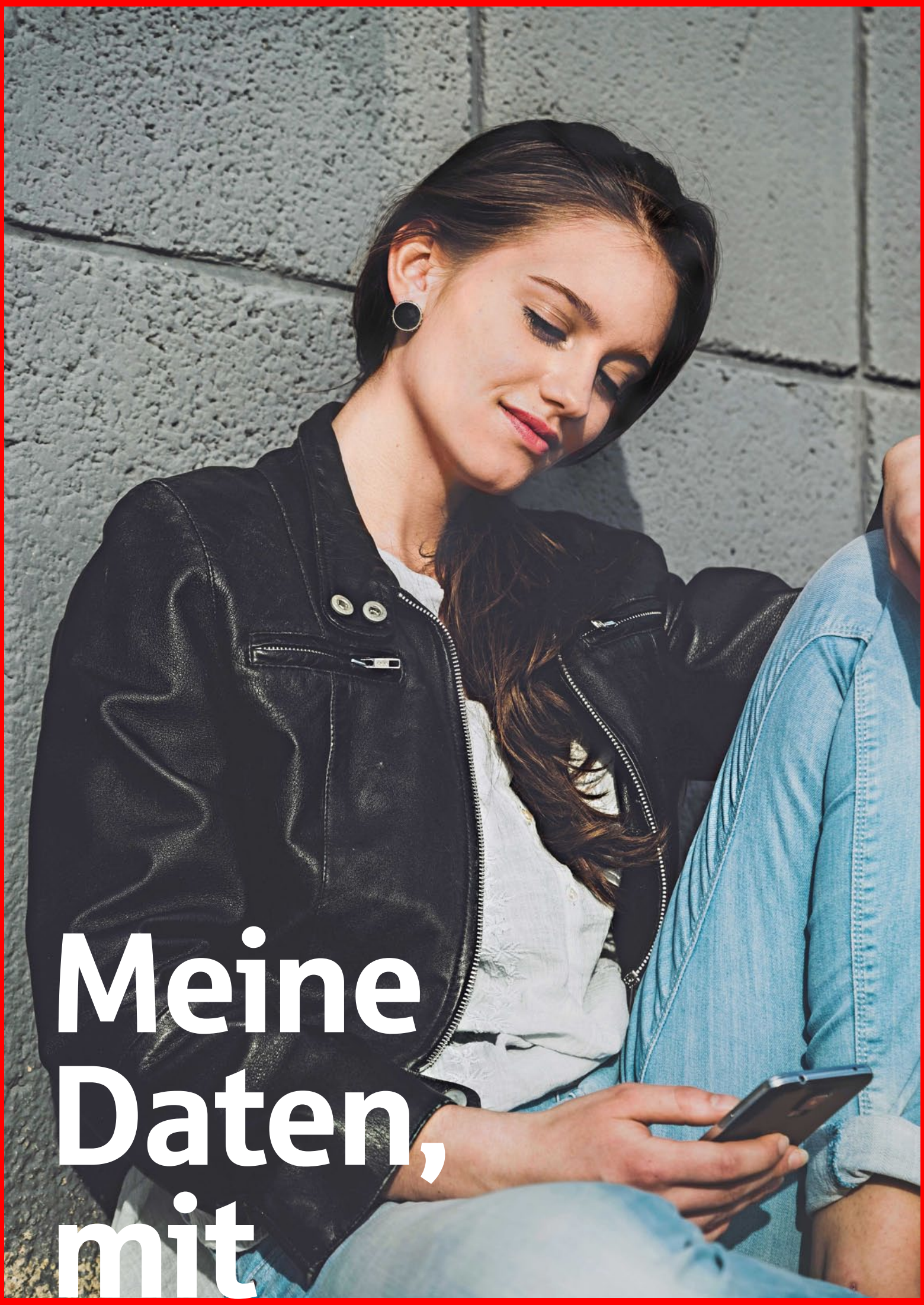
Sparkasse



Meine Daten, mit Sicherheit

Alles, was Sie zum Megathema Cyberschutz wissen müssen.

Alle reden von Daten und Hackern, von Trojanern und Malware. Aber was heißt das konkret für mich? Dieses E-Book verschafft Ihnen einen Überblick über aktuelle Bedrohungen im Netz und zeigt, wie man sich vor ihnen schützt. Durch bewusstes Nutzungsverhal-ten, hilfreiche Programme und gesunden Menschen-verstand. Damit man auch in Zukunft sicher im Netz unterwegs ist.

Die Fragen im Überblick

- Was ist eigentlich Identitäts-diebstahl?
- Merke ich überhaupt, wenn ich in Gefahr bin?
- Online-Banking mache ich nur auf dem PC. Das ist sicherer, oder?
- Was dürfen Apps auf meinem Smartphone?
- Phishing, Ransomware, Virus: Was ist noch mal was?
- Was wissen die großen Internet-konzerne eigentlich über mich?
- Wie sichere ich meine Daten?
- Mein Handy ist weg – und jetzt?
- Wie geht sicheres Shopping im Netz?
- Wie verhindere ich, dass ich Geld ausgebe, ohne es zu merken?
- Wie wehre ich mich gegen Cybermobbing?

Was ist eigentlich Identitäts-diebstahl?

Lena, 25

ÜBERSICHT

Liegt auf einmal eine Mahnung

im Briefkasten und flattern dann auch noch Drohschreiben von Inkassounternehmen ins Haus, die man sich nicht erklären kann, ist man wahrscheinlich Opfer von Identitätsmissbrauch geworden. Betrüger bestellen also unter fremdem Namen Waren im Internet. Dafür reichen oft bereits der Name und das Geburtsdatum, denn noch immer wird im Internet meist auf Rechnung bestellt. Der Online-Handel wird auch für Betrüger immer interessanter. Schätzungen gehen von 2,5 Milliarden Euro Schaden pro Jahr allein in Deutschland aus. Kriminelle spielen dieses Spiel

aber auch andersherum: Sie verkaufen oder versteigern nicht existente Produkte unter fremdem Namen und kassieren den Betrag. Empörte Anrufe der Käufer oder eventuell sogar Anzeigen wegen Betrugs gehen aber an das unbeteiligte Opfer. Wie kann man sich schützen? Es gelten die üblichen Regeln für Datensicherheit. Ein E-Mail-Alert für den eigenen Namen oder eine Google-Bildersuche zeigen, ob die eigene Identität irgendwo im Netz kursiert. Auch eine Auskunft bei der Schufa (1x im Jahr kostenlos) gibt Aufschluss darüber, ob unwissentlich Handy- oder Kreditverträge abgeschlossen wurden. Ist man tatsächlich selbst betroffen, sollte man sich juristischen Beistand holen.

→ Bei Identitätsmissbrauch erstattet die Starter Kreditkarte mit Cyber-Versicherung den Schaden

Identitätsdiebstahl, ein unterschätztes Phänomen.

12%

aller Internetnutzer sind bereits Opfer geworden.

10%

der Opfer ist dadurch auch ein finanzieller Schaden entstanden.

Quelle: schufa/forsa

ÜBERSICHT

Merke ich überhaupt, wenn ich in Gefahr bin?

Tommy, 21

ÜBERSICHT

Das Antiviren-programm ist aktiv.

Die Spam-Erkennung funktioniert, also kein Grund zur Sorge? Leider nein. Es passiert immer wieder, dass auf einmal Spam von vermeintlich bekannten Adressen auftaucht. Das gleiche Prinzip gibt es auch bei SMS und Anrufen. Wenn man vom Kumpel auf einmal Nachrichten mit Links zu dubiosen Websites bekommt, nennt der Fachmann das Spoofing. Entsprechende Programme gibt es frei im Netz. Aber woher haben die Angreifer überhaupt die Kontakte? Meistens durch Datenlecks. Die Website **https://haveibeenpwned.com** erlaubt

einen Überblick. Hier kann man prüfen, ob aktuelle und alte E-Mail-Adressen irgendwo frei im Netz kursieren. Ist das der Fall, sollte man umgehend alle Passwörter ändern!

ZAHLEN, BITTE (2/5)

Die fünf größten Datenlecks der Geschichte

BETROFFENE NUTZERKONTEN

1. **3 Milliarden**
   2013: Yahoo

2. **500 Millionen**
   2013: Marriott

3. **412 Millionen**
   2016: Adult Friend Finder

4. **145 Millionen**
   2014: ebay

5. **143 Millionen**
   2017: Equifax

Quelle: csoonline.com

Online-Banking mache ich nur auf dem PC. Das ist sicherer, oder?

Lina, 24

ÜBERSICHT

Ja, aber …

Grundsätzlich gilt, dass sich Nutzer um die Sicherheit ihres Computers mehr sorgen als um die ihres Smartphones. Hat man auf dem Handy sichere Apps, über die man die Bankgeschäfte erledigt, gilt es beim PC noch ein paar Sachen zu bedenken: Selbst bei aktiviertem Antivirus-Programm und Firewall kann man Risiken durch bewusste Nutzung noch minimieren. Etwa indem man sich mit einem Nutzerkonto mit eingeschränkten Zugriffsrechten anmeldet. Das verringert die Infektionsgefahr, weil dann auch Schadsoftware nicht die Berechtigung hat, sich auszuführen. Ach ja: Wenn man seine Bankgeschäfte an fremden Rechnern erledigt, immer daran

denken, sich korrekt abzumelden und den Browser zu schließen. So vermeidet man, dass sensible Daten im Cache gespeichert werden. Wer wirklich auf Nummer sicher gehen will, besorgt sich bei seiner Bank einen sogenannten TAN-Generator, ein kleines Gerät, das die für eine Überweisung erforderliche TAN-Nummer jedes Mal neu erstellt.

→ Die Cyber-Versicherung deckt u.a. Schäden durch Missbrauch von Zahlungskarten ab

ÜBERSICHT

Was dürfen Apps auf meinem Smartphone?

Sami, 18

ÜBERSICHT

Mikrofon, Kamera, GPS-Ortung:

Smartphone-Apps wollen oft Zugriff auf Funktionen des eigenen Telefons. In den Einstellungen eines jeden Smartphones lassen sich die Berechtigungen der einzelnen Apps verwalten. Gewähren Sie nur vertrauenswürdigen Apps Zugriff auf vertrauliche Daten wie Ihren Standort und Ihre Fotos. Bei den Berechtigungen lohnt sich ein kritischer Blick: Eine Taschenlampen-App braucht keinen Internetzugriff. Grundsätzlich gilt, dass man Apps nur von den Plattformen der großen Anbieter herunterladen sollte. Es

gibt zwar auch inoffizielle App-Stores, doch hier kann jeder seine Programme ohne Prüfung anbieten. Darunter sind dann oft auch Apps, die nichts Gutes im Sinn haben. Sogenannte Krypto-Mining-Programme zapfen etwa die Rechenleistung der eigenen Geräte an, um heimlich elektronisches Geld wie etwa Bitcoins zu produzieren. Der Nutzer hat davon natürlich nichts – außer einem langsamen Handy.

→ Die Cyber-Versicherung der Starter Kreditkarte schützt in vielen Fällen vor Missbrauch

Phishing, Ransomware, Virus: Was ist noch mal was?

Alex, 26

ÜBERSICHT

Schadprogramm ist nicht gleich Schadprogramm.

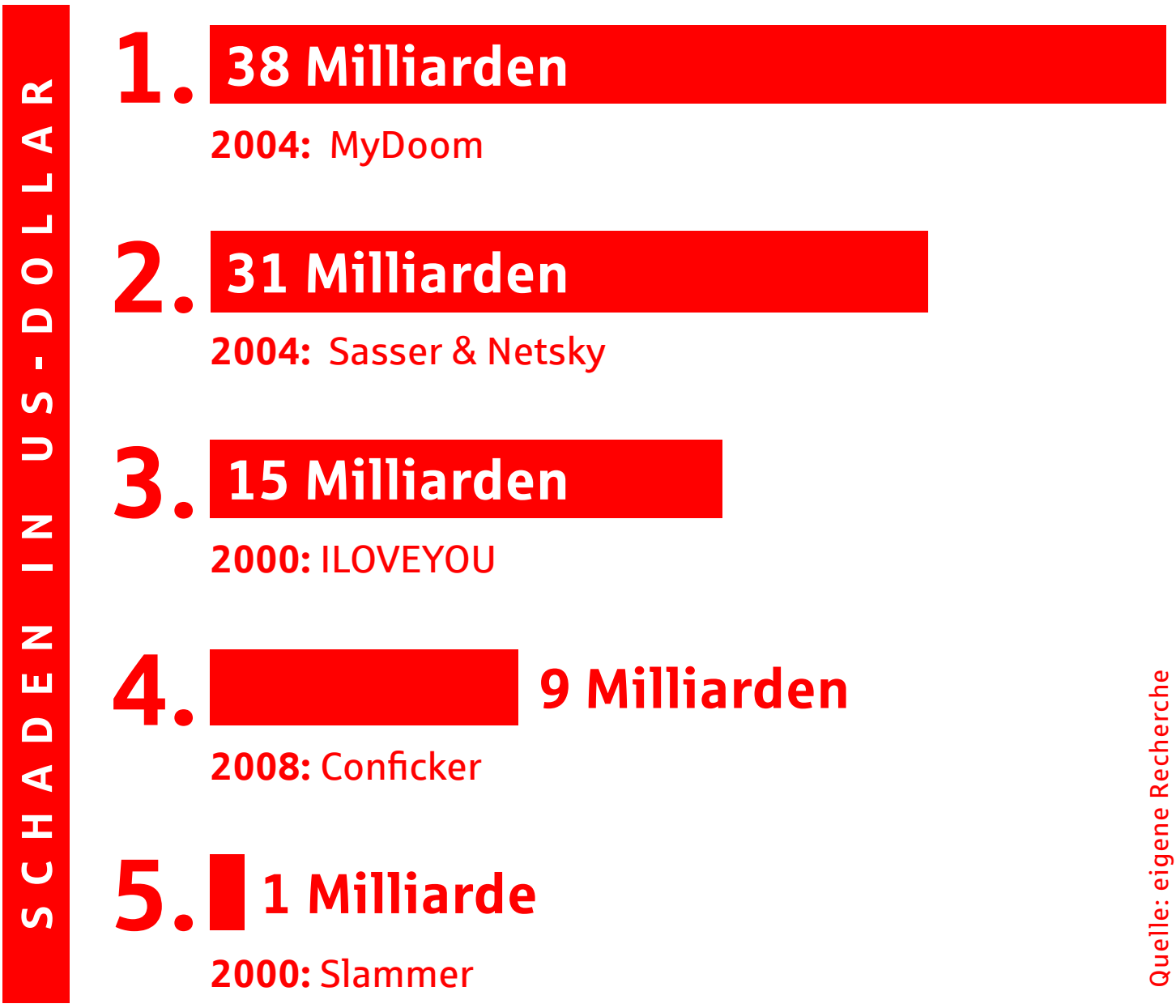
Im Fachwörter-Dschungel der IT-Welt kann man schon mal den Überblick verlieren. Zeit für einen Crash-Kurs. Die Zeiten, in denen Viren und Trojaner einfach nur dazu dienten, Computer und Software zu schädigen, sind vorbei. Auch Hacker haben heutzutage Geschäftssinn. Momentan hoch im Kurs steht sogenannte Ransomware. Also eine Software, die den eigenen Rechner verschlüsselt und erst gegen eine Zahlung von Lösegeld (Ransom) wieder freigibt. Auch die Zeiten, in denen per Spam nur dümmliche Viagra-

Werbung verschickt wurde, sind vorbei. Heute geht es vor allem um das Abgreifen (Phishing) von vertraulichen Daten mittels Links auf gefälschte Websites. Die E-Mail ist nach wie vor das wichtigste Einfallstor für Hacker. Mittlerweile berichten 83 Prozent aller Nutzer, schon mal Phishing-Mails erhalten zu haben. Unter Umständen suchen sich die Angreifer auch gezielt ein Opfer aus und versuchen, möglichst viel über dessen Leben herauszubekommen, um so überzeugender zu wirken oder Passwörter zu erraten, etwa durch Geburtsdaten oder Namen von Familienmitgliedern.Das nennt man dann Spear-Phishing oder Social Engineering.

→ Die Cyber-Versicherung deckt u.a. Schäden durch Phishing und Pharming im Internet ab

Die fünf schädlichsten Computerviren aller Zeiten

SCHADEN IN US-DOLLAR



Quelle: eigene Recherche

ÜBERSICHT

Was wissen die großen Internet-konzerne eigentlich über mich?

Fabian, 27

ÜBERSICHT

Schwer zu sagen,

das kommt schließlich darauf an, wie oft und intensiv man ihre Angebote nutzt. Wahrscheinlich aber lautet die Antwort: ziemlich viel. Selbst wenn man nicht bei Facebook eingeloggt ist, sammelt das Unternehmen Daten über die eigene Internetnutzung. Mit speziellen Anti-Tracking-Add-ons (Ghostery, Do Not Track) für den Browser lässt sich das verhindern. Zum Glück gibt es außerdem eine Reihe von sozialen Netzwerken und Suchmaschinen, die die persönlichen Informationen ihrer Nutzer gar nicht erst vermarkten. Zum Beispiel die Suchmaschine DuckDuckGo

oder der Browser Brave, die das Verhalten und die Gewohnheiten ihrer Nutzer nicht nachverfolgen. Die Ergebnisse sind gut, gerne mal ausprobieren! Denn selbst wenn man gar keinen großen Wert auf Privatsphäre legt, kann das Datensammeln der Konzerne zum Problem werden. Zum Beispiel, wenn deren Server gehackt werden.

→ Die Cyber-Versicherung erstattet Schäden durch Datenmissbrauch bis zu 15.000 €

ÜBERSICHT

Wie sichere ich meine Daten?

Sofie, 23

ÜBERSICHT

Hier mal ein paar Grundregeln:

Ein möglichst sicheres Passwort enthält Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Es sollte auch nicht leicht zu erraten sein, wenn man den Nutzer kennt (Name des Haustiers, Geburtstage etc). Ein Passwort sollte außerdem nicht im Wörterbuch stehen. Denn Online-Kriminelle nutzen sogenannte Brute-Force-Attacken. Dabei wird einfach automatisch nach und nach jedes im Duden befindliche Wort als Passwort ausprobiert, bis man Zugriff erhält. Es ist außerdem ratsam, für sämtliche Accounts jeweils ein

unterschiedliches Passwort zu haben. Aber wie merkt man sich ein paar Dutzend komplizierte Wörter und die passende Website? Ein Passwort-Manager löst das Problem. Eine kostenfreie und sichere Option ist etwa keepass.info. Die Software erzeugt Passwörter nach dem Zufallsprinzip, alle Log-in-Daten werden dort gespeichert. Geschützt werden sie durch ein Masterpasswort. Das sollte dann aber wirklich, wirklich sicher sein.

→ Die Cyber-Versicherung der Starter Kreditkarte zahlt bei Datenrettung bis zu 2.000 €

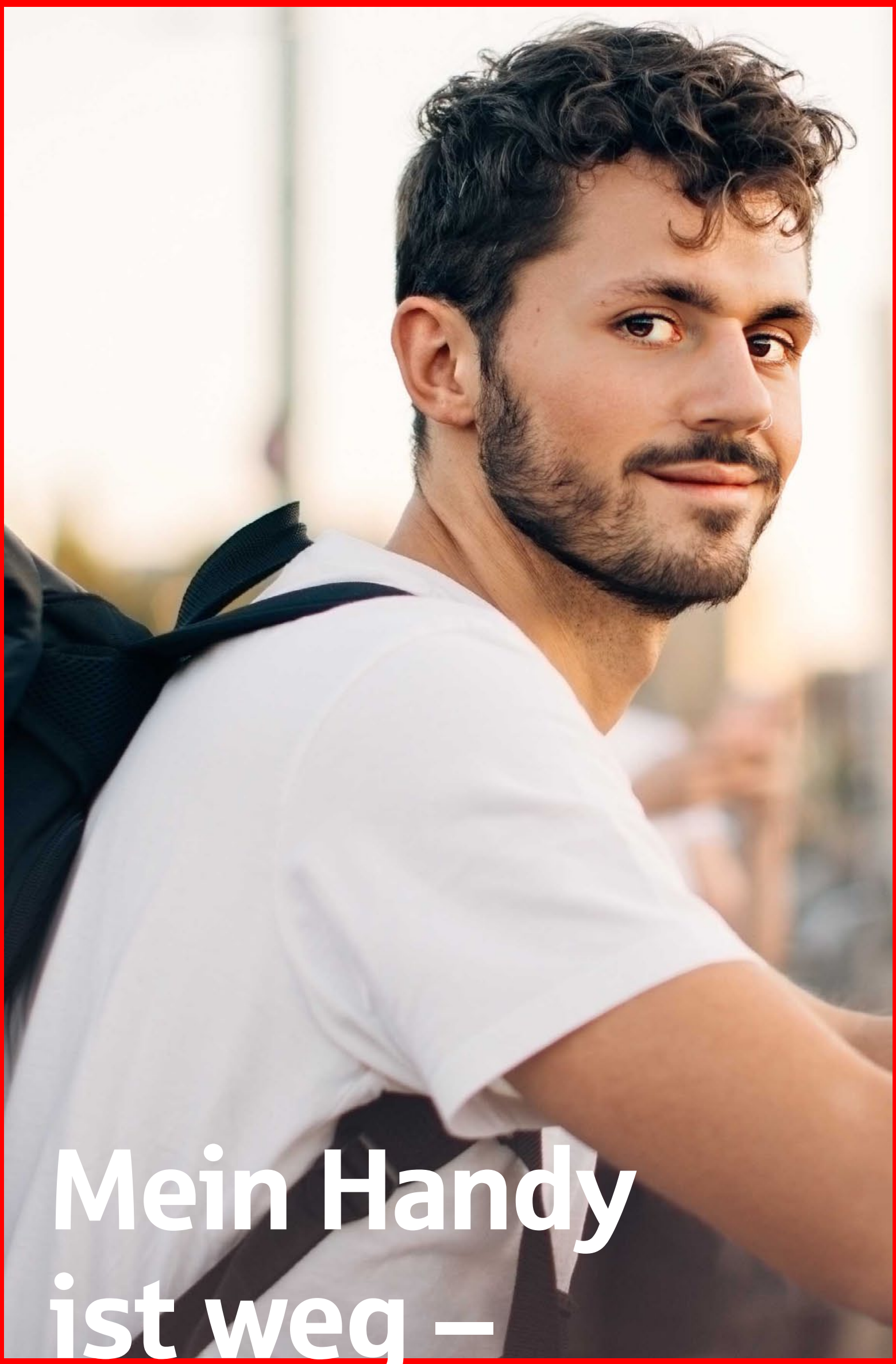
ÜBERSICHT

Die zehn häufigsten Passwörter in Deutschland 2018

1. 123456
2. 12345
3. 123456789
4. ficken
5. 12345678
6. hallo123
7. hallo
8. 1234
9. passwort
10. master

Quelle: Hasso-Plattner-Institut

ÜBERSICHT



Mein Handy ist weg – und jetzt?

Luca, 20

ÜBERSICHT

Erst mal den Schock verarbeiten.

Ohne Handy fühlt man sich halt nur als halber Mensch. Sowohl Android- als auch iOS-Geräte verfügen über eine mehr oder weniger genaue Fernortungs-funktion. Die funktioniert al-lerdings nur, wenn das Telefon auch eingeschaltet und GPS aktiviert ist. Wenn das Telefon nicht zu orten ist, sollte man zu-nächst über den Mobilfunk-Anbieter die SIM-Karte sperren. Um zu verhindern, dass ande-re Menschen auf das mit dem Handy verknüpfte Google- oder iCloud-Konto zugreifen können, sollte man eine sogenannte

2-Faktor-Authentifizierung einrichten. Dabei reicht es nicht, einfach ein Passwort einzugeben. Man bekommt zusätzlich noch einen Code etwa per SMS geschickt, der zur Entsperrung erforderlich ist. Hat man dann schließlich ein neues Gerät, kann man das Backup, das man hoffentlich rechtzeitig (und regelmäßig) angelegt hat, einfach aufspielen. Auch dafür bieten Apple und Android automatische Features an. Wie von Zauberhand sind alle Kontakte, Daten und installierten Apps wieder vorhanden. Puh.

→ Die Cyber-Versicherung bietet Unterstützung bei Sperrung von Karten und Konten

Wie geht sicheres Shopping im Netz?

Leonie, 22

ÜBERSICHT

WWW könnte gut auch

als Abkürzung für Wunderbare Warenwelt dienen. Fast jeder zweite Deutsche bestellt sich mehr als fünfmal im Monat etwas aus dem Internet. Will man aber abseits der großen Online-Shoppingplattformen einkaufen, sollte man auf ein paar Dinge achten. Einige sind naheliegend, zum Beispiel: die eigenen Kreditkarten-informationen nur eingeben, wenn Shops über verschlüs-selte Verbindungen verfügen (https). Moderne Browser zei-gen eine sichere Verbindung mit einem grünen Häkchen in der Adresszeile an. Ratsam ist es auch, auf Prüfsiegel wie Trusted

Shops zu achten, die belegen, dass es sich um seriöse Anbieter handelt. Es gibt (auch im Netz) nichts umsonst. Wenn das teure Videospiel plötzlich gratis angeboten wird, steckt wahrscheinlich ein illegaler Anbieter hinter dem Dienst. Und die finanzieren sich gerne mit dem Ausspähen von Daten oder der Verteilung von Viren und Trojanern. Bei allen legalen Geschäften gilt im Übrigen: In den allermeisten Fällen hat der Käufer bis zwei Wochen nach Warenerhalt ein Widerrufsrecht, er kann also den Kauf mit einer schlichten Begründung rückgängig machen.

→ Die Cyber-Versicherung der Starter Kreditkarte sichert Handel im Internet ab

ÜBERSICHT

Wie verhindere ich, dass ich Geld ausgebe, ohne es zu merken?

Max, 19

ÜBERSICHT

Man kennt das:

Das eigentlich kostenlose Smartphone-Spiel nervt penetrant mit Aufforderungen, kostenpflichtige Extras runterzuladen, um bessere Chancen zu haben. Das kann sehr schnell sehr teuer werden. Zum Glück gibt es sowohl bei iOS- als auch bei Android-Telefonen die Möglichkeit, In-App-Käufe komplett zu sperren. Auch bei sogenannten Abo-Fallen ist man schnell viel Geld los, wenn man nicht aufpasst. Verdächtig sind etwa fünfstellige Nummern, an die SMS gesendet werden sollen, oder teure 0900er-Nummern. Wer ganz auf Nummer sicher gehen will, kann bei seinem Mobilfunkprovider eine sogenannte Drittanbietersperre veranlassen.

Eine momentan beliebte Masche sind WhatsApp-Nachrichten, die mitteilen, dass man angeblich ein Abo abgeschlossen hat, und einen Link oder eine Handynummer angeben, um Einspruch einzulegen. In Wahrheit führen diese Nachrichten dann erst zum Abschluss des Abos. Das beste Mittel ist hier: einfach nicht reagieren. Schon seit Jahren gibt es die sogenannte Button-Lösung. Vor Abschluss eines Kaufs muss eine gut sichtbare Schaltfläche (Button) mit dem Hinweis „Jetzt zahlungspflichtig bestellen“ platziert werden muss. Fehlt der Button, ist der Kaufvertrag ungültig.

→ Die Cyber-Versicherung bietet Käufern und Verkäufern Schadenersatz bis 3.000 €

Wie wehre ich mich gegen Cyber-mobbing?

Anna, 20

ÜBERSICHT

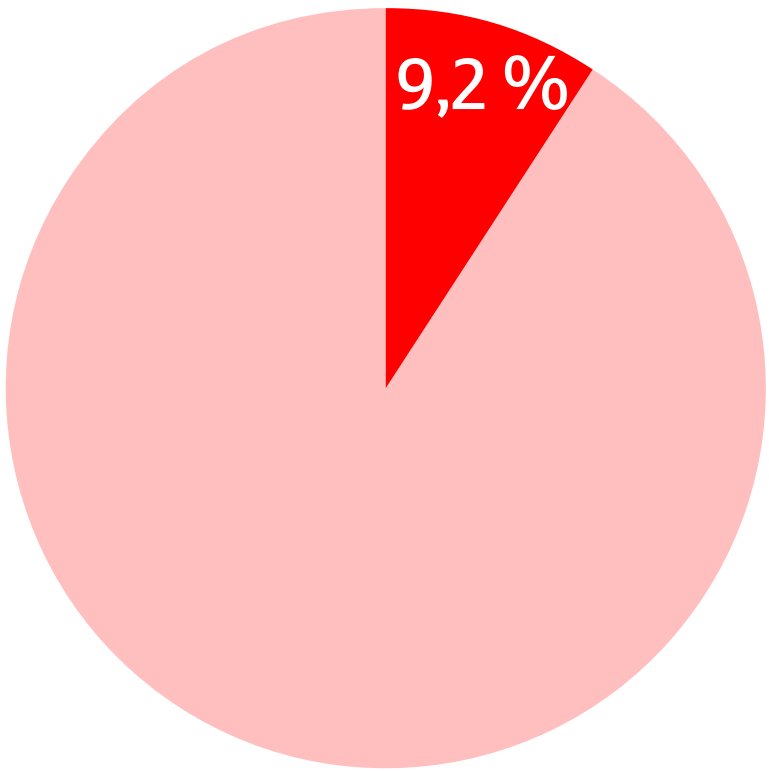
Im Netz über andere

Leute Schmutz zu verbreiten, ist unterste Schublade. Leider passiert es immer wieder. Einer repräsentativen Umfrage zufolge ist beinahe jeder fünfte junge Mensch schon mal Opfer von Cybermobbing geworden. Etwa 30 Prozent der Betroffenen geben an, dass die Mobbingerfahrung sie nachhaltig stark belaste. Ist man tatsächlich selbst betroffen, ist es vor allem wichtig, sich nicht aus der Ruhe bringen zu lassen. Das ist leicht gesagt, doch eine Reaktion ist genau das, was die Täter wollen. Außerdem: Beweise sichern. Screenshots von den betreffenden Chats oder Posts anfertigen,

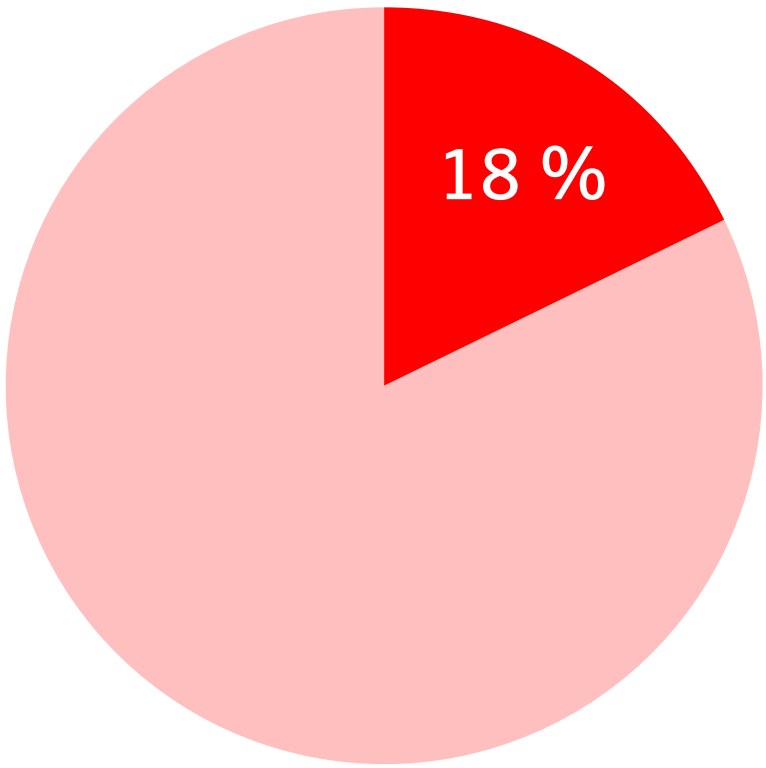
Gedächtnisprotokolle schreiben. Die entsprechenden Profile lassen sich blockieren oder stummschalten. Am besten ist es, offline eine Vertrauensperson zu suchen, das können die Eltern sein oder ein guter Freund. Unter der Nummer 116111 können sich Betroffene auch kostenlos und anonym beraten lassen. Im Extremfall muss man rechtliche Konsequenzen ziehen und die Polizei einschalten. Für die Zukunft gilt: Privatsachen bleiben auch im Netz genau das, was sie sind – nämlich privat. Persönliche Probleme sollte man nicht in sozialen Netzwerken vor einem potenziellen Millionenpublikum ausbreiten.

→ Die Cyber-Versicherung bietet psychologische Erstberatung für Mobbingopfer

Cybermobbing, ein Problem nicht nur von Jugendlichen



aller Befragten waren bereits Opfer von Mobbing im Netz.



In der Alters-klasse von 20 bis 25 Jahren sind es doppelt so viele Betroffene.

Quelle: Bündnis gegen Cybermobbing e.V.

ÜBERSICHT

Sparkasse

Die Karte für eine neue Generation.

Die Starter Kreditkarte bietet mit der einzigartigen Cyber-Versicherung den optimalen Schutz – für alle, die viel online sind. Mit Verlusterstattung bei Online-Käufen, Hilfe bei Identitätsmissbrauch und vielem mehr.

Beantragen Sie Ihre Starter Kreditkarte jetzt unter: www.sparkasse-starkenburg.de/starter

Sparkasse

Noch Fragen? Vereinbaren Sie noch
heute einen Termin mit Ihrem Berater

Sparkasse Starkenburg
An der Sparkasse
64646 Heppenheim

Telefon 06252/120-0
Telefax 06252/120-5000

info@sparkasse-starkenburg.de
www.sparkasse-starkenburg.de