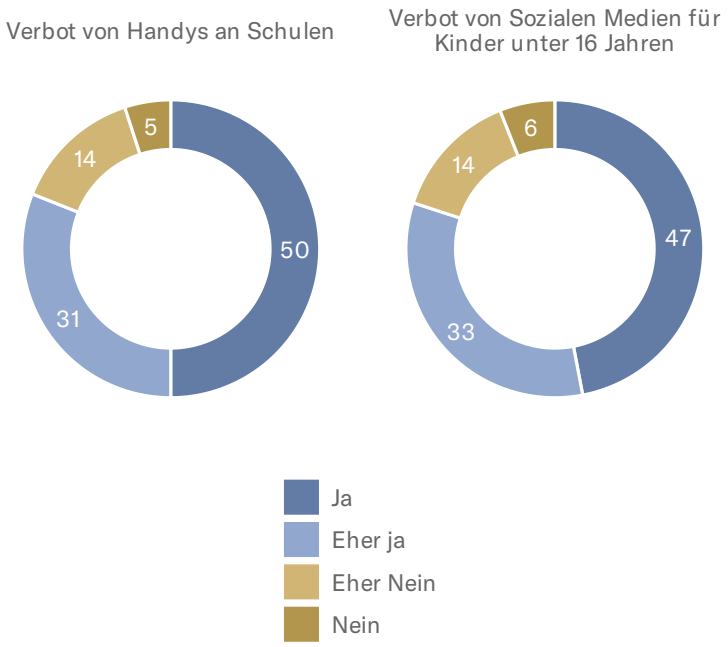



## 4.2 KLARE MEHRHEIT FÜR VERBOT VON SOZIALEN MEDIEN FÜR KINDER

Die oft diskutierte Idee, den Zugang zu Online-Plattformen für Kinder einzuschränken, findet breite Unterstützung: 80 Prozent der Befragten befürworten ein Verbot Sozialer Medien (z.B. Facebook, X / Twitter, Instagram, TikTok) für Kinder unter 16 Jahren. Fast ebenso hoch ist die Zustimmung für ein Handyverbot an Schulen (Abb. 36). Dies deutet auch auf ein Bedürfnis für Massnahmen zum Schutz von Kindern in der Online-Welt hin.

Handyverbot an Schulen und Social-Media Verbot für Kinder (Abb. 36)

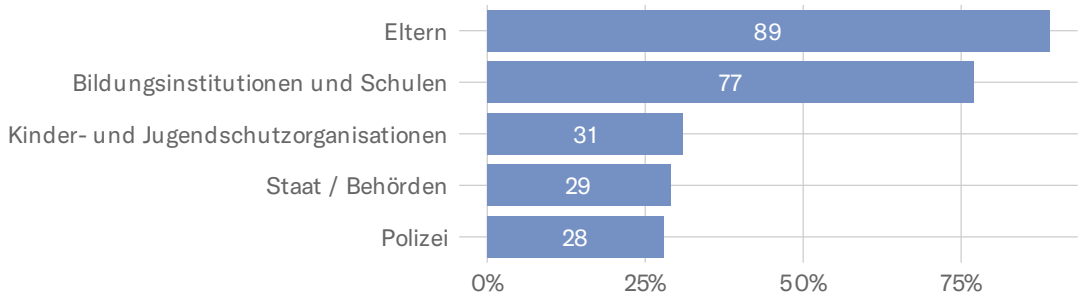
«Befürworten Sie ein generelles Verbot von Handys an Schulen?» und «Befürworten Sie ein Verbot von Social-Media-Plattformen für Kinder unter 16 Jahren?»




Doch wer ist für die Aufklärung von Kindern zu Sicherheitsrisiken im digitalen Raum verantwortlich? Wie Abbildung 37 zeigt, sieht die Bevölkerung primär die Eltern in der Pflicht (89%). Zudem finden 77 Prozent, dass die Aufklärung auch eine Sache der Schulen und Bildung ist. Jeweils ein Drittel der Befragten spricht sich für eine Beteiligung von Kinder- und Jugendschutzorganisationen, dem Staat oder der Polizei aus. Diese Einschätzungen zeigen die Meinungen klar: Die Sensibilisierung sollte zu Hause beginnen und allenfalls von zuständigen Institutionen unterstützt werden.

Verantwortung für Sicherheitsaufklärung (Abb. 37)

«Wer ist Ihrer Meinung nach verantwortlich dafür, Kinder und Jugendliche über solche Sicherheitsrisiken zu informieren?»



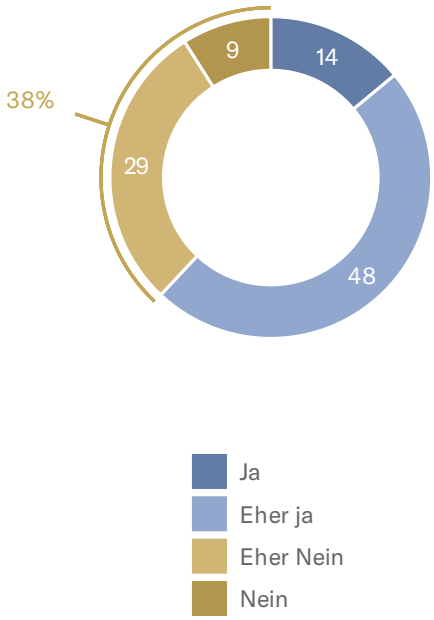

## 4.3 SICHERHEIT VON KINDERN IM INTERNET ÜBERFORDERT VIELE ELTERN

Die Ergebnisse verdeutlichen das Bedürfnis, Kinder besser über Gefahren im Internet zu informieren und die Aufklärung liegt in den Augen der Befragten bei den Eltern. Doch eine gerechte Aufklärung über Sicherheitsrisiken im Internet ist keine einfache Aufgabe – nicht zuletzt, weil sich der digitale Raum und die damit verbundenen Herausforderungen wandeln.

Die meisten Eltern von minderjährigen Kindern fühlen sich dieser Aufgabe aber gewachsen: 62 Prozent geben an sich in der Lage zu fühlen ihre Kinder ausreichend vor Cyberrisiken zu schützen (Abb. 38). Rund ein Drittel der Eltern gibt hingegen an, sich nicht in der Lage zu sehen, ihre Kinder ausreichend schützen zu können.

Schutz der eigenen Kinder vor Cyberrisiken (Abb. 38)

«Fühlen Sie sich in der Lage, Ihr Kind ausreichend vor Cyberrisiken zu schützen?» – Nur Eltern mit minderjährigen Kindern über 5 Jahren (N=250)




Familiäre Regeln oder Verbote können helfen, die sichere Nutzung von Online-Plattformen zu gewährleisten. Doch die Umsetzung solcher Regeln fällt vielen Eltern schwer. Äussere Einflüsse wie sozialer Druck unter Kindern, der Wunsch, beim Internetsurfen dazuzugehören, oder die fehlende vollständige Kontrolle über die Internetaktivitäten von Kindern können diese Aufgabe erschweren.

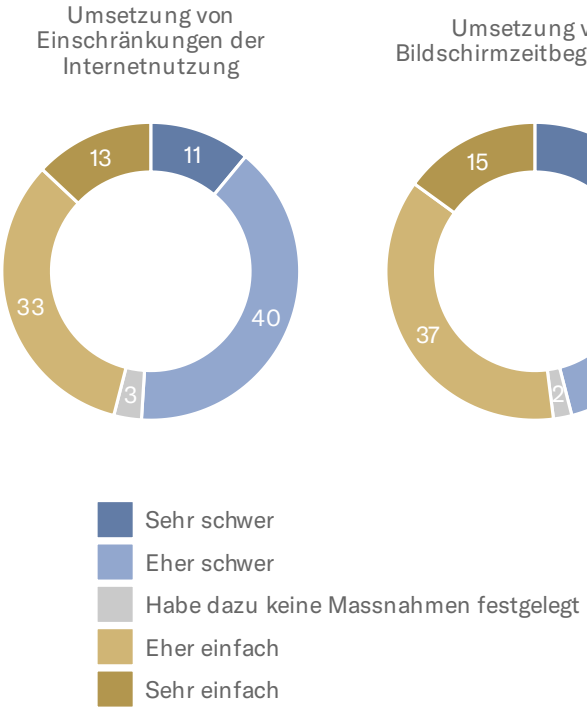
# 97 Prozent der Eltern haben Massnahmen zur Internetnutzung festgelegt.

Wie die Abbildung 39 zeigt, haben beinahe alle Eltern mit Kindern über fünf Jahren Massnahmen festgesetzt – sowohl zur Einschränkung von Online-Plattformen als auch zur Bild-

schirmzeit von Kindern. Wiederum empfinden über die Hälfte der Eltern die Umsetzung von Einschränkungen von Internet-Apps als (eher) schwierig. Dies sogar tendenziell etwas schwieriger als eine Bildschirmzeitbegrenzung, bei der 46 Prozent der Eltern Mühe haben, sie bei ihren Kindern umzusetzen.

Umsetzung von Massnahmen zur sicheren Internetnutzung von Kindern (Abb. 39)

«Wie schwer fällt es Ihnen, Massnahmen (z.B. ein Verbot oder Einschränkungen von Online-Plattformen oder Apps) umzusetzen, um die sichere Nutzung des Internets durch Ihr Kind zu gewährleisten?» und «Wie schwer fällt es Ihnen, Massnahmen umzusetzen, um die Bildschirmzeit von Ihrem Kind auf digitalen Geräten zu begrenzen?» – Nur Eltern mit minderjährigen Kindern über 5 Jahren (N=254)

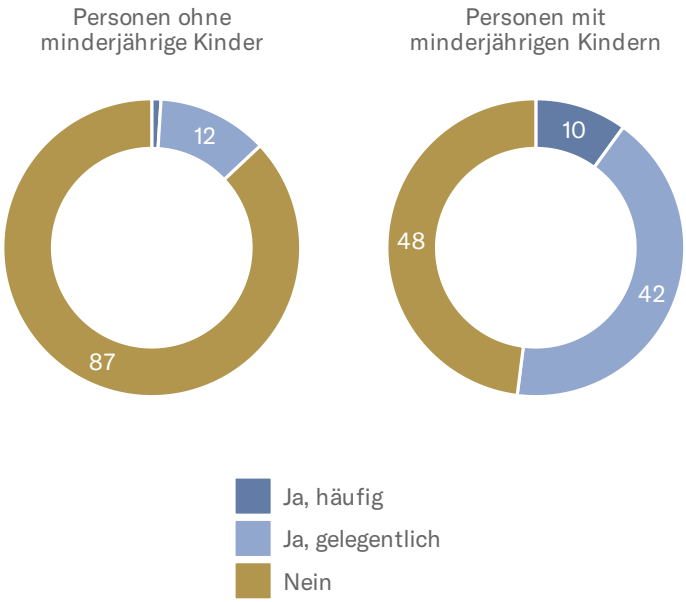



Dass Regeln nicht immer einfach umzusetzen sind und oft Konfliktpotenzial beinhalten, zeigt auch die Abbildung 40. So hat über die Hälfte der Eltern mit minderjährigen Kindern zumindest gelegentlich zuhause Streit über die Dauer der Bildschirmnutzung (52%). Im Vergleich dazu sind Konflikte bei Personen,

die keine minderjährigen Kinder haben, viel seltener: 87 Prozent trägt hierzu zuhause nie Diskussionen aus.

Konflikte über Bildschirmzeit (Abb. 40)

«Gibt es bei Ihnen zuhause Konflikte bezüglich der Dauer der Bildschirmzeit?»




Wie Eltern mit der Internetnutzung ihrer Kinder umgehen sollen, sorgt also nicht nur für Unsicherheit, sondern auch für Konflikte am Familientisch. Die Gefahren im Internet für Kinder werden von Eltern wahr- und ernstgenommen. Entsprechend haben fast alle Eltern gewisse einschränkende Massnahmen für die Online-Aktivitäten ihrer Kinder festgelegt (Abb. 39). Allgemein kann gesagt werden, dass nicht nur Eltern Herausforderungen für Kinder im Internet erkennen, sondern die gesamte Bevölkerung in der Schweiz. Dabei sticht heraus, dass vor allem Belästigungsdelikte wie Cybermobbing oder Cybergrooming als eine hohe Herausforderung wahrgenommen werden (Abb. 33). Mögliche Massnahmen, wie beispielsweise ein Verbot sozialer

Medien für unter 16-Jährige, in denen Cybermobbing besonders verbreitet ist, finden in der Bevölkerung klare Unterstützung (Abb. 36).

# Datenerhebung und Methodik

Die Daten wurden zwischen dem 26. Februar und dem 10. März 2025 erhoben. Die Grundgesamtheit der Befragung bildet die sprachintegrierte Wohnbevölkerung aus der Deutschschweiz und der französischsprachigen Schweiz ab 18 Jahren. Die Befragung erfolgte online. Die Teilnehmenden wurden über das Online-Panel von Sotomo und Bilendi rekrutiert. Befragt wurden ausschliesslich volljährige Personen. Nach Bereinigung und Kontrolle der Daten konnten die Angaben von 1706 Befragten für die Auswertung verwendet werden.

Da sich die Teilnehmenden der Umfrage selbst rekrutieren (opt-in), ist die Zusammensetzung der Stichprobe nicht von vornherein repräsentativ für die Grundgesamtheit. Um repräsentative Resultate zu erhalten, wird den Verzerrungen in der Stichprobe mittels statistischer Gewichtungsverfahren entgegengewirkt. Zu den Gewichtungskriterien gehören Geschlecht, Alter, Bildung, politische Orientierung, Sprachregion und Elternschaft von minderjährigen Kindern. Dieses Vorgehen gewährleistet eine hohe soziodemografische Repräsentativität der Stichprobe. Für die vorliegende Gesamtstichprobe beträgt das 95-Prozent-Konfidenzintervall (für 50 Prozent Anteil) +/-2.4 Prozentpunkte.

SOTOMO