Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen,
dass Sie
sicher leben.
Ihre Polizei

Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit

Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI)

1 Zielsetzung der Bürgerbefragung zur Cyber-Sicherheit

Das Digitalbarometer 2020 untersucht den aktuellen Kenntnisstand der Bevölkerung zum Thema IT-Sicherheit und Cyberkriminalität. Es basiert auf einer repräsentativen Online-Befragung der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Neben den Einstellungen, Erfahrungen und Kenntnissen der Gesamtbevölkerung betrachtet die Erhebung auch unterschiedliche Altersgruppen genauer. Das Digitalbarometer ist erstmals 2019 erschienen.

Die repräsentative Online-Befragung umfasste neben demografischen Merkmalen vier Themenschwerpunkte:

- Informationsverhalten zur IT-Sicherheit,
- persönliche Erfahrungen mit Kriminalität im Internet,
- BSI und ProPK: Bekanntheit und Nutzen,
- die Themen „Gaming“ und „Verbreitung von illegalen Inhalten, z. B. Kinderpornografie“.

Sie wurde im Frühjahr 2020 von Ipsos Public Affairs GmbH durchgeführt.

Die Erhebung im Überblick

Methode
Computer Assisted Web Interviewing (CAWI)

Zielgruppe
Deutschsprachige Bevölkerung im Alter von 14 bis 69 Jahren, die in einem Privathaushalt in Deutschland lebt und über einen Internetzugang verfügt.

Stichprobe
Die repräsentative Stichprobe wurde anhand der Merkmale Alter, Geschlecht, Bildung und Bundesland aus dem Ipsos Online-Access-Panel gezogen.

Anzahl der Interviews
2.000

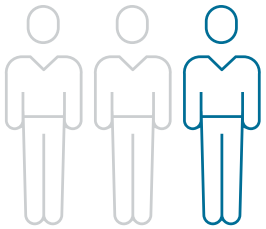
Feldarbeit
9. bis 18. April 2020

Gewichtung
Die ausgewiesenen Ergebnisse wurden anhand der Bevölkerungsstrukturmerkmale Alter, Geschlecht, Bundesland und Bildung in Deutschland gewichtet.

2 Sicherheit und Schutzmaßnahmen

2.1 Jede/r Vierte von Kriminalität im Internet betroffen

Opfer von Cyberkriminalität wurden bereits 25 Prozent der Befragten, davon wiederum jede/r Vierte in den letzten zwölf Monaten. Am häufigsten wurden die Betroffenen Opfer von Online-Betrug. **Mehr als zwei Drittel aller Betroffenen erlitten durch Cyberkriminalität einen Schaden.** Bei den meisten von ihnen (36 %) handelt es sich um einen theoretischen finanziellen Schaden, in denen der Verlust beispielsweise als Versicherungsfall eingestuft und somit erstattet wurde.

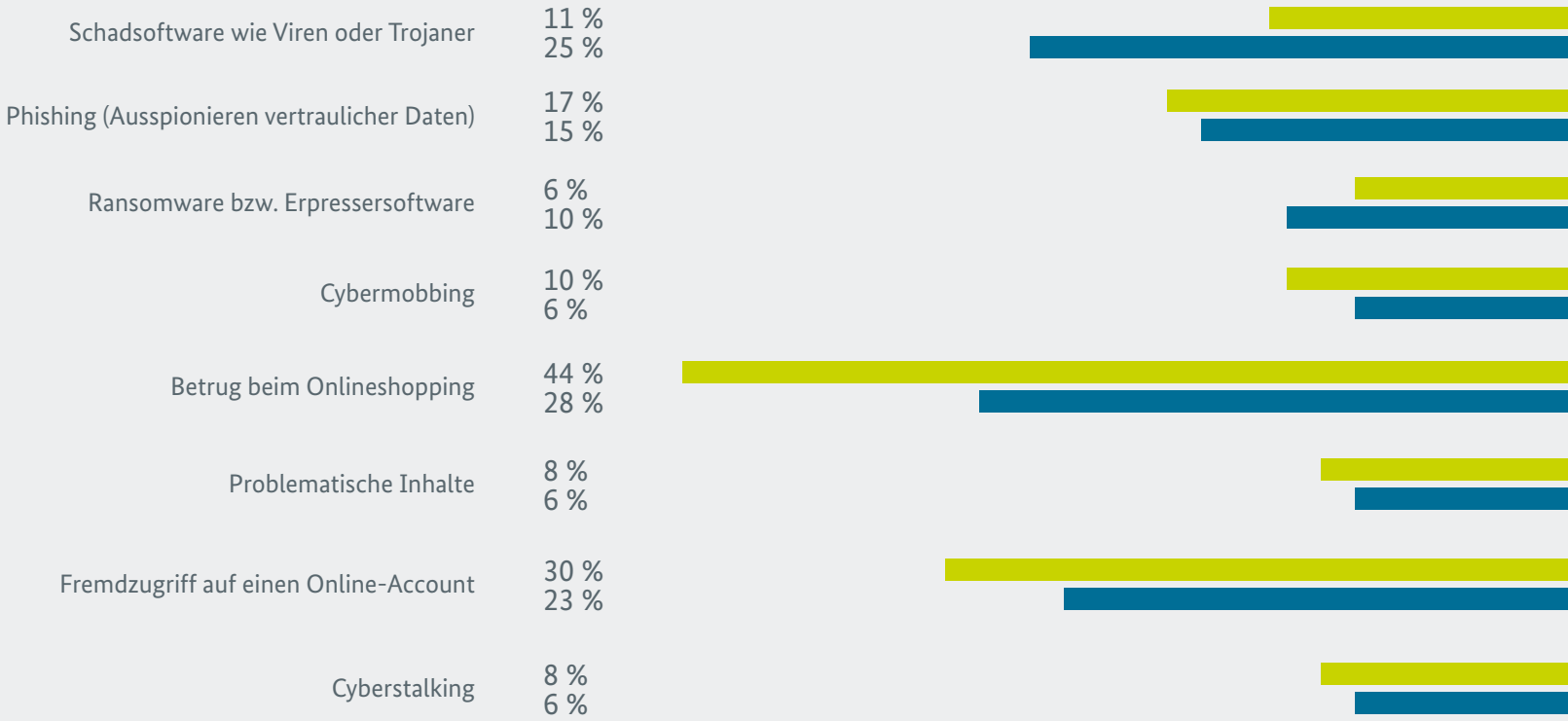


Ein Drittel (32 %) hatte einen realen finanziellen Schaden.

Die Spannbreite der Schadenssummen ist sehr groß: **So liegt der höchste angegebene Schadenswert bei 50.000 Euro.** Die meisten Schäden liegen jedoch unter 100 Euro. Aber auch ein emotionaler Schaden, beispielsweise in Folge von Cybermobbing (25 %), ein Verlust von Daten oder ein zeitlicher Schaden (jeweils 23 %) treten regelmäßig auf. Mehrfach Opfer von Straftaten im Internet wurden vier Prozent der Befragten.

Das Digitalbarometer 2019 zeigte ein ähnliches Bild: Damals gaben 24 Prozent der StudienteilnehmerInnen an, von Straftaten im Internet betroffen zu sein. Während 2019 die Infektion mit Schadsoftware am häufigsten genannt wurde, rückt in den letzten zwölf Monaten der Betrug beim Onlineshopping und der Fremdzugriff auf Online-Accounts in den Vordergrund.

Um welche Art von Straftat handelte es sich dabei, als sie Opfer von Kriminalität im Internet geworden sind?



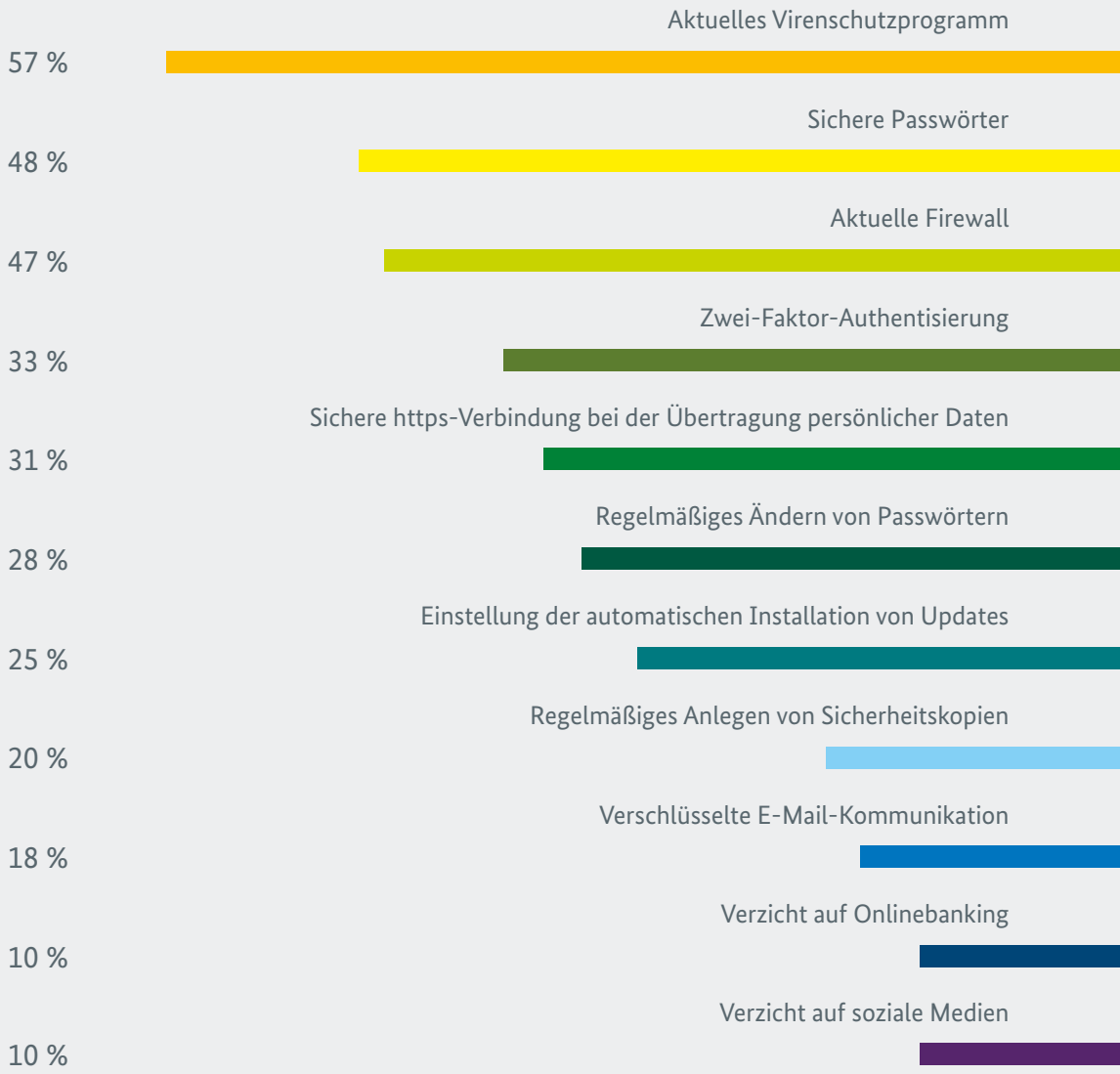
Basis: Befragte, die früher als innerhalb der letzten 12 Monaten Opfer von Internetkriminalität geworden sind (*N*=368).
Befragte, die innerhalb der letzten 12 Monaten Opfer von Internetkriminalität geworden sind (*N*=126).

2.2 Jede/r Zehnte ohne Schutzmaßnahme

Am häufigsten nutzen die Befragten als Schutzmaßnahmen ein aktuelles Virenschutzprogramm (57 %), sichere Passwörter (48 %) und eine aktuelle Firewall (47 %). Diese Maßnahmen sind wichtig, reichen jedoch nicht aus.

Um schnell Sicherheitslücken in Programmen und Betriebssystemen schließen zu können und sich so vor Angriffen durch Cyberkriminelle zu schützen, sollten NutzerInnen beispielsweise die automatische Installation von Updates einstellen. In der Umfrage zeigt sich, dass nur jede/r Vierte diese Option bewusst nutzt. Sie rangiert auf Platz sieben der **am häufigsten eingesetzten Schutzmaßnahmen.** Zehn Prozent geben an, keine Schutzmaßnahmen zu nutzen.

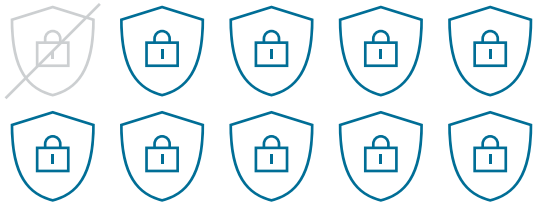
Wie schützen Sie sich vor Gefahren im Internet?



Basis: Alle Befragten (*N*=2.000). Mehrfachnennungen möglich.

Verzicht als Schutzmaßnahme

Auffallend ist, dass jede/r Zehnte der Befragten auf die Nutzung eines Onlineangebots verzichtet, um sich zu schützen. Auf Onlinebanking verzichten eher jüngere Befragte (15 % der 14- bis 18-Jährigen und 14 % der 19- bis 29-Jährigen), auf soziale Netzwerke eher Senioren (13 % der 60- bis 69-Jährigen).



Wer mehr Geräte hat, wird häufiger Opfer

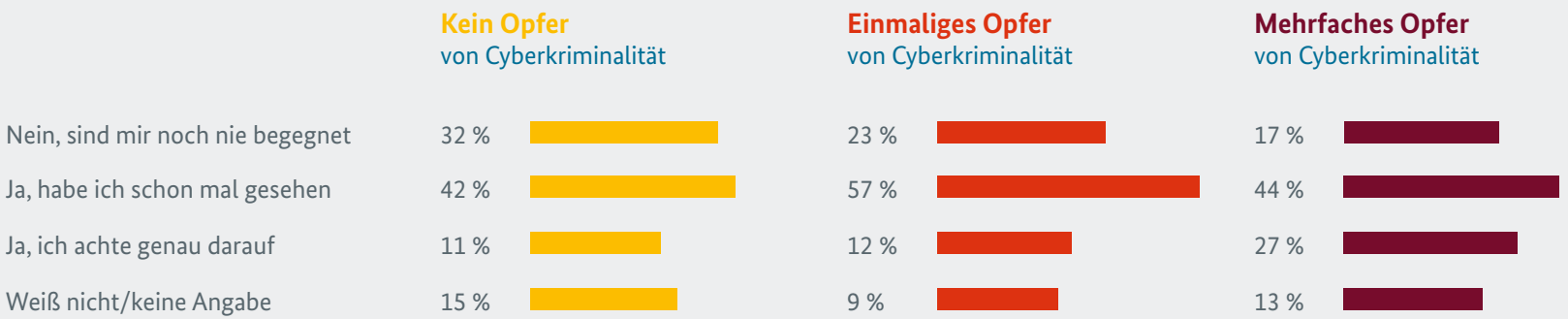
Durchschnittlich verfügen die StudienteilnehmerInnen über vier Geräte, mit denen sie das Internet nutzen. **Je mehr Geräte eine Person besitzt, desto höher ist die Wahrscheinlichkeit, dass sie bereits Opfer von Cyberkriminalität wurde.** In den meisten Fällen erhöhen Betroffene ihre eingesetzten Schutzmaßnahmen nach einem Vorfall nicht. Im Gegenteil: **Die Betroffenen wenden die gängigen Schutzmaßnahmen oftmals seltener an als die Gesamtgruppe der Befragten.** Während nur 47 Prozent der Betroffenen sich mithilfe eines aktuellen Antivirenprogramms schützen, nutzen 57 Prozent aller Befragten eine solche Software. 26 Prozent der Opfer von Cyberkriminalität setzen die Zwei-Faktor-Authentisierung ein, unter allen Befragten sind es hingegen 33 Prozent.

2.3 Direkte Umsetzung von Empfehlungen zeigt Wirkung

Ein Großteil der Befragten setzt Sicherheitsempfehlungen nicht präventiv um: Knapp ein Drittel (29 %) hat Empfehlungen zum Schutz von Geräten und Daten noch nie bewusst wahrgenommen. Über die Hälfte (55 %) kennt sie zwar, aber **nur jede/r Zehnte achtet bewusst darauf und verfolgt entsprechende Meldungen, etwa auf Computer- und Technikportalen oder allgemein mit Hilfe von Suchmaschinen.** Außerdem dienen Sicherheits- und Antivirenprogramme sowie FreundInnen, Familie, Bekannte und ArbeitskollegInnen als Informationsquelle. Wer die Empfehlungen kennt, handelt in der Regel danach: 41 Prozent tun dies allerdings erst, wenn sie daran denken. Immerhin 39 Prozent der Befragten setzen die Empfehlungen sofort um.

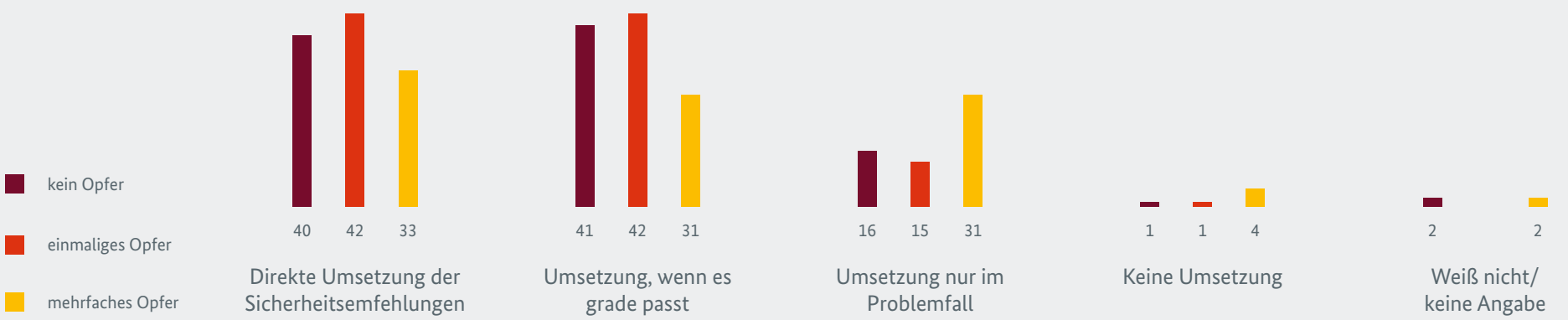
Eine direkte Umsetzung von Sicherheitstipps scheint wirkungsvoll vor Kriminalität im Internet zu schützen: Befragte, die bisher gar nicht oder nur einmalig Opfer wurden, geben häufiger an, die Empfehlungen direkt umzusetzen. Hingegen setzen Menschen, die mehrfach Opfer waren, Sicherheitsempfehlungen eher nur im Problemfall um – in 31 Prozent der Fälle.

Kennen Sie die aktuellen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet?



Basis: Alle Befragten (*N*=2.000).

Inwiefern halten Sie sich an diese Sicherheitsempfehlungen?



Basis: Befragte, welche Sicherheitsempfehlungen kennen (*N*=1.129), Angaben in Prozent.

2.4 Selbsthilfe weiterhin ein Thema

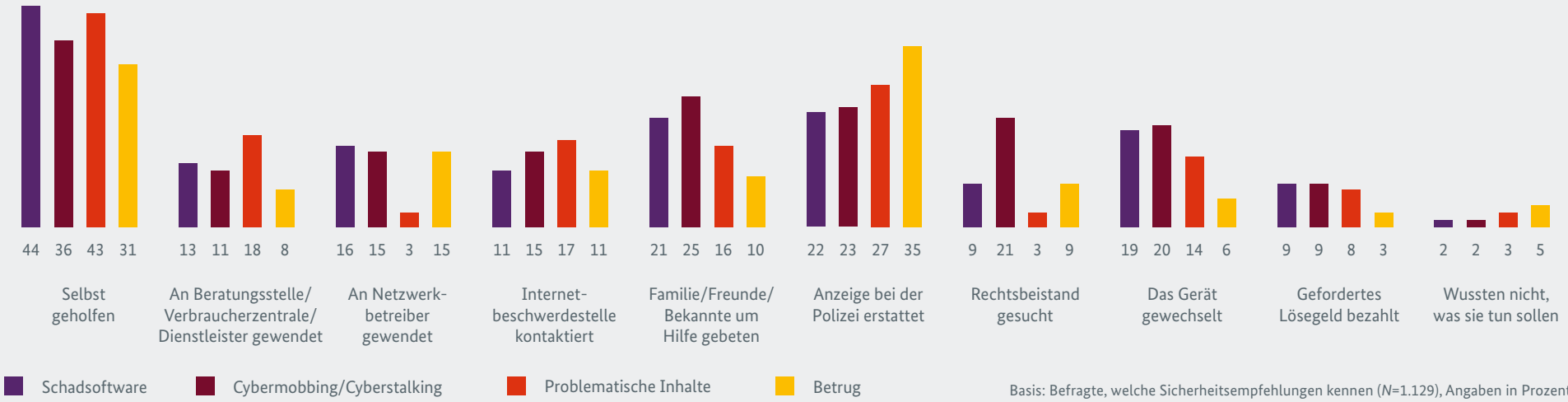
Am häufigsten haben sich Betroffene von Cyberkriminalität im Ernstfall selbst geholfen (36 %) oder Anzeige bei der Polizei erstattet (34 %). Nur fünf Prozent wussten nicht, was sie tun sollen. Diese Ergebnisse korrespondieren mit dem Informationsbedürfnis der Befragten: **Mehr als die Hälfte der Betroffenen wünscht sich eine Checkliste für den Notfall sowie Hinweise, wie sie Kriminalität im Internet erkennt und was sie im Ernstfall tun kann.** Etwa jede/r Dritte wünscht sich Beratung von der Polizei, vor allem für Fragen zu Cybermobbing, Cyberstalking und Betrug.

Außerdem wurden die StudienteilnehmerInnen gefragt, wie sie handeln würden, wenn sie eine Straftat im Zusammenhang mit der Internetnutzung vermuten. Die Mehrheit würde aktiv werden, jede/r Zweite sich an die Polizei wenden (52 %). **Jede/r Zehnte weiß jedoch nicht, wie er reagieren sollte. Nur drei Prozent würden gar nichts tun.**

Großteil informiert sich sporadisch auf Webseiten

Der größte Teil der Befragten informiert sich „hin und wieder“ (37 %) über CyberSicherheit, ein Viertel gar nicht und knapp jede/r Fünfte nur im Problemfall (19 %). Nur 15 Prozent informieren sich regelmäßig. Webseiten sind mit Abstand der beliebteste Informationskanal (64 %). Am häufigsten werden Computer- und Technikportale von Befragten aufgesucht (35 %), in vielen Fällen wird über eine Suchmaschine recherchiert (28 %). Weitere Quellen für Informationen über Cyber-Sicherheit sind FreundInnen und Bekannte (33 %) sowie Fachzeitschriften (22 %).

Wie haben Sie auf die jeweilige Straftat reagiert?



Basis: Befragte, welche Sicherheitsempfehlungen kennen (*N*=1.129), Angaben in Prozent.

3 Themenfokus Sicherheit

3.1 Wenn’s ums Geld geht, ist Sicherheit wichtig

Etwa zwei Drittel der Befragten shoppen mindestens einmal im Monat online oder führen Geschäfte per Onlinebanking aus. **Diese Tätigkeiten gehören nach dem allgemeinen Surfen sowie der Kommunikation per E-Mail und Messenger zu den häufigsten Onlineaktivitäten.** Entsprechend sind das die Bereiche, bei denen den Befragten auch Sicherheit wichtig ist (60 % bei Onlinebanking und 40 % bei Onlineshopping). Gleichzeitig wurden 44 Prozent derjenigen, die schon einmal Cyber-Kriminalität erlebt haben (25 %), in den letzten zwölf Monaten **Opfer von Betrug beim Onlineshopping.**

3.2 Account-Schutz gewinnt an Bedeutung – auch bei Onlinespielen

Unter den Opfern von Cyberkriminalität verzeichnete etwa jede/r Dritte in den letzten zwölf Monaten einen Fremdzugriff auf einen Online-Account (30%). **Maßnahmen zum Schutz ihrer Online-Konten ergreifen PrivatanwenderInnen noch nicht flächendeckend:** Knapp die Hälfte der Befragten legt Wert auf sichere Passwörter (48 %) und ein Drittel setzt auf eine Zwei-Faktor-Authentisierung, um einen Online-Account zu schützen (33 %). Im Bereich Gaming nutzen beispielsweise 20 Prozent der OnlinespielerInnen einen zweiten Faktor bei der Anmeldung. Diejenigen, die das bislang noch nicht tun, haben verschiedene Gründe dafür: Etwa jede/r Vierte gibt an, nicht zu wissen, was die Zwei-Faktor-Authentisierung ist (27 %). Für ein weiteres Viertel der Befragten ist sie nicht wichtig (23 %). Weitere Gründe sind das fehlende Angebot der Zwei-Faktor-Authentisierung bei den Spielanbietern (16 %), die zu komplizierte Einrichtung und die Unfähigkeit, die Einstellungsmöglichkeit zu finden (jeweils 7 %).

Nutzen Sie die Zwei-Faktor-Authentisierung beim Start des Onlinespiels?

Basis: Befragte, die digitale Spieleangebote nutzen (*N*=967).

OnlinespielerInnen haben wenig schlechte Erfahrungen

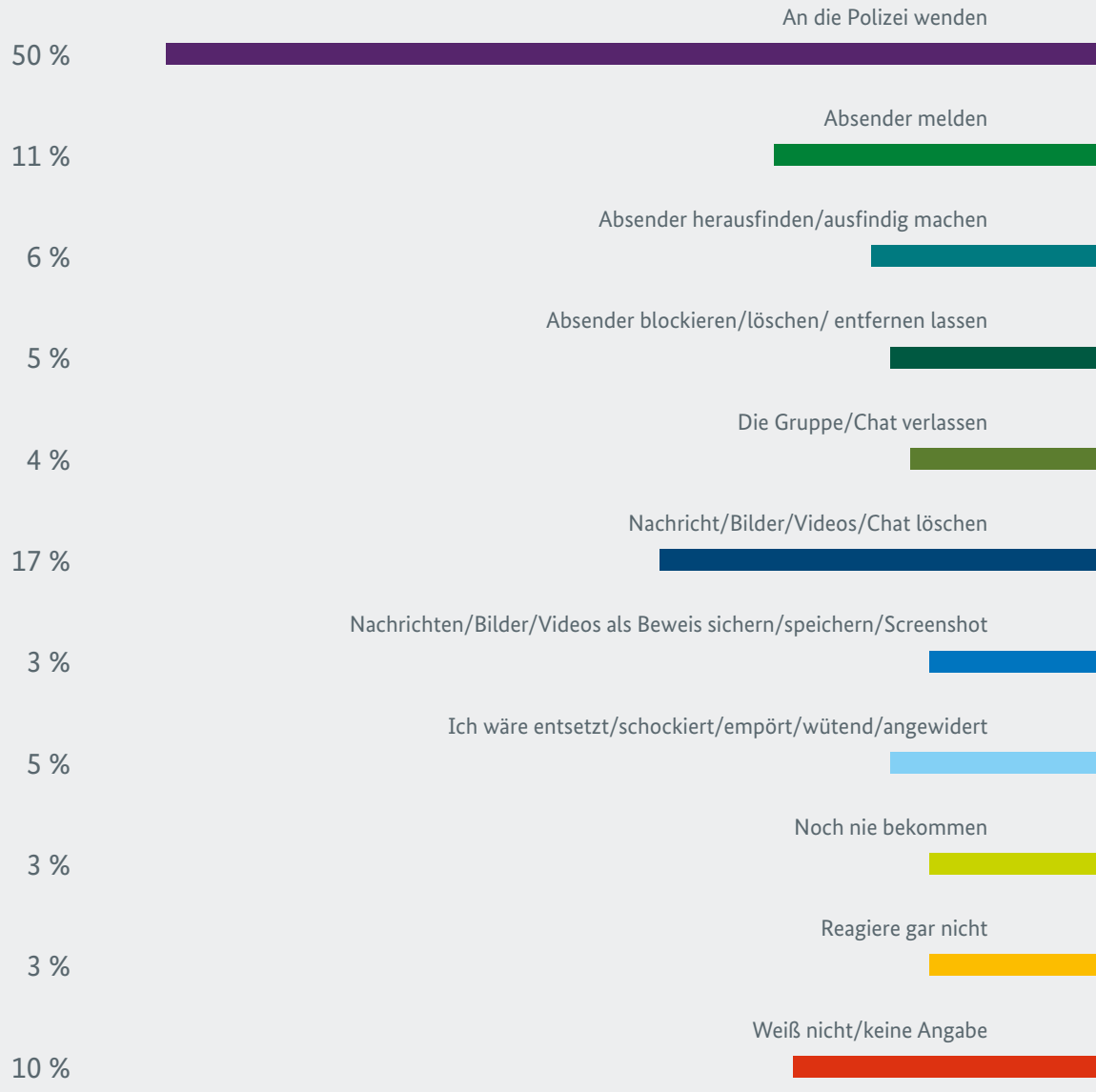
Für ein Drittel der Befragten gehören Onlinespiele zum Alltag: 35 Prozent geben an, digitale Spieleangebote zu nutzen. Davon spielt fast die Hälfte täglich (45 %), viele mindestens einmal in der Woche (35 %). Den meisten (71 %) ist keine der abgefragten Straftaten widerfahren. Allerdings hat etwa ein Drittel Erfahrungen mit unangemessenen Dialogen (15 %), Betrug beim Onlinespielen (11 %), Schadprogrammen (8 %) und Diebstahl eines Online-Accounts (6 %) gemacht (Mehrfachnennungen waren möglich).

3.3 Verbreitung von problematischen Inhalten

Acht Prozent der Befragten geben an, in den letzten zwölf Monaten problematische und vermutlich strafbare Inhalte über das Internet erhalten zu haben. Anschließend wurden sie mithilfe von zwei Fallbeispielen nach ihrer konkreten Reaktion nach Erhalt problematischer Inhalte gefragt:

Im ersten Fallbeispiel werden über eine Messenger-Gruppe Inhalte gesendet, die Erwachsene und Kinder in sexualisierter Art und Weise zeigen. **Die Hälfte der Befragten nimmt diese Situation sehr ernst und gibt an, sich in solch einem Fall an die Polizei zu wenden.** Fast ein Fünftel der StudienteilnehmerInnen (17 %) würde die Inhalte hingegen nur löschen und keine weiteren Maßnahmen ergreifen. Etwas mehr als jede/r Zehnte (11 %) würde den Absender melden. Nur drei Prozent würden überhaupt nicht reagieren.

Fallbeispiel 1 „Kinderpornografie in einer Messenger-Gruppe“



Basis: Alle Befragten (*N*=2.000). Mehrfachnennungen möglich.

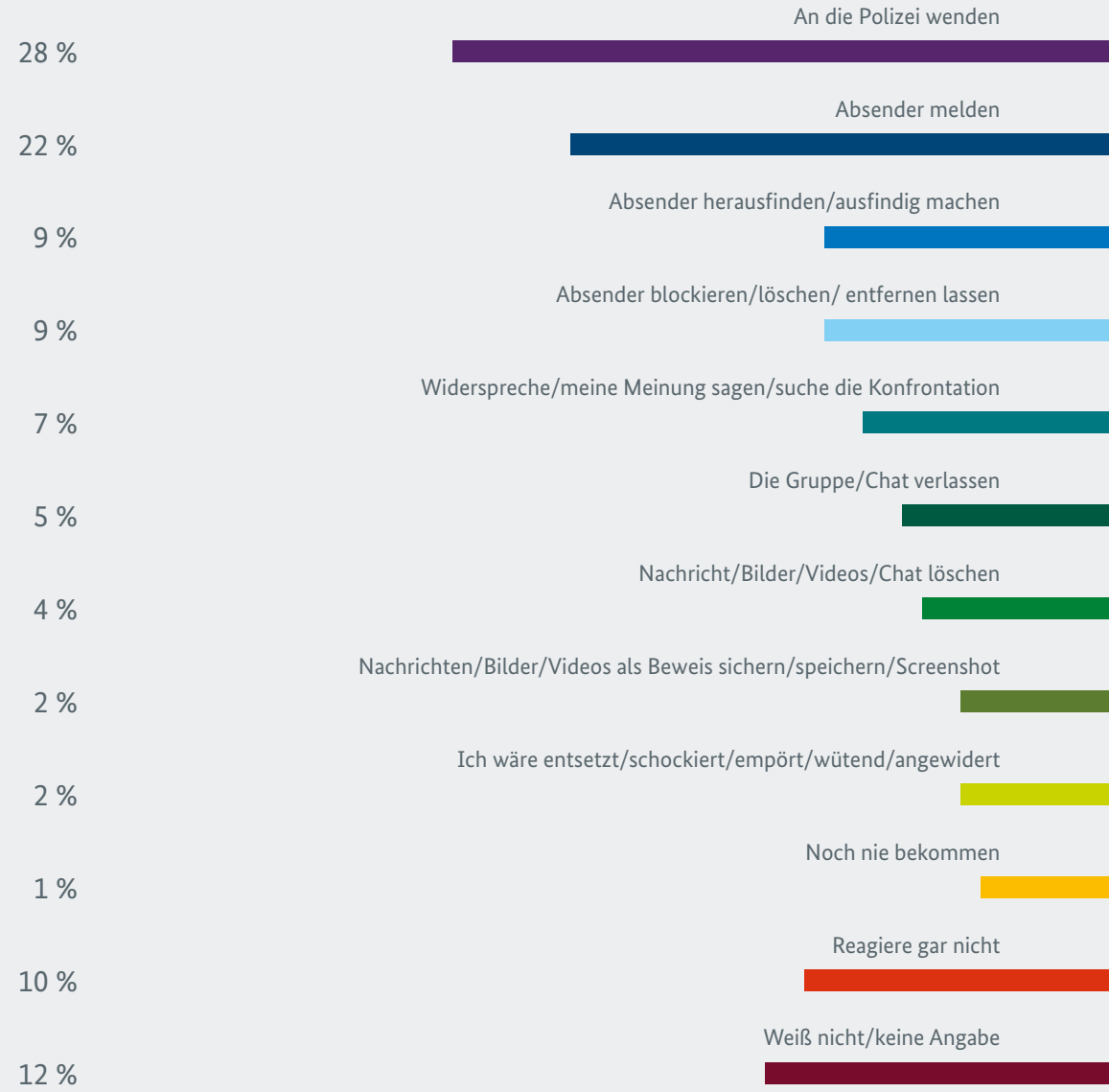
Im zweiten Fallbeispiel geht es um die konkrete Reaktion auf Hasskommentare in einer Chat-Gruppe.

Sie sind gern in einem Chat unterwegs, um sich mit anderen zu Ihrem Lieblingshobby auszutauschen. Ein Chatteilnehmer postet dort wiederholt Kommentare, die Migranten beleidigen. In seinen Kommentaren heute erklärt er, welche Gewalttaten er allen Flüchtlingen antun würde. Er beschreibt sehr genau alle Details.

Wie reagieren Sie auf solche Kommentare?

Die Fragen nach der Reaktion auf die beiden Vorfälle konnten die Befragten offen beantworten. Ziel der offenen Fragestellung war es, **einen Überblick über die Handlungskompetenzen der NutzerInnen zu gewinnen und so Präventionsmaßnahmen stärker darauf ausrichten zu können.** Beide Fälle verdeutlichen, dass **bis zu einem Fünftel der Befragten nicht weiß, wie sie handeln soll.** Hinzu kommen 34 Prozent, die sich Tipps wünschen, um mit problematischen Inhalten umgehen zu können.

Fallbeispiel 2 „Hasskommentare in einem Chat“



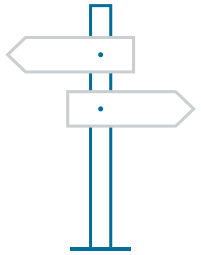
Basis: Alle Befragten (*N*=2.000). Mehrfachnennungen möglich.

4 Präventionsmaßnahmen

1. Checklisten für mehr Sicherheit

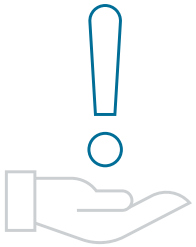
Mit dem Digitalbarometer 2019 rückte insbesondere der Aspekt Hilfe zur Selbsthilfe stärker in den Fokus von ProPK und BSI. Gemeinsam entwickelten sie die Reihe **„Checkliste für den Ernstfall“**, die es bislang für die Themen Phishing, Betrug beim Onlinebanking und Schadprogramme gibt. Ziel ist es, Betroffenen eine praxisnahe Anleitung an die Hand zu geben, wie sie im Notfall reagieren sollten. **Aus dem Digitalbarometer 2020 lassen sich weitere thematische Schwerpunkte für die Aufklärungsarbeit von BSI und ProPK ableiten.**

2. Orientierung bei den Schutzmaßnahmen



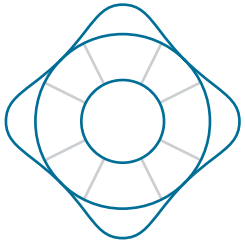
Der Einsatz eines Antivirenprogramms ist nach wie vor eine der am häufigsten umgesetzten Schutzmaßnahmen. **Seine Nutzung ist Teil eines guten Grundlagenpakets zur Absicherung von PCs, Laptops oder mobilen Geräten.** Doch Maßnahmen wie die Aktivierung automatischer Updates oder die Verwendung starker Passwörter sind mindestens ebenso wichtige Bausteine des Basisschutzes. Jedoch nehmen viele Betroffene sie bisher nicht als solche wahr. Deswegen soll die Aufklärungsarbeit zukünftig Orientierung bei der Priorisierung der Schutzmaßnahmen und der Bedeutung ihres Zusammenspiels geben. Dazu gehört auch die Klärung der Frage: **„Mit welchen Maßnahmen schütze ich welches Gerät?“**

3. Empfehlungen schnell zur Hand



Wer Empfehlungen direkt umsetzt, wird tendenziell seltener Opfer. Um die Umsetzungsbarrieren möglichst gering zu halten, **sollten Tipps zum sicheren Umgang mit Online-Diensten sowie internetfähigen Geräten schnell auffindbar, leicht verständlich und gut aufbereitet sein.** Die Polizei und das BSI stellen bereits umfangreiche Empfehlungen zur Verfügung. Um PrivatanwenderInnen stärker zu unterstützen, sollen sie zukünftig noch besser auffindbar und verständlicher sein.

4. Hilfe zur Selbsthilfe weiter ausbauen

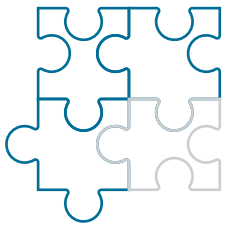


Schritt-für-Schritt-Anleitungen können im Ernstfall helfen, Schaden abzuwenden und im Nachgang ein möglichst hohes Maß an Sicherheit zu erreichen. ProPK und BSI stellen insbesondere für häufige Straftaten im Internet Informationen zur Verfügung, die der Hilfe zur Selbsthilfe dienen. Darunter fällt unter anderem der Ausbau der Checklisten-Reihe.

5. BSI befasst sich intensiv mit dem Thema Online-Accountschutz

Durch den Einsatz starker Passwörter und der Zwei-Faktor-Authentisierung lassen sich wichtige Online-Konten und die dort hinterlegten persönlichen Daten effektiv schützen. Das BSI erstellt und erprobt Informationsmaterial, das BürgerInnen bei der Umsetzung dieser Schutzmaßnahmen effektiv unterstützen soll.

6. ProPK gibt verstärkt Orientierung bei problematischen Inhalten



Die Polizei setzt sich in ihrer Präventionsarbeit seit längerer Zeit mit der Verbreitung von problematischen und strafrechtlich relevanten Inhalten auseinander. **Sie wird die Erkenntnisse aus der Befragung nutzen, um die bisherigen und zukünftigen Präventionskonzepte in diesem Themenbereich besser auszurichten –** und der Bevölkerung so zielgerichtet Empfehlungen zu vermitteln. Aktuelles Beispiel ist eine Kampagne, um junge Menschen über die strafbare Verbreitung von Kinderpornografie über digitale Medien aufzuklären.

Impressum

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

Die Bürgerbefragung für das „Digitalbarometer“ wurde vorgelegt von: Ipsos Public Affairs, Schwartzkopffstraße 11, 10115 Berlin

Autoren der Studie: Armgard Zindler, Carolin Bolz

Bezugsquelle: Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185–189, 53175 Bonn

E-Mail: bsi@bsi.bund.de

Telefon: +49 (0) 22899 9582-0 · Telefax: +49 (0) 22899 9582-5400

www.bsi.bund.de · www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

Bildnachweis: Titelbild: © tba

Gestaltung: Faktor 3 AG

Stand: 08/2020