gfs-zürich
MARKT- & SOZIALFORSCHUNG

Schlussbericht 2019:

Sicherheit im Internet

Repräsentative Befragung der Deutsch- und Westschweizer Bevölkerung

Studie im Auftrag von:

ICTswitzerland, Andreas Kaelin
Information Security Society Switzerland ISSS, Umberto Annino
Schweizerische Akademie der Technischen Wissenschaften SATW, Nicole Wettstein
Swiss Internet Security Alliance SISA, Daniel Nussbaumer
SwissICT, Christian Hunziker
SWITCH, Martin Leuthold
Informatiksteuerungsorgan des Bundes ISB, Daniel Rudin

gfs-zürich, Markt- und Sozialforschung

Karin Mändli Lerch (Projektleitung)

Zürich, 18. März 2019

SCHWEIZER MARKTFORSCHUNG
Verband Schweizer Markt- und Sozialforschung
Mitglied swiss interview institute®

Riedtlistrasse 9
CH 8006 Zürich

Tel. +41 44 360 40 20

E-mail: gfs@gfs-zh.ch
Internet: www.gfs-zh.ch

Inhaltsverzeichnis

1 Management Summary

Vom 25. Januar bis 15. Februar 2019 führte das Markt- und Sozialforschungsinstitut gfs-zürich 913 bevölkerungsrepräsentative Interviews in der Deutsch- und Westschweiz durch, mit Personen, die zumindest ein internetverbundenes Gerät besitzen. Es galt dabei, die Kenntnisse und Gefahreneinschätzung von Cyberrisiken zu ermitteln.

Sicherheit im Internet
gfs-zürich, Karin Mändli Lerch
Veröffentlicht: 28. März 2019

Telefonische Mehrthemenbefragung
n=913 (Basisstichprobe: n=1001)
Vertrauensintervall: +/- 3.3 %
(bei einer Irrtumswahrscheinlichkeit von 5 % und einer Verteilung von 50 / 50)
Random-Quota-Stichprobe

Zu diesem Bericht
Die Inhalte des vorliegenden Berichts beziehen sich auf Frauen und Männer. Aus Gründen der besseren Lesbarkeit wird jedoch die männliche Form für die Personenbezeichnungen gewählt. Die weibliche Form wird dabei stets mitgedacht. Eine Ausnahme bilden die Inhalte, die ausdrücklich auf Frauen bezogen werden.

1.1 Wissensstand und Informationsquellen

Eine deutliche Mehrheit der Befragten (59 %) beurteilt den eigenen Informationsgrad als eher oder sehr gut. Jüngere Befragte (18-39 Jahre: 65 %) und Männer (64 %) schätzen sich selbst dabei als besser informiert ein als dies die anderen Gruppen tun (40-64 Jahre: 56 %, 65+ Jahre: 49 %, Frauen: 54 %). Am tiefsten schätzen sich die Befragten über 65 Jahren ein (50 % eher/sehr tiefer Informationsgrad).

Ihre Informationen zur Sicherheit im Internet beziehen die Befragten in erster Linie aus ihrem persönlichen Umfeld wie Freunde, Bekannte, Familie (41 %) oder den Arbeitskollegen (19 %). Medien werden deutlich weniger als Quelle genannt (neue Medien 28 % bzw. klassische Medien 27 %).

1.2 Sicherheitsgefühl und Betroffenheit

Informationsgrad und Sicherheitsgefühl haben nur bedingt miteinander zu tun; so fühlen sich Personen mit tiefem Informationsgrad trotzdem sicher (67 %), während sich auch einige Personen mit hohem Informationsgrad unsicher fühlen (11 %).

Generell ist das Sicherheitsgefühl sehr hoch, 80 % beurteilen sich als eher oder sehr sicher. Der Anteil an Unsicheren ist bei den über 65-jährigen (32 %) und den wenig Informierten (31 %) am höchsten.

Was die Unsicheren am meisten befürchten, ist ein Datenverlust bzw. -diebstahl (51 %) sowie der Missbrauch von persönlichen Daten (43 %).

Die Befragten, die sich eher oder sehr sicher fühlen, begründen dies mit ihren technischen Sicherheitslösungen (43 %) und damit, dass sie nicht auf gefährliche Seiten gehen (36 %).

Dem gegenüber steht die hohe Betroffenheitszahl: Rund jede siebte Person (15 %) war schon einmal von einem Cyberangriff betroffen, welcher entweder einen finanziellen Schaden angerichtet hat, viel Mühe für die Bereinigung oder emotional sehr zu schaffen gemacht hat. Hochgerechnet auf die Grundgesamtheit bedeutet dies rund eine Million betroffener Schweizerinnen und Schweizer.

1.3 Angriffserkennung und Supportstellen

Nach Anzeichen für einen Cyberangriff gefragt, antworten rund zwei Fünftel der Befragten (43 %), dass ihre technische Schutzlösung wie z.B. ein Antivirusprogramm Alarm geben würde. Rund ein Drittel (34 %) wird misstrauisch, wenn der Computer sich komisch verhält oder langsamer wird. Durchschnittlich nennen die Befragten 1.6 solcher Alarmzeichen, Männer (1.7), Junge (1.7) und Westschweizer (1.8) etwas mehr als die anderen Subgruppen.

Als Supportstellen, wo die Befragten im Falle eines Angriffs Hilfe holen würden, wird zuerst wieder das persönliche Umfeld (Familie und Freunde: 43 %) genannt. An zweiter Stelle wird das Geschäft genannt, wo man das Gerät gekauft hat (37 %).

1.4 Umsetzung von Schutzmassnahmen

1.4.1 Anwendung von Passwörtern

13 % der Befragten geben an, immer das gleiche Passwort zu benutzen. Hochgerechnet auf die Grundgesamtheit ergibt das rund 870'000 Schweizer, welche sich damit dem Risiko aussetzen, bei einem Passwortdiebstahl gleich mehrfach geschädigt zu werden.

Rund ein Drittel der Befragten (32 %) verwendet dabei Passwörter mit mindestens 10 Zeichen, weitere 39 % wählen zumindest teilweise so lange Passwörter und erhöhen dadurch ihre Sicherheit gegenüber den Personen, welche mit kürzeren Passwörtern arbeiten (25 %).

1.4.2 Schutzmassnahmen

Als häufigste angewendete Schutzmassnahme gegen Cyberangriffe nennen die Befragten mit dem Antivirusprogramm (61 %) eine technische Lösung. Erst mit grossem Abstand folgen als zweite und dritte Schutzmassnahmen zwei Verhaltensregeln, nämlich nicht auf seltsame Links zu klicken und Mails mit unbekanntem Absender genau zu prüfen bzw. zu löschen (je 27 %).

1.4.3 Sicherheit des Computers vs. Handy

Fast die Hälfte der Befragten (46 %) kümmert sich mehr um die Internetsicherheit des Computers als des Handys (43 % schenken beiden Geräten gleich viel Aufmerksamkeit bezüglich Sicherheit).

1.4.4 Durchführung von Updates

Softwareupdates werden von rund vier Fünfteln der Befragten (79 %) innert einer Woche durchgeführt. Die Höhe dieses Wertes hat die Studienautoren erstaunt und wird zumindest teilweise auf den steigenden Druck zurückzuführen sein, welche die Updates selbst ausüben (Pop-Up Nachrichten, Erinnerungen, Automatisierungen).

1.5 Verbesserung des Informationsgrads

Nur eine knappe Minderheit der Befragten (43 %) wünscht sich, besser über Sicherheit im Internet informiert zu sein. Dieses mehrheitliche Desinteresse dürfte eine Herausforderung sein, wenn die Resilienz gegenüber Cyberangriffen durch Kompetenzerhöhung in der Bevölkerung erreicht werden soll.

1.6 Fazit

Grundsätzlich waren die Studienautoren bezüglich des Wissensstandes in der Bevölkerung positiv überrascht; trotzdem gibt es wichtige Lücken zu schliessen. Der hohe Betroffenheitsgrad steht im Widerspruch zum hohen Sicherheitsgefühl, genauso wie der hohe selbst eingeschätzte Informationsgrad im Widerspruch zu gewissem Verhalten steht (z.B. nur ein Passwort für mehrere Anwendungen zu verwenden).

Die Befragten vertrauen in erster Linie auf ihre technischen Massnahmen, über deren Stand und Aktualität die hier vorliegende Studie aber keine Auskunft geben kann. Verhaltensmassnahmen stehen erst an zweiter Stelle und werden evt. unterschätzt, was in Zeiten von immer professionelleren Phishing-Attacken und Social Engineering eine Gefahr darstellen kann.

2 Ausgangslage und Ziele

2.1 Mandat und Fragestellung

Aufgrund der Befürchtung einer zu tiefen Cyberawareness und damit auch einer zu tiefen Resilienz gegen Cyberangriffe, wurde im Auftrag des Dachverbands ICTswitzerland, der Information Security Society Switzerland ISSS, der Schweizerische Akademie der Technischen Wissenschaften SATW, der Swiss Internet Security Alliance SISA, SwissICT und Switch in Zusammenarbeit mit dem Informatiksteuerungsorgan des Bundes ISB mit einer repräsentativen Bevölkerungsbefragung die Cyberawareness gemessen.

Mittels einer Befragung lässt sich die subjektive Selbsteinschätzung der Befragten messen bzw. kann das erfasst werden, was die Befragten bereit sind, von sich selbst preiszugeben. Bei Wissenstests wie dem folgenden ist deshalb mit einer gewissen Verzerrung gegenüber der Wirklichkeit zu rechnen, weil die Befragten sich vielleicht über- oder unterschätzen, oder weil sie sich keine Blösse geben wollen, etwas nicht zu wissen.

Trotzdem ist die klassische Befragung eine sinnvolle Annäherung an die Wirklichkeit, weil auch das Sicherheits*gefühl* der Befragten, ihre persönliche Einschätzung ihrer Sicherheit und Sicherheitsmassnahmen, sowie ihr Wissen (in offenen Fragen erfasst) über Cyberrisiken von hoher Bedeutung für allfällig geplante Kommunikationsmassnahmen oder politische/gesetzgeberische Massnahmen ist.

2.2 Konzept und Fragebogen

Die hier angewendete Methode der telefonischen Mehrthemenbefragung hat den Vorteil, dass nicht nur am Thema interessierte Personen teilnehmen. Das Interview wurde eingeleitet mit der Information, dass Fragen zu «aktuellen gesellschaftlichen Themen» gestellt würden. Fragte die Zielperson zurück, um welche Themen es ginge, antworteten die gfs-Befrager, dass sie Fragen zu den Themen «Gesundheit, Umwelt und Internet» hätten, was aufgrund der anderen Auftraggeber für die Mehrthemenbefragung auch der Fall war.

Der Fragebogen wurde unter Anleitung von gfs-zürich von einem Fach-Team der an der Studie beteiligten Auftraggeber (siehe Titelblatt) erarbeitet und in die vier Themenbereiche «Wissensstand und Informationsquellen», «Sicherheitsgefühl und Betroffenheit», «Angriffserkennung und Supportstellen» sowie «Umsetzung von Schutzmassnahmen» unterteilt. Die durchschnittliche Interviewdauer lag bei 8.6 Minuten. Der Fragebogen wurde möglichst allgemeinverständlich getextet und wir haben uns auf die verbreitetsten Risiken und Sicherheitsmassnahmen beschränkt.

2.3 Befragung und Stichprobe

Die Befragung wurde vom 25. Januar bis 15. Februar 2019 mit 1001 Personen der Deutsch- und Westschweiz ab 18 Jahren durchgeführt. Daraus ergab sich eine Stichprobe von 913 Personen, welche mindestens ein mit dem Internet verbundenes Gerät besitzen.

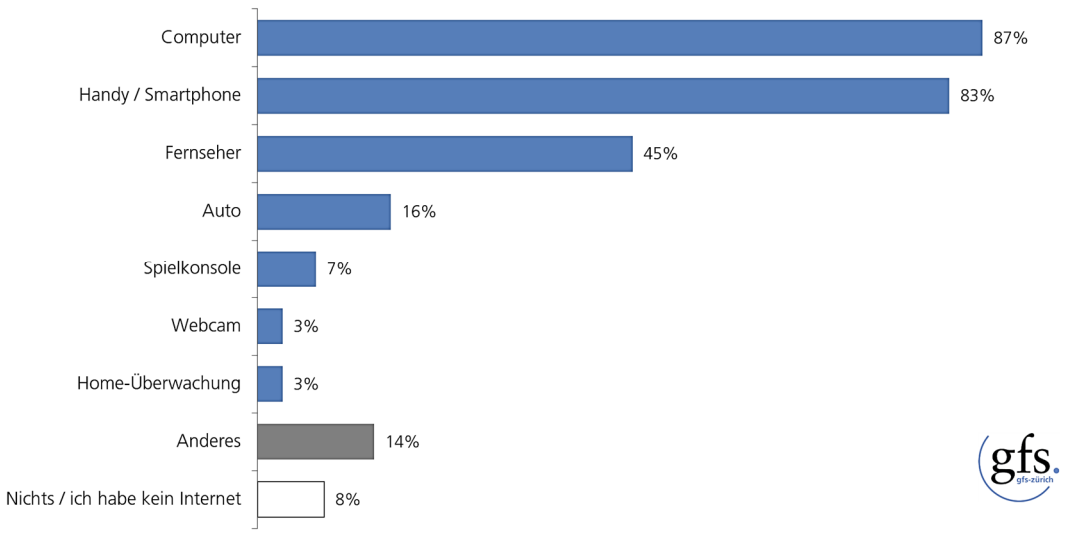
Grundgesamtheit:	Erwachsene Bevölkerung in der Deutsch- und Westschweiz ab 18 Jahren
Stichprobe:	n=1001 Basisstichprobe, davon n=913 mit Geräten, die mit dem Internet verbunden sind
Repräsentativität:	Das Vertrauensintervall der befragten Stichprobe (Personen mit Geräten, die mit dem Internet verbunden sind) liegt bei +/- 3.3 % bei einer Sicherheit von 95% (50/50 Verteilung). Die Erhebung zeigt ein repräsentatives Abbild der Deutsch- und Westschweizer Schweizer Bevölkerung, die Ergebnisse sind somit auf die Grundgesamtheit übertragbar.
Methode:	CATI-Mehrthemenbefragung
Stichprobenmethode:	Random-Quota: Zufallsziehung aus den im Telefonbuch enthaltenen Privathaushalten (80 %) sowie zufällig generierte Mobile-Nummern (20 %) in der Deutsch- und Westschweiz, Steuerung mit Quoten nach Sprachregion, Alter und Geschlecht
Quoten:	Geschlecht (♂ 50 %, ♀ 50 %) Alter (18-39 J. 35 %; 40-64 J. 43 %; 65+ J. 22 %) Sprachregion (75 % D-CH; 25 % W-CH)
Gewichtung:	Keine
Befragungszeitraum:	25. Januar bis 15. Februar 2019

Die Adressen stammen zu 80 % aus dem Telefonbuch (Festnetznummern), 20 % wurden zufällig generiert (Mobile Nummern). Die Festnetznummern wurden nach Sprachregion vorgeschichtet, die Quotierung erfolgte gemäss den am Telefon erhobenen Antworten (Alter, Geschlecht).

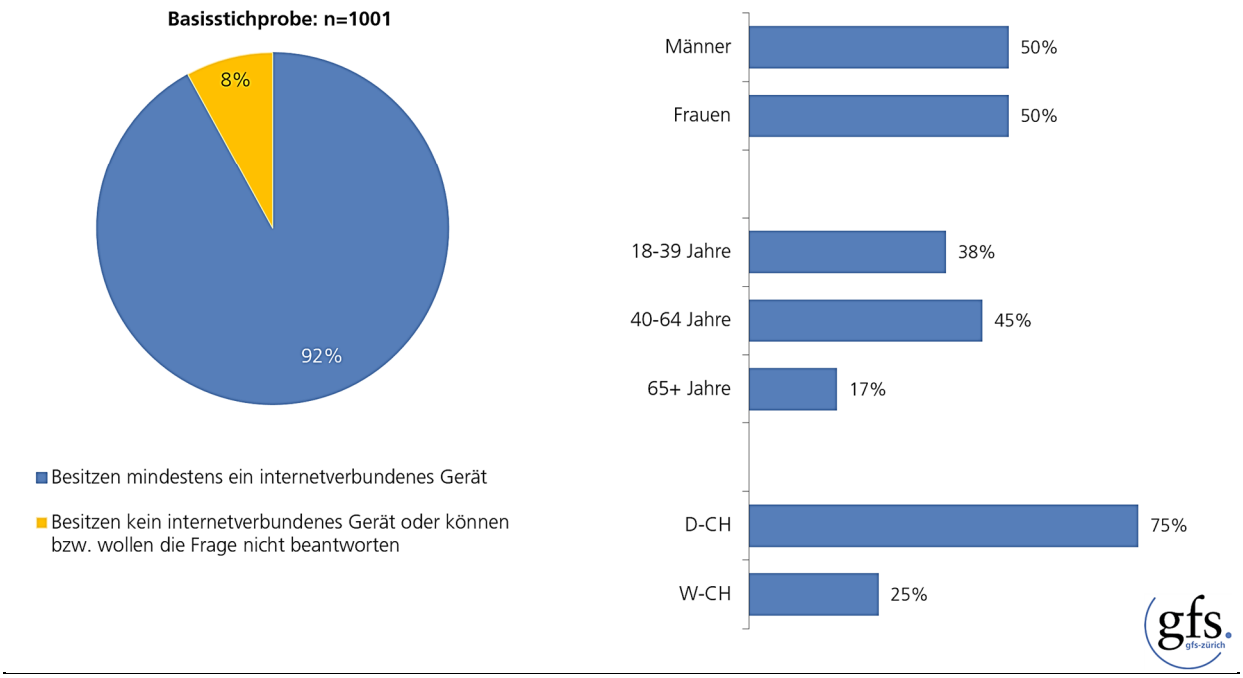
Mit dem Internet verbundene Geräte in den Schweizer Haushalten

1: Nun kommen wir zu ein paar Fragen zum Thema «Sicherheit im Internet». Bitte denken Sie dabei an Ihre Situation zuhause und nicht am Arbeitsplatz.

Heutzutage sind nicht mehr nur Computer und Handy mit dem Internet verbunden, sondern auch Geräte wie z.B. smarte Fernseher, Lautsprecher, das Auto usw. Welche Geräte besitzen Sie, die mit dem Internet verbunden sind? Bitte zählen Sie alle auf, die Ihnen in den Sinn kommen, auch Computer und/oder Handy.
n=1001 (Basisstichprobe) / offene, vorcodierte Frage / Mehrfachnennungen



Rund jede 12. befragte Person (8 %) gab an, über kein internetverbundenes Gerät zu verfügen, und wurde somit für den weiteren Fragebogen nicht mehr berücksichtigt. Daraus ergab sich eine Stichprobe von n=913 mit den nachfolgenden Merkmalen:



Zu beachten ist, dass der Ausschluss dieser 8 % ohne internetverbundenes Gerät sich kaum auf die soziodemografische Verteilung auswirkt. Es ergibt sich lediglich eine minimale Verschiebung zu den zwei jüngeren Altersgruppen. (18-39 Jahre effektiv: 36 %; 40-64 Jahre effektiv: 43 %; 65+ Jahre: 22 %)

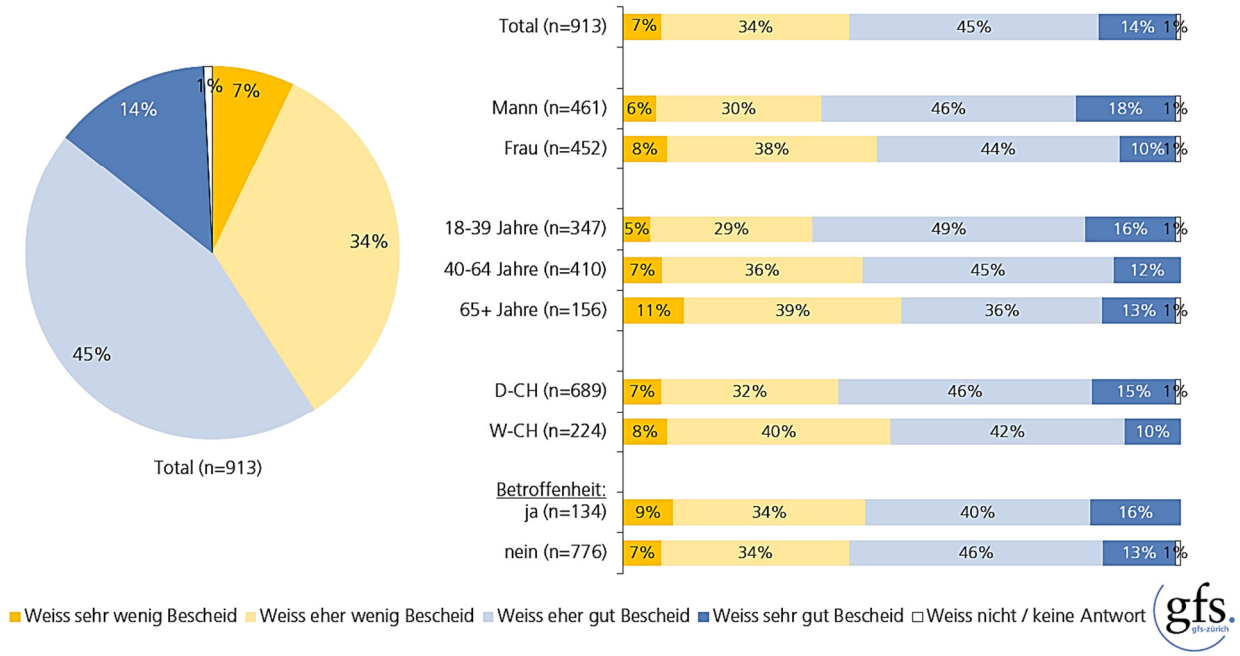
3 Ergebnisse

3.1 Wissensstand und Informationsquellen

3.1.1 Selbsteinschätzung Wissensstand

Als Einstieg in das Thema wurden die Befragten um ihre Selbsteinschätzung bezüglich ihrer Cyberschutz-Kenntnisse gebeten («Wie gut wissen Sie Ihrer Meinung nach darüber Bescheid, wie Sie sich vor Angriffen aus dem Internet schützen können?»). Sie konnten auf einer 4er-Skala antworten:

2: Wie gut wissen Sie Ihrer Meinung nach darüber Bescheid, wie Sie sich vor Angriffen aus dem Internet schützen können?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / eine Antwort



Mit 59 % schätzen deutlich mehr als die Hälfte der Befragten, dass sie sehr oder eher gut Bescheid wissen. Dabei beurteilen sich die Männer (64 %) als kompetenter als es die Frauen (54 %) tun.

Am kritischsten sich selbst gegenüber ist die älteste Altersgruppe (65+), dabei ergibt sich die Regel «je älter, desto selbstkritischer». Knapp die Hälfte der über 65-jährigen (49 %) wählt noch die Skalenwerte «eher gut Bescheid» und «sehr gut Bescheid».

Auch zwischen den Sprachregionen ergibt sich eine unterschiedliche Selbsteinschätzung, so beurteilen sich die Deutschschweizer selbst als besser informiert (61 %) als die Westschweizer (52 %)

Unter «Betroffenheit» sind diejenigen Befragten abgebildet, die (Frage 8a) schon einmal von einem Angriff aus dem Internet betroffen waren und Schaden daraus gezogen haben (= Betroffenheit

«ja», n=134). Betroffene unterscheiden sich in ihrem Informationsgrad nicht signifikant von Nicht-Betroffenen; es ist anzunehmen, dass die entsprechende Erfahrung bei einigen Leuten dazu führt, dass sie ihren Informationsgrad als noch tiefer beurteilen, während andere sich gerade aufgrund der Erfahrung besser informiert fühlen.

3.1.2 Informationsquellen

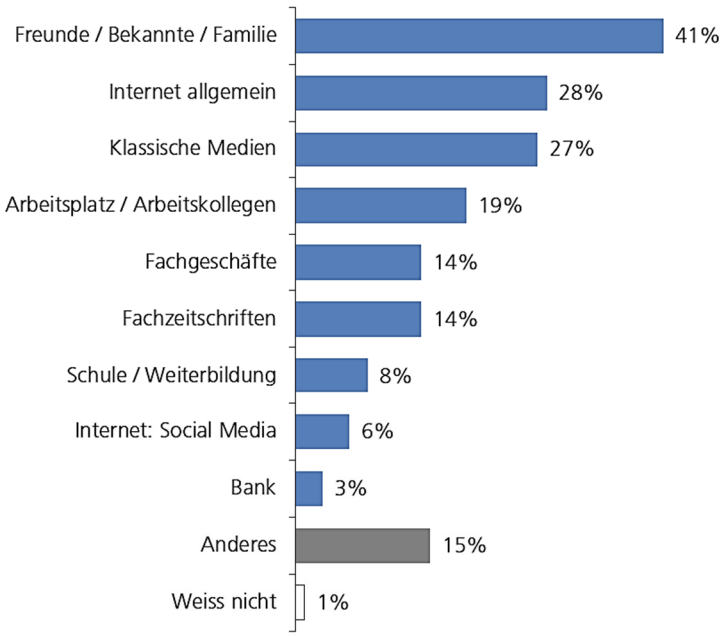
Bei den Informationsquellen bezüglich «Sicherheit im Internet» steht das persönliche Umfeld der Befragten deutlich an erster Stelle; einerseits durch die «Freunde, Bekannte und Familie», die von 41 % der Befragten angegeben werden, andererseits durch «Arbeitsplatz, Arbeitskollegen», welche von weiteren 17 % genannt werden.

An zweiter Stelle folgen die Medien mit dem «Internet allgemein» (28 %) und «Klassische Medien» (27 %). «Social Media», welche wohl als Mischung zwischen persönlichem Umfeld und neuen Medien betrachtet werden können, werden von 6 % der Befragten genannt.

Fachquellen wie Fachgeschäfte (14 %), Fachzeitschriften (14 %), aber auch Banken (3 %), werden erst an dritter Stelle genannt.

Rund jeder zwölfte Befragte (8 %) nennt die Schule bzw. Weiterbildung als Informationsquelle.

3: Woher oder von wem stammen Ihre Informationen zum Thema «Sicherheit im Internet»?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / offene, vorcodierte Frage / Mehrfachnennungen



Im Vergleich zwischen den Altersgruppen fällt auf, dass die Informationen der jüngsten Gruppe (18-39 Jahre) signifikant häufiger aus der Schule / Weiterbildung (13 %) und aus den Social Media (11 %) stammen als bei den anderen beiden Altersgruppen. Die über 65-jährigen hingegen geben als häufigste Informationsquelle die klassischen Medien (46 %) an; dieser Wert unterscheidet sich signifikant von denjenigen der 18-39jährigen (19 %) und den 40-64jährigen (26 %).

Zwischen den Deutsch- und Westschweizern sticht die unterschiedliche Nutzung von Fachzeitschriften als Informationsquelle für Sicherheit im Internet hervor: Knapp ein Drittel der Westschweizer (30 %) geben Fachzeitschriften («Magazines spécialisés») an, aber nur knapp jeder zehnte Deutschschweizer (9 %).

Auch Social Media (17 %) und Banken (8 %) werden in der Westschweiz signifikant häufiger genannt als in der Deutschschweiz (3 % bzw. 1 %), wobei die Westschweizer generell mehr Antworten gaben auf diese Frage (Ø 2.0) als die Deutschschweizer (Ø 1.7).

3.2 Sicherheitsgefühl und Betroffenheit

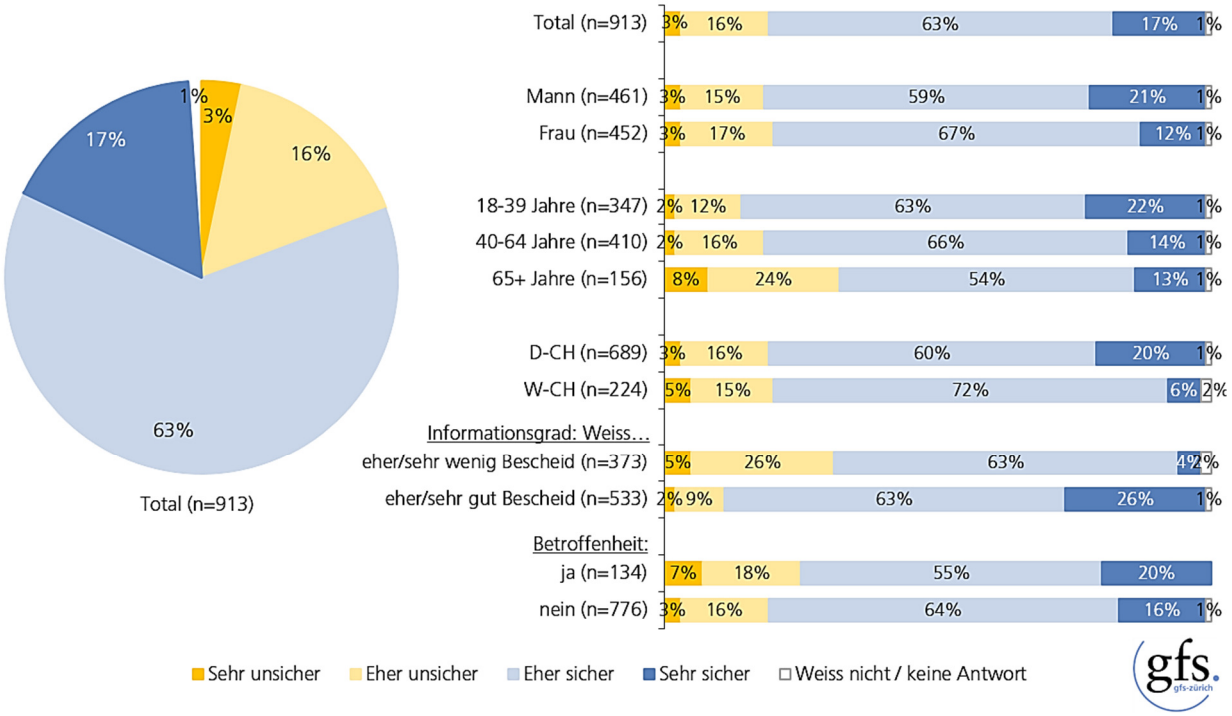
3.2.1 Sicherheitsgefühl im Umgang mit dem Internet

Neben der Selbsteinschätzung zum Informationsgrad wurde auch das Sicherheitsgefühl abgefragt, denn ein tiefer Informationsgrad führt nicht zwingend zu einem tiefen Sicherheitsgefühl. So fühlen sich rund zwei Drittel (67 %) derjenigen Befragten, die sich selbst einen tiefen Informationsgrad attestieren, trotzdem eher oder sehr sicher. Personen mit hohem gefühlten Informationsgrad fühlen sich zwar signifikant sicherer als Personen mit tiefem gefühltem Informationsgrad, aber auch unter ihnen befinden sich 11 % mit einem eher oder sehr tiefen Sicherheitsgefühl.

Alles in allem fühlen sich vier Fünftel der Befragten (80 %) eher oder sehr sicher, nur knapp ein Fünftel der Befragten (19 %) fühlt sich eher oder sehr unsicher.

Auch die von einem Cyberangriff betroffenen Befragten fühlen sich mehrheitlich eher oder sehr sicher (75 %). Das Sicherheitsgefühl sinkt durch Cyberangriffe nur minimal: Der Anteil an sehr unsicheren Befragten steigt durch die Betroffenheit signifikant von 3 % auf 7 %, addiert mit den eher unsicheren Befragten steigen die Werte von 19 % (nicht betroffen) auf 25 % (betroffen).

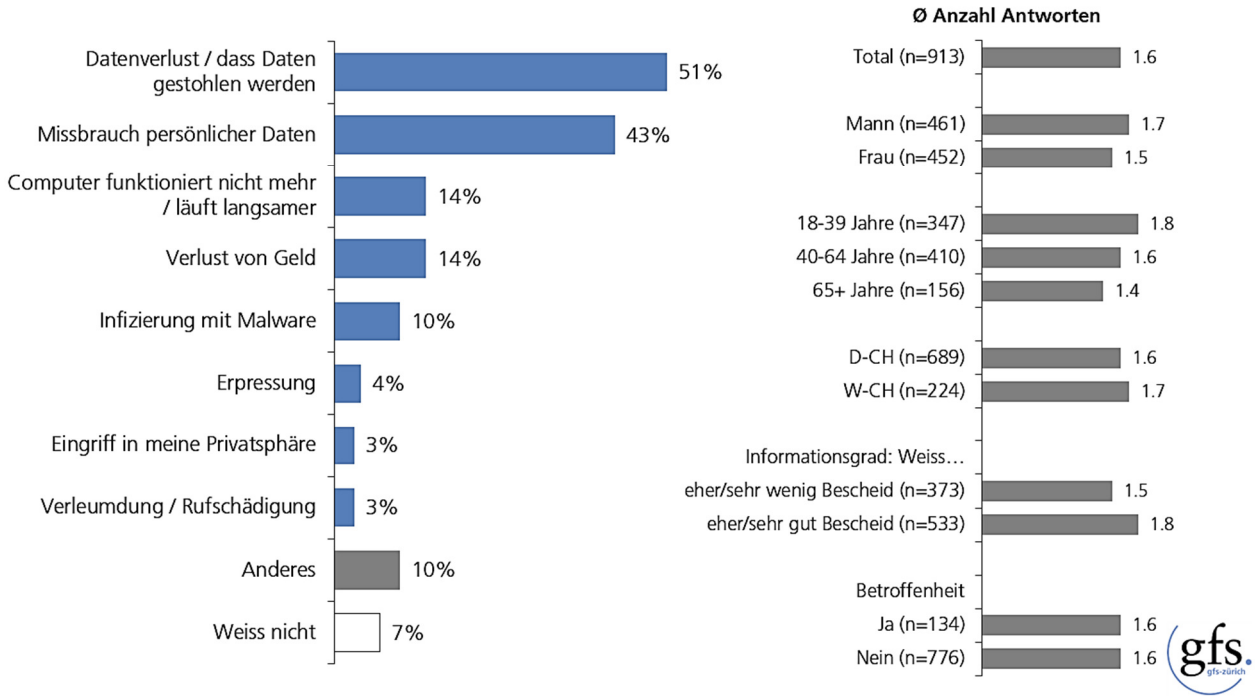
4: Wie sicher fühlen Sie sich im Umgang mit dem Internet?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / eine Antwort



3.2.2 Konkrete Befürchtungen

Die 176 Befragten, die sich (Frage 4) als eher oder sehr unsicher bezeichneten, wurden nach ihren konkreten Befürchtungen gefragt. Dabei erweist sich der Datenverlust resp. -diebstahl (51 %) sowie der entsprechende Missbrauch (43 %) mit Abstand als die grösste Befürchtung.

5: Was befürchten Sie, was passieren könnte?
n=176 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist und fühlt sich im Internet eher oder sehr unsicher / offene, vorcodierte Frage / Mehrfachnennungen



Deutlich seltener genannt wird die Befürchtung, dass der Computer nicht mehr oder nur noch langsam funktioniert (14 %) oder Geld verloren geht (14 %).

Die Befragten äussern durchschnittlich 1.6 konkrete Befürchtungen, wobei Männer (1.7), 18-39jährige (1.8), Westschweizer (1.7) und Personen mit selbst eingeschätztem hohen Informationsgrad (1.8) jeweils etwas mehr unterschiedliche Befürchtungen nennen.

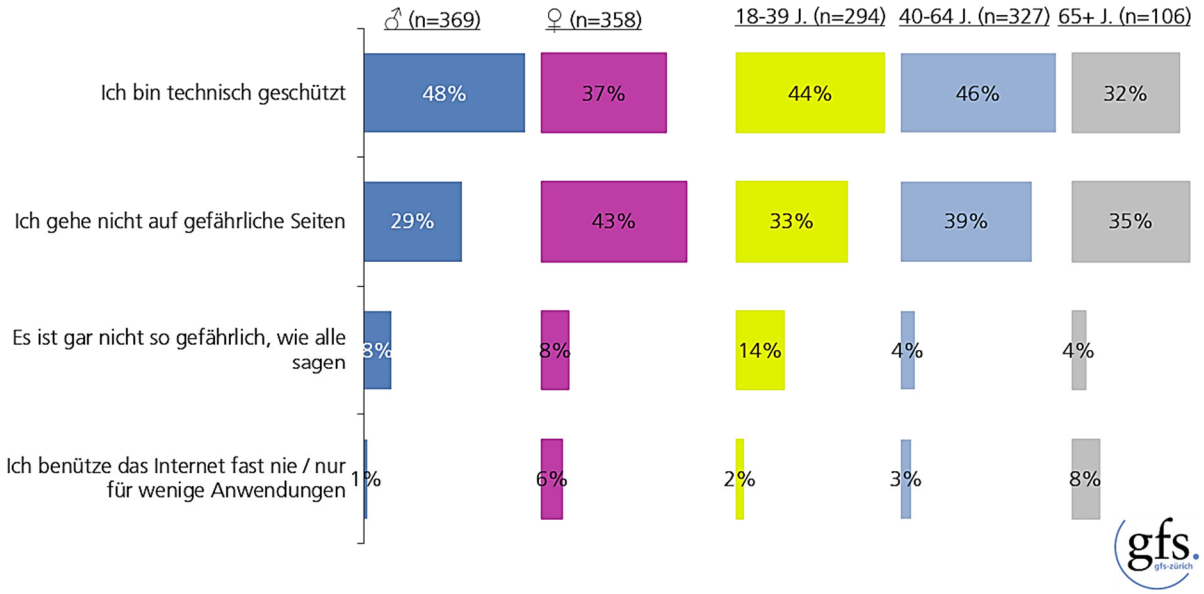
3.2.3 Gründe für das positive Sicherheitsgefühl

Als Hauptgrund für ihre gefühlte Sicherheit nennen die 727 Befragten, die sich eher oder sehr sicher fühlen, ihre technischen Schutzlösungen (43 %). Diese Begründung wird signifikant häufiger von Männern (48 %) genannt als von Frauen (37 %). Letztere nennen dafür den zweiten Hauptgrund signifikant häufiger: Nicht auf gefährliche Seiten zu gehen (Frauen: 43 %, Männer: 29 %).

6: Weshalb fühlen Sie sich sicher?
n=727 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist und fühlt sich im Internet eher oder sehr sicher / offene, vorcodierte Frage / Mehrfachnennungen

Dass das Internet «gar nicht so gefährlich ist, wie alle sagen», ist vor allem die Meinung der 18-39jährigen (14 %), der Westschweizer (11 %) und derjenigen, die gem. Selbsteinschätzung eher oder sehr gut Bescheid wissen (10 %).

6: Weshalb fühlen Sie sich sicher?
n=727 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist und fühlt sich im Internet eher oder sehr sicher / offene, vorcodierte Frage / Mehrfachnennungen



3.2.4 Persönliche Betroffenheit

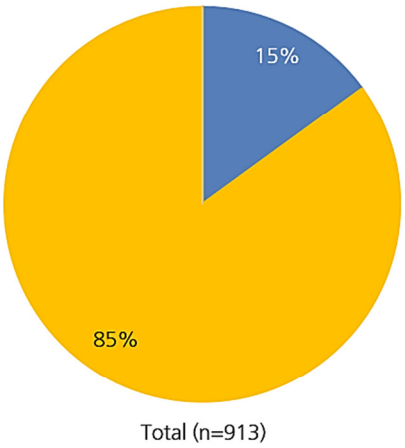
Rund jede siebte Person wurde gemäss eigener Aussage schon einmal durch einen Angriff aus dem Internet geschädigt, wobei es in den Subgruppen keine nennenswerten Unterschiede gibt. Die entsprechende Frage wurde bewusst so formuliert, dass kleinere Ereignisse wie erfolgreich gelöschte Phishing-Mails oder ähnliches hier nicht genannt wurden. Trotzdem beurteilen die Befragten die Angriffe und deren Tragweite unterschiedlich, und bei der nachfolgenden Frage, was konkret passiert sei, wurden 10 von 155 Nennungen als «wahrscheinlich kein Cyberangriff» codiert.

Bei den häufigsten Nennungen handelt es sich um Virus-/Malware-Infizierungen, bei denen die beschriebenen Folgen vom Bereinigen durch eine Virensoftware bis zum Kauf eines neuen Geräts oder der kostenintensiven Bereinigung durch Fachpersonen reichen.

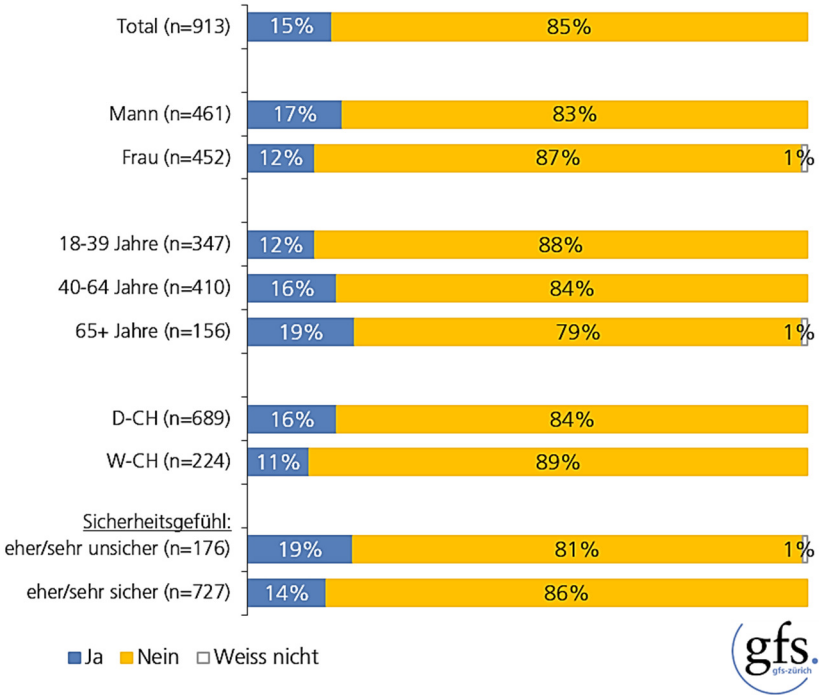
Da die Stichprobe repräsentativ für die erwachsene Deutsch- und Westschweizer Bevölkerung erhoben wurde, lässt sich die folgende Hochrechnung anstellen, mit der von rund einer Million betroffenen Schweizern ausgegangen werden kann:

	Geschädigt durch Cyberangriff:
Prozentualer Anteil in der Stichprobe (n=913):	15 %
Grösse der repräsentierten Grundgesamtheit: (Bevölkerung 18+ der D- und W-CH, Quelle: STATPOP BfS, ständige Wohnbevölkerung nach Alter, Kanton, Bezirk und Gemeinde, am 31.12.2017)	6,667 Mio
Geschätzte Anzahl betroffene Personen:	1,000 Mio
Spannbreite unter Berücksichtigung des Vertrauensintervalls: (bei einem Sicherheitsmass von 95 % bzw. einer Irrtumswahrscheinlichkeit von 5 %)	976'000 - 1,024 Mio

8a: Waren Sie schon einmal von einem Angriff aus dem Internet betroffen, der bei Ihnen entweder einen finanziellen Schaden angerichtet hat, Ihnen viel Mühe für die Bereinigung gemacht hat, oder Ihnen emotional sehr zu schaffen gemacht hat?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist



Total (n=913)



8b: Was ist passiert?
n=134 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / War von einem Angriff aus dem Internet betroffen / offene, vorcodierte Frage / Mehrfachnennungen

3.3 Angriffserkennung und Supportstellen

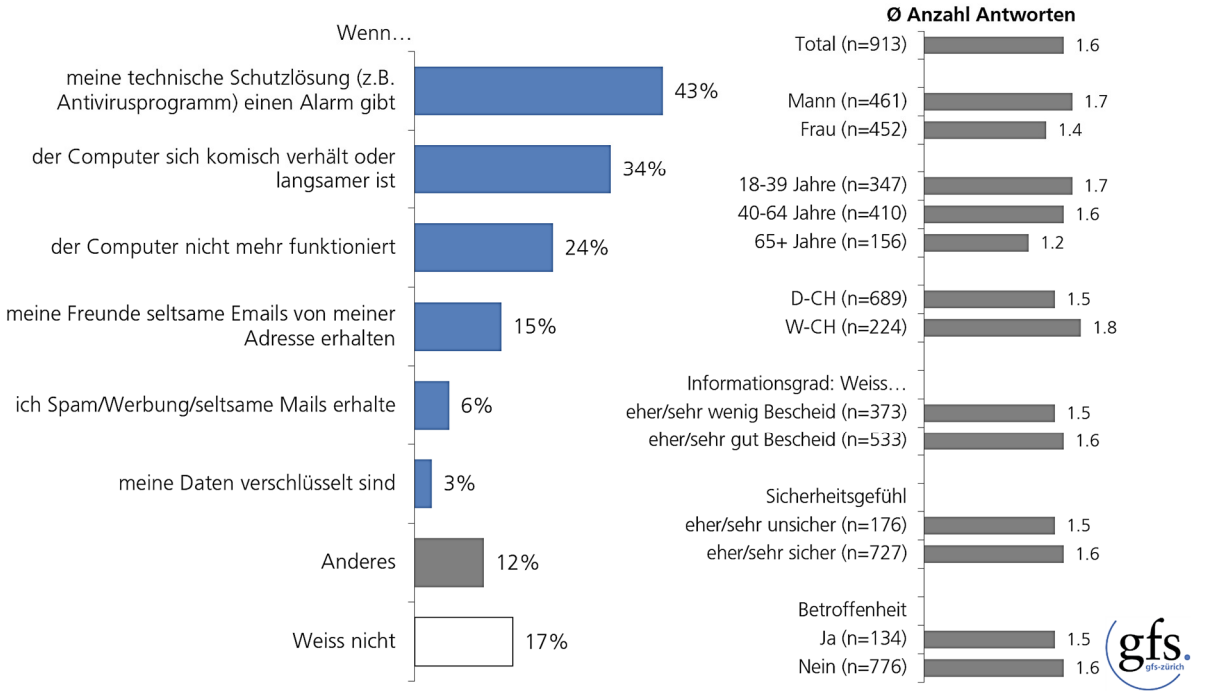
3.3.1 Angriffserkennung

Rund zwei Fünftel der Befragten (43 %) verlässt sich bei der Angriffserkennung auf die technische Schutzlösung, rund ein Drittel (34 %) wird misstrauisch, wenn der Computer sich «komisch verhält» oder langsamer ist. Im Durchschnitt wird die Frage mit 1.6 Antworten beantwortet, wobei gilt: Je jünger die Befragten sind, desto mehr Warnzeichen werden genannt (18-39 Jahre: Ø 1.7, 40-64 Jahre: Ø 1.6, 65+ Jahre: Ø 1.2 Nennungen).

Auch nennen Männer (Ø 1.7) mehr Warnzeichen als Frauen (Ø 1.4) und Westschweizer (Ø 1.8) mehr als Deutschschweizer (Ø 1.5).

Geschätzter Informationsgrad, Sicherheitsgefühl und Betroffenheit haben kaum Einfluss darauf, wie viele Warnzeichen genannt werden.

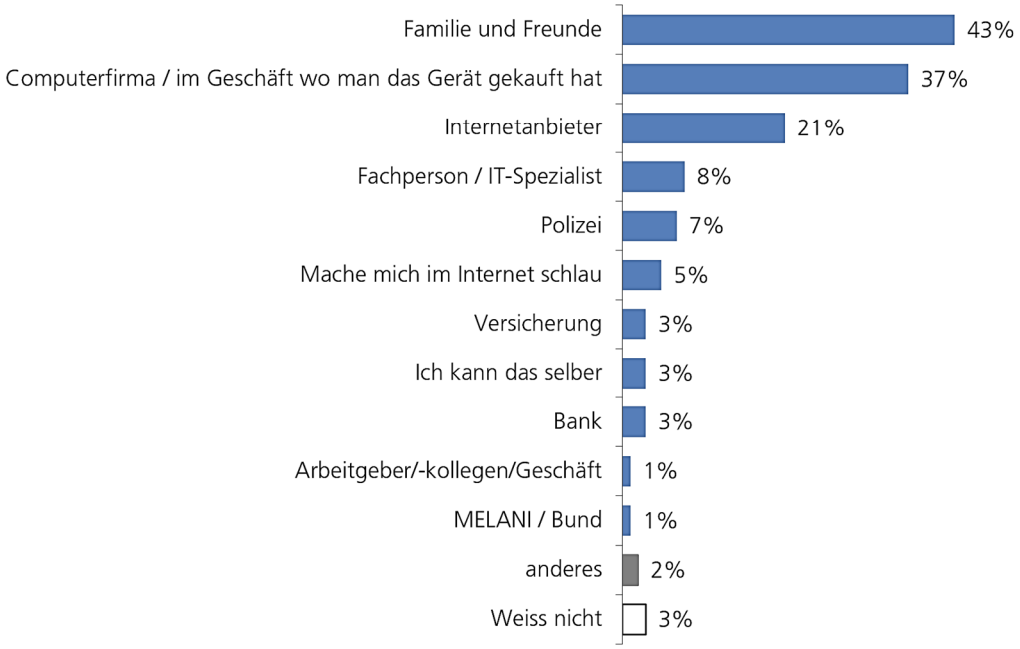
7: Können Sie mir Anzeichen aufzählen, woran Sie an Ihrem Computer erkennen, dass er durch einen Angriff aus dem Internet infiziert wurde?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / offene, vorcodierte Frage / Mehrfachnennungen



3.3.2 Supportstellen

Wie schon bei den Informationsquellen, so werden auch bei den Supportstellen bei Internetangriffen zuerst die Familie und Freunde genannt (43 %), wobei hier die Westschweizer signifikant häufiger antworten (54 %) und diejenigen Befragten, die nach eigener Einschätzung eher oder sehr wenig Bescheid wissen (49 %). Bei den Deutschschweizern (41 %) und bei denjenigen, die eher oder sehr gut Bescheid wissen wollen (40 %), steht das Geschäft, in dem das Gerät gekauft wurde, an erster Stelle.

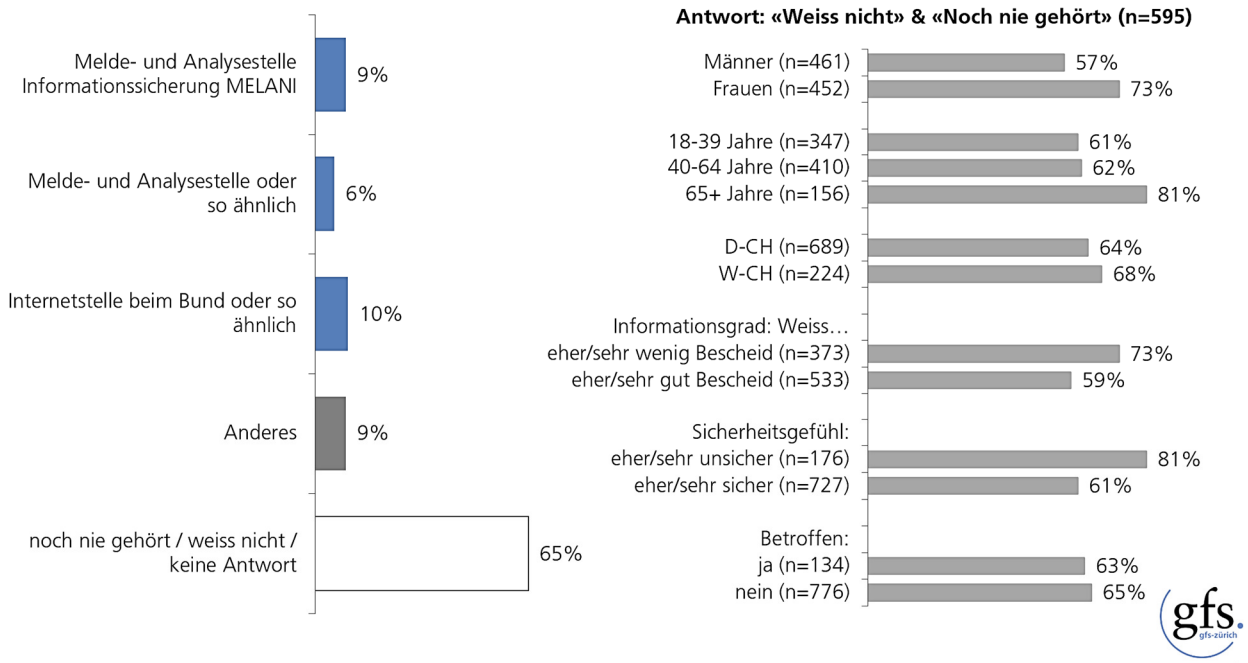
9: Was denken Sie, wo würden Sie sich Hilfe holen, wenn Ihr Computer zuhause durch einen Angriff aus dem Internet infiziert worden wäre?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / offene Frage / Mehrfachnennungen



3.3.3 Awareness MELANI

Wird konkret nachgefragt, wofür dass «MELANI» steht, antwortet ein Viertel der Befragten (25 %) mit einer zumindest teilweise richtigen Beschreibung. Rund zwei Drittel (65 %) jedoch sagen, es gar nicht zu kennen oder noch nie davon gehört zu haben. Dabei handelt es sich vorwiegend um Frauen (73 %), um über 65-jährige (81 %), Personen die ihren eigenen Informationsgrad als tief einschätzen (73 %) und Personen, die sich eher oder sehr unsicher fühlen (81 %). Zwischen von einem Angriff betroffenen und nicht-betroffenen ergibt sich kein signifikanter Unterschied.

10: Was denken Sie, wofür steht «MELANI»?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / offene, vorcodierte Frage / Mehrfachnennungen

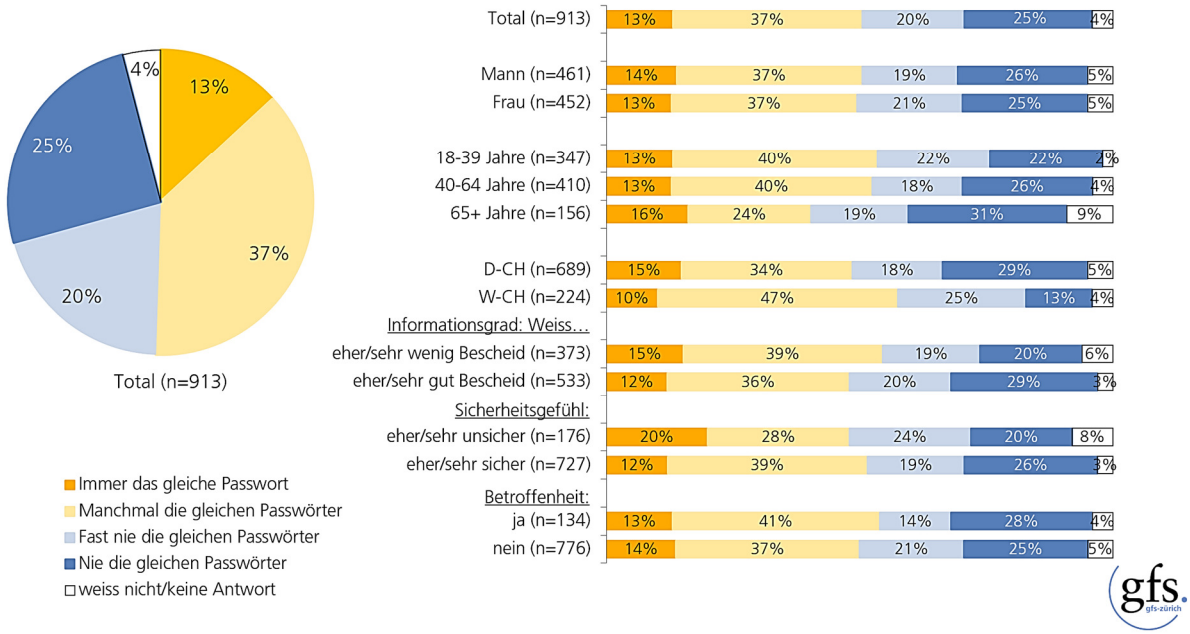


3.4 Umsetzung von Schutzmassnahmen

3.4.1 Anwendung von Passwörtern

Die Verwendung von möglichst sicheren Passwörtern ist eine der wichtigsten Massnahmen für Privatpersonen, um ihre Cybersicherheit zu verbessern. In der Studie wurde nach der Menge, der Länge und der Anzahl unterschiedlicher Passwörter gefragt.

11: Passwörter benötigt man einerseits, um sich am Computer zu Hause anzumelden, aber auch für diverse Dienstleistungen im Internet. Benutzen Sie an verschiedenen solchen Orten ein Passwort mehrfach?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / eine Antwort



Die Hälfte der befragten Personen (50 %) benützt immer oder manchmal das gleiche Passwort und setzt sich damit dem Risiko aus, im Falle eines Passwortdiebstahls bei mehreren statt nur bei einer Anwendung geschädigt zu werden.

Eine Hochrechnung der Personen, welche immer das gleiche Passwort benützen (13 %), auf die erwachsene Deutsch- und Westschweizer Bevölkerung ergibt rund 870'000 Personen, welche sich einem entsprechenden Risiko aussetzen:

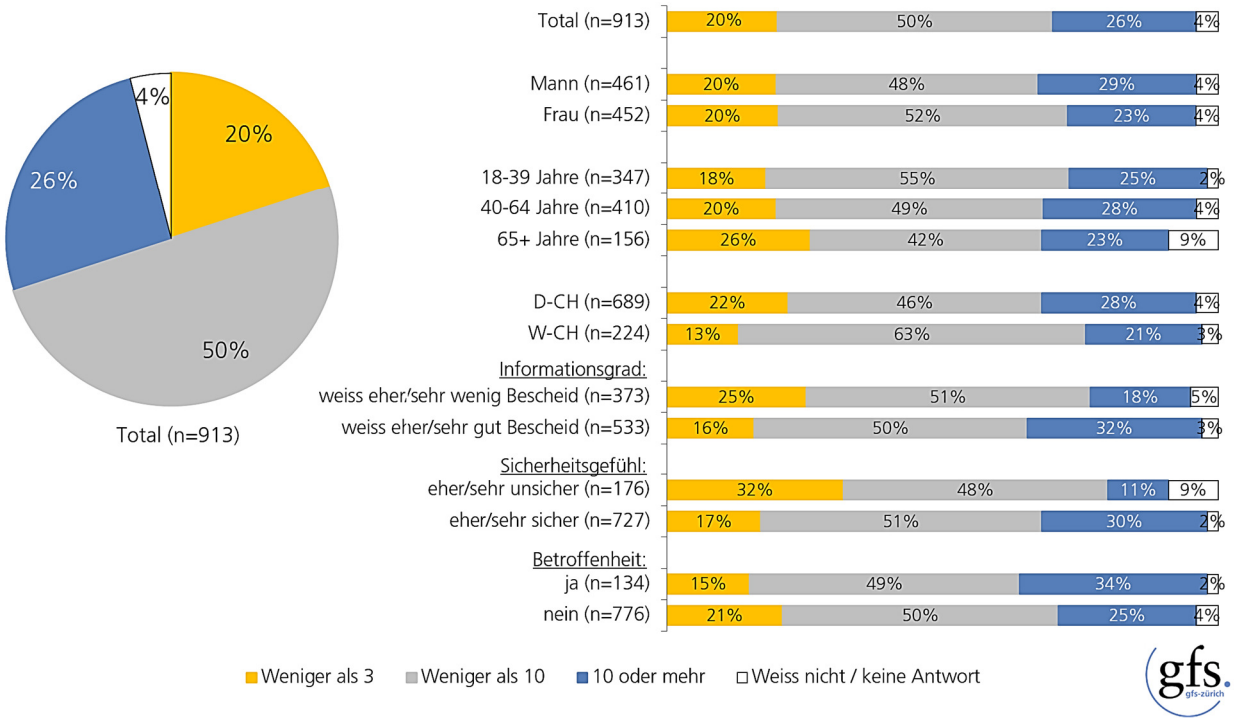
	Benützen immer das gleiche Passwort:
Prozentualer Anteil in der Stichprobe (n=913):	13 %
Grösse der repräsentierten Grundgesamtheit: (Bevölkerung 18+ der D- und W-CH, Quelle: STATPOP BfS, ständige Wohnbevölkerung nach Alter, Kanton, Bezirk und Gemeinde, am 31.12.2017)	6,667 Mio
Geschätzte Anzahl Personen, welche immer das gleiche Passwort benützen:	867'000
Spannbreite unter Berücksichtigung des Vertrauensintervalls: (bei einem Sicherheitsmass von 95 % bzw. einer Irrtumswahrscheinlichkeit von 5 %)	847'000 - 886'000

Auffallend ist hier, dass gerade die Altersgruppe der über 65-jährigen, die sich selbst den tiefsten Wissensstand attestieren und sich am unsichersten fühlen, am häufigsten mit «benutze nie die gleichen Passwörter» (31 %) antworten und sich damit am sichersten verhalten.

Da nicht erhoben wurde, für *wie viele* Anwendungen die Befragten die jeweiligen Passwörter benutzen, kann hier nur geschätzt werden: Es kann angenommen werden, dass die Bevölkerungsgruppe der über 65-jährigen eher weniger Anwendungen benutzt als die jüngeren und deshalb tatsächlich weniger Passwörter benötigt (siehe auch nächste Frage nach der Menge der Passwörter), was es wiederum leichter macht, für jede Anwendung ein eigenes Passwort zu verwenden.

Grundsätzlich verfügen diejenigen Personen, die sich selbst als eher oder sehr gut informiert bezeichnen, häufiger über verschiedene Passwörter pro Anwendung als die eher oder sehr schlecht informierten. Trotzdem befinden sich auch unter ihnen 12 %, die nur ein einziges Passwort für alle ihre Anwendungen verwenden. Das gleiche gilt beim Sicherheitsgefühl: 12 % fühlen sich sehr oder eher sicher, obwohl sie nur ein einziges Passwort verwenden.

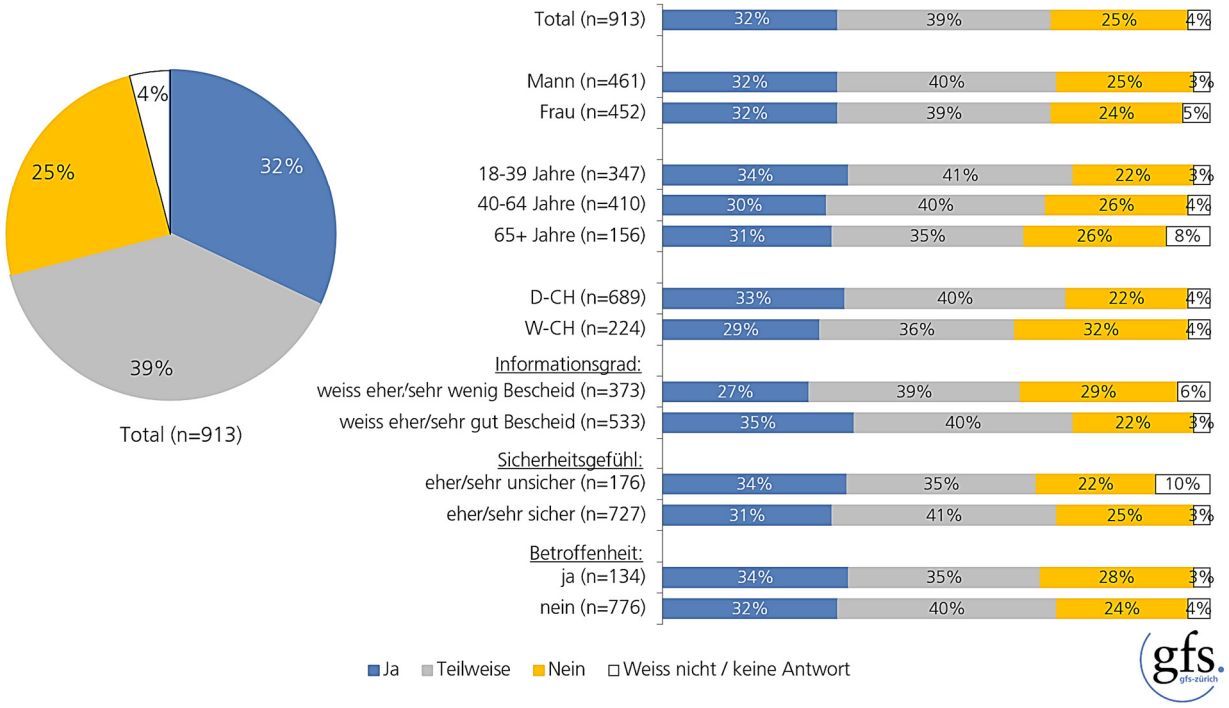
12: Wie viele unterschiedliche Passwörter verwenden Sie insgesamt ungefähr?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist



Ein Fünftel der Befragten verwendet weniger als 3 unterschiedliche Passwörter, die Hälfte weniger als 10 und rund ein Viertel (26 %) mehr als 10 unterschiedliche Passwörter. Hier zeigt sich, dass die über 65-jährigen am wenigsten unterschiedliche Passwörter verwenden (26 % weniger als 3 Passwörter), was als Hinweis darauf verstanden werden kann, dass sie weniger Anwendungen im Internet benutzen als jüngere Altersklassen, da sie bei der vorherigen Frage signifikant häufiger mit «benutze nie das gleiche Passwort» geantwortet haben.

Personen, die besser Bescheid wissen und sich sicherer fühlen, verwenden signifikant mehr unterschiedliche Passwörter – nach Annahme der Studienautoren auch mehr Internetanwendungen.

13: Sind Ihre Passwörter mindestens 10 Zeichen lang?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist

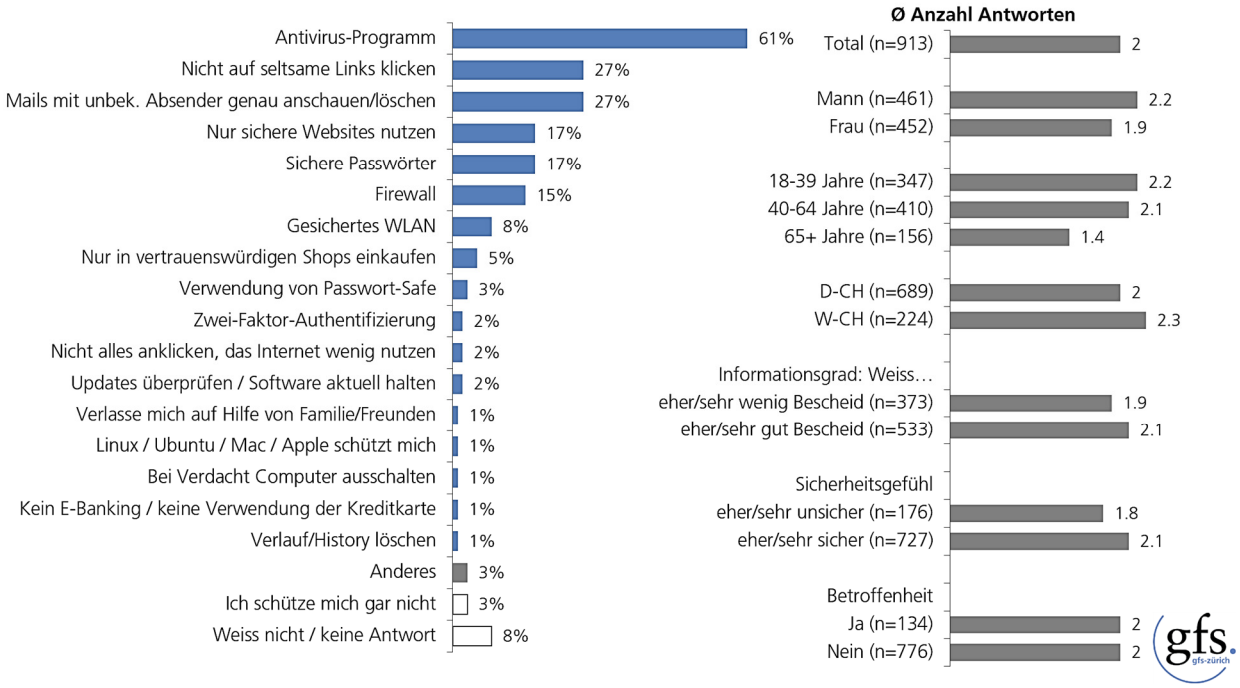


Rund ein Drittel der Befragten (32 %) verwendet grundsätzlich Passwörter mit mindestens 10 Zeichen, weitere 39 % verwendet teilweise so lange Passwörter. Zwischen den Subgruppen gibt es dabei nur wenige Unterschiede.

3.4.2 Schutzmassnahmen

Bei der am häufigsten genannten Schutzmassnahme handelt es sich um eine technische Vorkehrung: Knapp zwei Drittel der Befragten (61 %) nennt ein Antivirusprogramm als angewandte Massnahme. Sie wird von allen Subgruppen an erster Stelle genannt, besonders häufig von den Männern (65 %), den 18-39jährigen (70 %), den Westschweizern (67 %) und den Personen, die eher oder sehr gut Bescheid wissen (65 %).

14: Können Sie mir spontan ein paar Massnahmen nennen, wie Sie sich gegen Angriffe aus dem Internet schützen, also z.B. gegen Viren, Trojaner, Phishing, Datendiebstahl oder Onlinebetrug?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / offene, vorcodierte Frage / Mehrfachnennungen



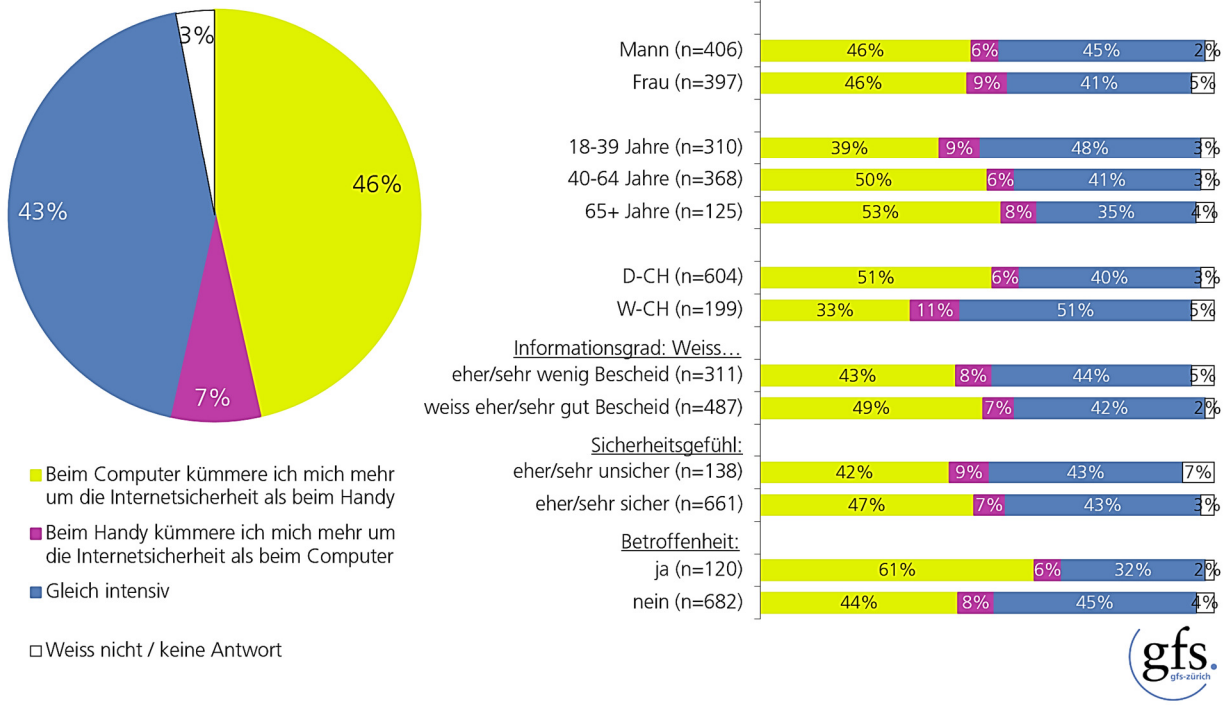
Dem Antivirus-Programm folgen verhaltensbezogene Massnahmen wie nicht auf seltsame Links zu klicken und Mails mit unbekanntem Absender genau zu prüfen oder zu löschen (je 27 %). Weiter folgen mit je 17 % die ausschliessliche Nutzung von sicheren Websites und die Verwendung von sicheren Passwörtern, erst dann folgt wieder eine technische Massnahme, die Firewall, die von 15 % der Befragten genannt wird.

Durchschnittlich antworten die Befragten mit 2 Nennungen auf diese Frage, wobei Männer mehr angewandte Massnahmen nennen (Ø 2.2) als Frauen (Ø 1.9) und Westschweizer (Ø 2.3) mehr als Deutschschweizer (Ø 2.0). Je älter die Befragten sind, desto weniger Massnahmen nennen sie. Wer sich selbst als besser informiert einschätzt und sich sicherer fühlt, weiss ebenfalls mehr Massnahmen zu nennen (je Ø 2.1). Die Betroffenheit von einem Cyberangriff hingegen hat keinen Einfluss auf die Anzahl Antworten, die hier gegeben werden (je Ø 2.0).

3.4.3 Sicherheit des Computers vs. Handy

Bei der Frage, ob der Sicherheit des Computers oder des Handys mehr Aufmerksamkeit gewidmet wird, hatten die Studienautoren die Theorie, dass sich die Befragten nur um die Sicherheit des Computers, nicht aber des Handys kümmern. Diese Theorie erwies sich in ihrer extremen Aussage als falsch, man kümmert sich nicht «nicht» um die Sicherheit des Handys: 43 % der Befragten antworten, dass sie sich um beide Geräte gleich intensiv kümmern, während 7 % sich mehr um die Sicherheit des Handys als des Computers kümmern, und 46 % – immerhin fast die Hälfte – kümmern sich mehr um die Sicherheit des Computers als die des Handys. In Anbetracht des aufkommenden Mobile Bankings und Mobile Payments dürfte diese Haltung sicherheitsrelevant sein.

15: Wie intensiv beschäftigen Sie sich mit der Internet-Sicherheit von Ihrem Handy im Vergleich zu Ihrem Computer?
n=803 / Filter: Person besitzt ein Handy UND einen Computer / eine Antwort



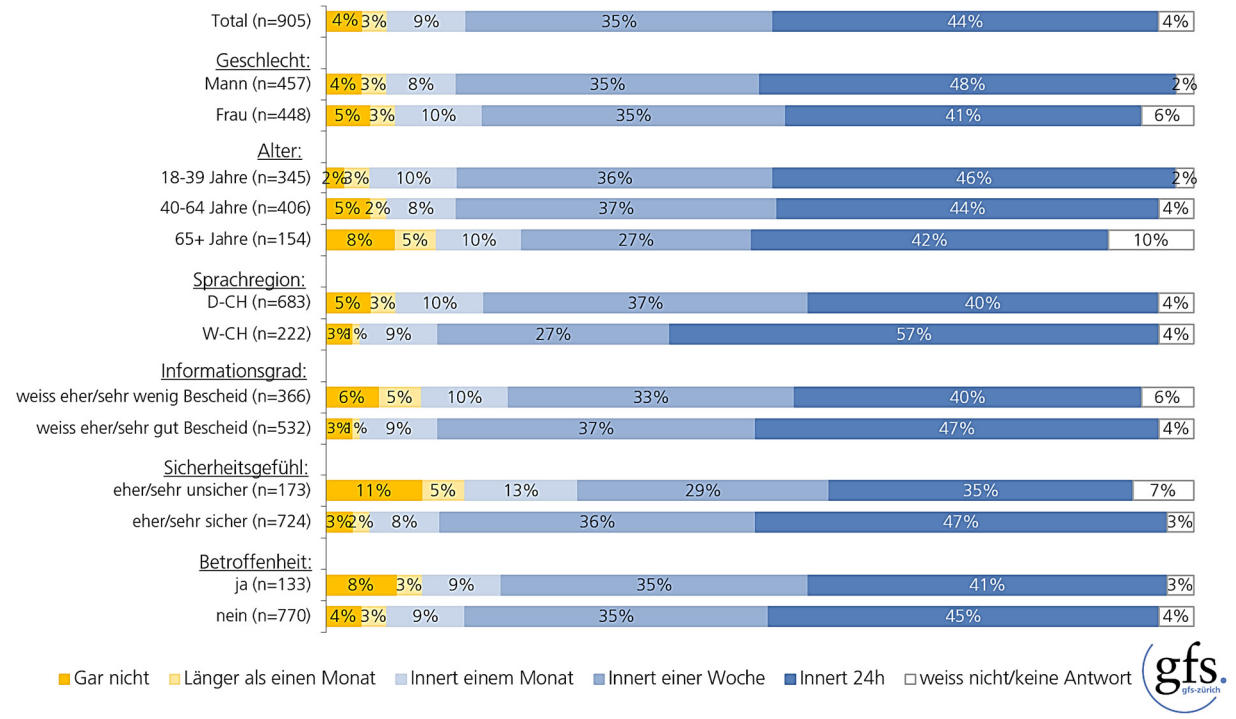
3.4.4 Durchführung von Updates

Neben sicheren Passwörtern ist die rasche Durchführung von Software-Updates eine weitere fundamentale Sicherheitsmassnahme. Dazu wurde die Frage gestellt, wie schnell diese Updates durchgeführt werden, wenn das Gerät (Computer oder Handy) dazu auffordert.

Rund zwei Fünftel der Befragten (44 %) geben an, Updates innerhalb von 24 Stunden durchzuführen, weitere 35 % benötigen dazu maximal eine Woche. Nur 3 % nehmen sich mehr als einen Monat Zeit, 4 % sagen aus, nie ein Softwareupdate durchzuführen.

Dieses mehrheitlich vorbildliche Verhalten wird von den Studienautoren als sehr positiv beurteilt und zumindest teilweise auf den Druck (z.B. Pop-Ups, Erinnerungen und Automatik-Funktionen) zurückgeführt, den die Softwarehersteller mit den Updates ausüben.

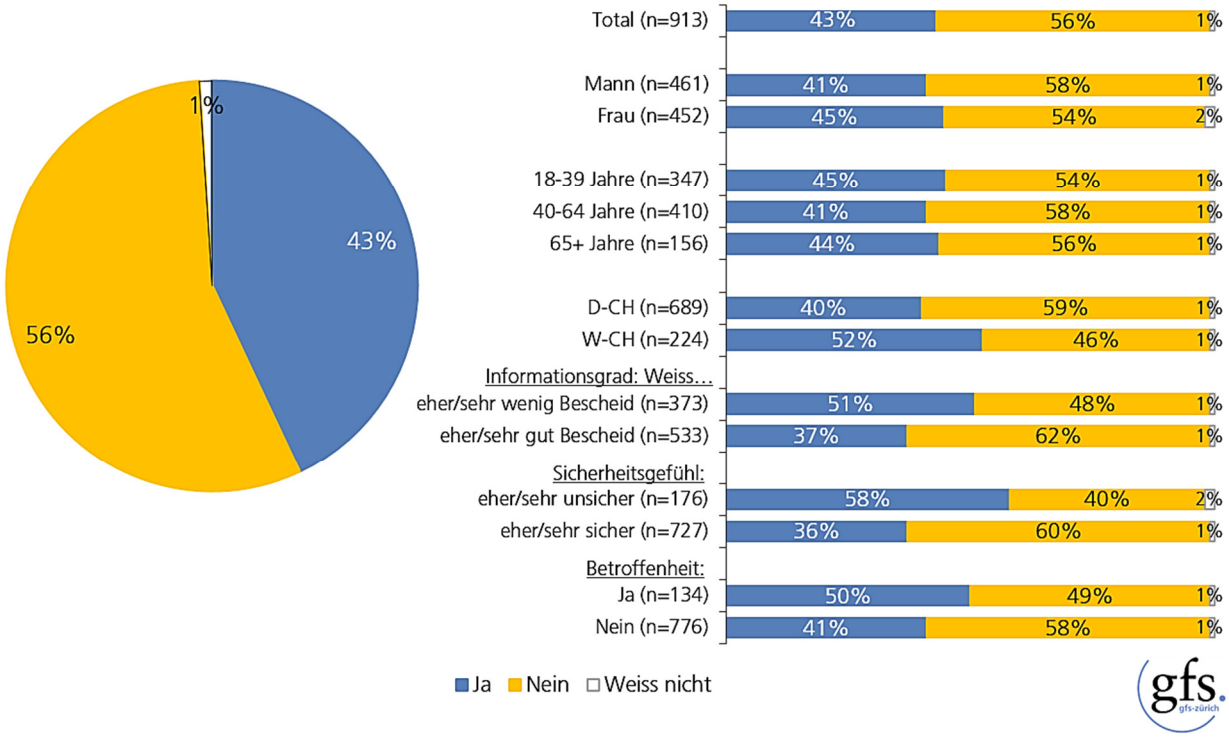
16: Wenn Ihr Computer oder Ihr Handy Sie auffordert, ein Software-Update durchzuführen, tun Sie das dann:
n=905 (Filter: Person besitzt ein Handy ODER einen Computer



3.5 Verbesserung des Informationsgrads

Zum Abschluss der Befragung wurde gefragt, ob man gerne besser über das Thema «Sicherheit im Internet» informiert wäre. Nur eine Minderheit der Befragten (43 %) bejahte dies:

17: Wären Sie gerne besser informiert über das Thema «Sicherheit im Internet»?
n=913 / Filter: Besitzt mindestens ein Gerät, das mit dem Internet verbunden ist / eine Antwort



Wer sich eher oder sehr schlecht informiert (51 %) bzw. unsicher fühlt (58 %), wünscht sich eher einen besseren Informationsgrad. Allerdings haben die vorangegangenen Ergebnisse gezeigt, dass auch gut informierte bzw. sich sicher fühlende Personen durchaus noch Potential haben, sich sicherer zu verhalten. Sollte die Resilienz gegenüber Cyberangriffen gestärkt werden, dürfte es eine besondere Herausforderung sein, das teilweise unbegründete Sicherheitsgefühl und Desinteresse zu überwinden.

4 Studiendesign in Kürze

Auftraggeber:	ICTswitzerland, Andreas Kaelin Information Security Society Switzerland ISSS, Umberto Annino Schweizerische Akademie der Technischen Wissenschaften SATW, Nicole Wettstein Swiss Internet Security Alliance SISA, Daniel Nussbaumer SwissICT, Christian Hunziker SWITCH, Martin Leuthold Informatiksteuerungsorgan des Bundes ISB, Daniel Rudin
Inhalt:	Cybergefahren: Wissensstand, Informationsquellen, Sicherheitsgefühl, Betroffenheit, Schutzmassnahmen
Grundgesamtheit:	Bevölkerung der Deutsch- und Westschweiz 18+ mit mindestens einem internetverbundenen Gerät
Methode:	Telefonische Mehrthemenbefragung (CATI)
Stichprobe:	n=1001 (Basisstichprobe), davon 913 mit mindestens einem internetverbundenen Gerät
Gewichtung:	keine
Quoten	Sprachregion (geschichtet), Alter, Geschlecht
Interviewdauer:	8.6 Minuten
Sprachen:	Deutsch, Französisch
Auswertung:	Tabellenband Grafiken Schriftlicher Bericht
Feldphase:	25. Januar bis 15. Februar 2019
Projektleiterin gfs-zürich:	Karin Mändli Lerch