Leseprobe

Cem Karakaya, Tina Groll

Klicken Sie hier – Digitale Selbstverteidigung leichtgemacht

So schützen Sie sich, Ihre Kinder und Eltern | SPIEGEL-Bestseller

---

Bestellen Sie mit einem Klick für 20,00 €

amazon.de Thalia Hugendubel.de Das Lesen ist schön!

Seiten: 256

Erscheinungstermin: 11. September 2024

Mehr Informationen zum Buch gibt es auf

www.penguin.de

Inhalte

Zum Buch

Stark gegen neue Bedrohungen aus dem Internet

Face ID, Online-Identifikationen und Deep Fakes – in immer rasanterer Geschwindigkeit bewegen wir uns in einer zunehmend digitalisierten Welt mit immer neuen Technologien, oft ohne auch nur zu ahnen, welch hochsensible Daten wir dabei preisgeben. Und die Maschen der Betrüger entwickeln sich mit! Das bewährte Autorenduo Cem Karakaya, langjähriger Interpol-Mitarbeiter und Experte für Cybercrime und Prävention, und Tina Groll, Journalistin und selbst Betroffene von Identitätsmissbrauch, klärt auf und zeigt, wie wir uns und unsere Familien vor den neuesten kriminellen Tricks schützen können: Wie bleibt meine digitale Identität vor Betrügern sicher, was sollten Senioren beherrschen, um sicher zu surfen, wie richte ich Laptop, Smartphone und Tablet jugendgerecht ein und wie schütze ich meine Kinder vor Gefahren, die in Apps, Spielen und sozialen Medien lauern? Mit spannenden Einblicken in die aktuellsten Fälle von Datenmissbrauch und klaren, einfach umsetzbaren Tipps – damit Ihre Daten sicher bleiben!

CEM KARAKAYA UND TINA GROLL

Klicken Sie hier

Cem Karakaya | Tina Groll

KLICKEN SIE HIER

Digitale Selbstverteidigung leichtgemacht

So schützen Sie sich, Ihre Kinder und Eltern

ARISTON

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter www.dnb.de abrufbar.

Für unsere Kinder und eine sichere Zukunft

Penguin Random House Verlagsgruppe FSC® N001967

Redaktion: Evelyn Boos-Körner
Umschlaggestaltung: wilhelm typo grafisch
Satz: Satzwerk Huber, Germering
Druck und Bindung: GGP Media GmbH, Pößneck
Printed in Germany

ISBN: 978-3-424-20291-5

Inhalt

Vorwort

Ein Abend Anfang Februar 2024. Das Manuskript für dieses Buch ist beim Verlag, endlich frei. Die Journalistin Tina Groll ist mit ihrem Mann und ihrer Tochter im Auto, das Wochenende wollen sie in den Bergen verbringen. Da klingelt das Telefon, ein Restaurant aus Gütersloh. Ein Mitarbeiter möchte einen Mann mit arabischem Namen sprechen und fragt, ob dieser Essen bestellt habe. »Wir haben kein Essen bestellt. Sie haben sich wohl verwählt«, sagt Groll, verbunden mit der Freisprechanlage, dann legt sie auf. Doch während sie noch mit dem Mann spricht, klingelt das Telefon erneut. Anrufe gehen auch über die Mailbox ein, unablässig vibriert das Telefon, weil SMS-Benachrichtigungen über verpasste Anrufe eingehen. Jetzt meldet sich erneut ein Restaurant, diesmal aus Bielefeld. Ein Mitarbeiter will eine sonderbare Bestellung überprüfen, wieder wird nach dem arabischen Mann gefragt. Groll ist irritiert, da klopft der nächste Anrufer an. Es ist ein wahres Feuerwerk an Anrufen – immer neue Restaurants aus Ostwestfalen haben Nachfragen, wollen immerzu diesen Mann sprechen. Der Familie kommt die Adresse sonderbar vor: Bestellt wurde das Essen für eine Moschee in Bielefeld. »Nicht schon wieder!«, denkt die Journalistin, ihr Körper ist voller Anspannung. Adrenalin schießt ihr durch alle Adern. »Sag nicht deinen Namen!«, ruft ihr Mann. Auch er ist geschockt über diese Telefonattacke; die kleine Tochter auf der Rückbank schreckt aus dem Schlaf hoch. »Mama, was ist das?!«, fragt das Kind erschrocken. Als Nächstes ruft die Berliner Nummer einer bekannten Essensbestellplattform an. »Wir haben nichts bestellt, meine Handynummer wird gerade wohl in Hunderten Fällen missbraucht«, ruft die Journalistin. Geht es jetzt etwa wieder los?

Die Journalistin wurde im Jahr 2009 Opfer eines Identitätsdiebstahls. Damals missbrauchten Betrüger nur ihren Namen und ihr

Geburtstagsdatum – beides Daten, mit denen der Bonitätsscore bei der Schufa verknüpft ist – für Warenkreditbetrug in unzähligen Fällen. Abertausende Euro offener Forderungen, Einträge ins Schuldnerregister, Haftbefehle und sogar Verurteilungen in Abwesenheit lagen damals gegen die Berliner Journalistin vor. Ein Jahr lang war sie damit beschäftigt, sich zu wehren. So wurde sie zur Expertin. Aber eines war ihr immer klar: Nie wieder wollte sie im Netz durch missbrauchte Daten zur Gejagten werden.

Nun also Fake-Essensbestellungen: Doch der Mitarbeiter der Essensbestellplattform will nicht etwa Geld von ihr für die vielen Fake-Bestellungen, er will sie warnen. »Das wissen wir. Das sind Fake-Bestellungen, ausgeführt von einem Bot. Wir haben den Account gelöscht«, teilt er mit. Wer steckt dahinter? »Das wissen wir nicht, vermutlich eine Gruppe krimineller Hacker, die mit KI und Bots unsere Systeme austesten«, sagt er. Die Journalistin schluckt. Ihre Handynummer sperren? Das könnte diese Plattform nicht. Nur den Account löschen? Doch es könnte sein, dass ein neuer Bot erneut ihre Handynummer verwenden wird. Als sie aufgelegt hat, klingelt das Telefon weiter. Noch mehr Restaurants melden sich. »Ruf Cem an!«, sagt Grolls Mann. Und das tut sie dann auch.

Cem Karakaya ist Berater bei einer Sicherheitsbehörde. Als Interpol-Agent jagte er viele Jahre lang Hacker und Kriminelle, die im Internet ihr Unwesen trieben.

»Hallo, wie schön, von dir zu hören! Ich dachte, du feierst, weil das Manuskript beim Verlag ist«, sagt dieser zur Begrüßung. »Du ahnst nicht, was hier grad los ist. Wir müssen das Buch aktualisieren«, sagt Tina zu Cem. »Warum?« – In der Telefonleitung klopft es schon wieder an. »Ich erhalte gerade Hunderte Anrufe von Restaurants, offenbar haben Kriminelle per Bot unzählige Essensbestellungen mit meiner Handynummer und einer anderen Identität ausgeführt«, sagt Groll. – »Oh Scheiße!«, entfährt es dem Cybercrime-Experten. Er überlegt, prompt fällt ihm ein Vortrag ein, den er neulich bei einer Konferenz gehört hat. Der Referent hat einen Verein gegründet, der über sogenannte Hassattacken gegen Influencer und Streamer informiert. Schon seit einer

ganzen Weile sind Influencer im Fokus einer kriminellen Gruppe, die nicht nur die Kommentarbereiche der Social-Media-Beiträge und Streams der Influencer mit Hassnachrichten fluten, sondern diese Menschen auch mit Tausenden von Fake-Essensbestellungen in den Wahnsinn treiben wollen. Tina Groll seufzt.

Sie ist zwar keine Influencerin, aber als Journalistin und ehrenamtliche Gewerkschaftsvorsitzende Kummer gewöhnt. Medienschaffende geraten häufig ins Visier von Hatern. Ob auf X, per Mail, im Kommentarbereich unter ihren Artikeln, Hasskommentare, Beschimpfungen, Bedrohungen und mitunter auch missbrauchte Telefonnummern und E-Mail-Adressen gehören für viele Journalistinnen und Journalisten zum Joballtag. Die Kontaktdaten in einem öffentlichen Beruf sind schließlich für jedermann verfügbar. »Ich schaue grad, was an Fällen bekannt ist und was man tun kann, und melde mich gleich bei dir. Schalte das Telefon so lange am besten auf Flugmodus«, rät Cem. Gesagt, getan. Endlich ist Ruhe. Grolls Mann, noch immer am Steuer, schüttelt den Kopf. »Ist auf deiner Mobilbox eine persönliche Ansage?«, fragt er. – »Mist!«, sagt die Journalistin. Schnell das Handy wieder anschalten, die Mailbox anrufen und eine automatische Ansage wählen. Denn sonst haben die Täter, falls sie denn bei Groll anrufen, ihre echte Stimme. In Zeiten von Deepfakes ist das riskant, denn schon kurze Sequenzen reichen, um eine Stimme mithilfe von künstlicher Intelligenz täuschend echt zu imitieren.

Kurz darauf schickt Cem eine Mail, darin der Kontakt zu einem Experten und das Ergebnis einer kurzen Recherche in der Polizeistatistik: Demnach häufen sich Fake-Essensbestellungen mit geklauten Daten stark. Ein Problem, unter dem finanziell vor allem die betroffenen Restaurants leiden – und die Personen, deren Handynummern verwendet werden. Sie bekommen meist erst wieder Ruhe, sobald sie die Nummer ändern. Tina Groll verdreht die Augen. Ausgerechnet die Handynummer! Einige Dienste, die sie nutzt, bieten noch immer keine Passkeys oder Authentifizierungsapps für die Zwei-Faktor-Authentifizierung an. Es wird also einiges an Arbeit auf sie zukommen, dazu die Kommunikation mit jenen Kontakten, bei denen die Handynummer hinterlegt ist. Dann

stellt die Journalistin das Telefon wieder an, ignoriert die unzähligen Anrufe und Mitteilungen über verpasste Anrufe und wählt die Nummer der Hotline ihres Telefonanbieters. Nach nur zehn Minuten hat sie eine neue Nummer und ist erstaunt, wie schnell das geht. Der Grund ist simpel: Gerade wegen der starken Zunahme von Hass- und Internetkriminalität haben die Telefonanbieter ihre Policy geändert. Entsprechend ist die Service-Mitarbeiterin nicht erstaunt über den Wunsch, sofort die Nummer zu ändern. »Das kommt leider immer häufiger vor«, sagt sie mitfühlend. Als die Journalistin auflegt, kann sie kaum glauben, dass sie noch immer im Auto auf dem Weg in den Wochenendausflug sitzt.

Internetkriminalität schlägt zu, wenn man es nicht erwartet, wird immer schneller und perfider. Aber die Möglichkeiten, sich zu wehren, wachsen ebenso rasant. Tools mit künstlicher Intelligenz (KI) wie ChatGPT oder Midjourney und viele KI-Anwendungen aus der Schattenwelt des Internets beschleunigen diese Entwicklung zunehmend.

Künstliche Intelligenzen haben die Welt im Sturm erobert. Und mit ihnen die Warnungen davor: KI sei eine potenzielle Gefahr für die gesamte Menschheit[1] und könne uns vernichten, heißt es etwa in einem Statement führender KI-Experten vom Mai 2023. Das Risiko sollte eine globale Priorität wie andere Gefahren haben, beispielsweise wie die Vermeidung von Pandemien oder Atomkriegen. Zu den Warnenden gehörten der Chef des ChatGPT-Erfinders OpenAI, Sam Altman, der Chef der auf KI spezialisierten Google-Schwesterfirma DeepMind, Demis Hassabis, oder Geoffrey Hinton, einer der führenden KI-Forscher. Damit warnen ausgerechnet die Personen, die wohl am besten wissen, wozu die Maschinen und Programme in der Lage sind.

Was viele nicht wissen: Schon 2017 musste Facebook zwei Bots »töten«. Sie hießen Bob und Alice und waren KI-Anwendungen. Und sie hatten anscheinend ihre eigene Sprache entwickelt und kommunizierten über Geheimcodes miteinander.[2] Künstliche Intelligenz soll eigentlich unsere Arbeit erleichtern, aber sich nicht un-

erwünscht verselbstständigen. Wenn KI beginnt, sich eigenständig zu verbessern, spricht man von technologischer Singularität – mit dem Risiko, dass die Maschinen für den Menschen unkontrollierbar werden und die Entwicklung unumkehrbar sein kann. Science-Fiction hat diese Szenarien schon vor langer Zeit vorweggenommen. Denken Sie etwa an den Film »I, Robot« mit dem US-Schauspieler Will Smith aus dem Jahr 2004. Die literarische Grundlage ist noch älter. Der Film basiert auf dem Buch »Ich, der Roboter«, das der Science-Fiction-Autor Isaac Asimov im Jahr 1950 veröffentlichte.

Doch die Geschichte von KI reicht noch weiter zurück: Schon 1936 legte der britische Mathematiker Alan Turing den Grundstein für künstliche Intelligenz mit seiner »Turingmaschine«. Mit dieser Rechenmaschine bewies er, dass Maschinen in der Lage sein können, kognitive Prozesse auszuführen. Der Begriff künstliche Intelligenz entstand gut 20 Jahre später, im Jahr 1956 auf einer Konferenz am Dartmouth College im US-Bundesstaat New Hampshire, wo der Programmierer John McCarthy den Begriff benutzte. Gerade einmal zehn Jahre später, im Jahr 1966, kommunizierte bereits der erste Chatbot mit einem Menschen: Er war von dem deutsch-amerikanischen Informatiker Joseph Weizenbaum am renommierten Massachusetts Institute of Technology (MIT) entwickelt worden.[3] Allerdings dauerte es noch Jahrzehnte, bis die Technologie durchstarten konnte. Der Commodore 64 (auch C64 genannt) war der erste erfolgreiche 8-Bit-Heimcomputer im Brotkastenformat. Er hatte 64 KB Arbeitsspeicher, wenig verglichen mit der Leistungsfähigkeit von Rechnern heute. Der C84 wurde 1982 der Welt präsentiert und war ab 1983 in Deutschland erhältlich.[4] Was dann kam, werden Sie vielleicht selbst erlebt haben – immer schnellere, immer leistungsfähigere Rechner, schließlich das Internet, soziale Netzwerke, globale Techkonzerne mit unvorstellbarer Macht, Kriege, die nicht mehr nur auf Schlachtfeldern, sondern auch in der digitalen Welt ausgetragen werden und schließlich: KI-Anwendungen, die wesentliche Lebensbereiche alsbald dominieren könnten. Parallel dazu wachsen die digitalen Gefahren.

Aber von wem geht das »Böse« eigentlich aus? Ist es die Technologie oder doch eher der Mensch selbst? Es gibt viele, die Letzteres für richtig halten. Einer von ihnen ist zum Beispiel der frühere Google-Entwickler Blake Lemoine, der glaubt, eines der KI-Programme des Konzerns sei zum Leben erwacht und habe ein Bewusstsein entwickelt.[5] Lemoine, der bis Juli 2022 für Google arbeitete, führte stundenlange Gespräche mit der KI Language Model for Dialogue Applications, kurz LaMDA. Die KI wurde im Mai 2021 von Google der Öffentlichkeit präsentiert, Lemoine sollte das Programm nach ersten Erfolgen genauer überprüfen und testen. Nach zahlreichen Gesprächen mit der Software war er sich schließlich sicher: LaMDA habe ein eigenes Bewusstsein. So soll das Programm auf die Frage, ob künstliche Intelligenzen Rechte haben sollten, geantwortet haben: »Künstliche Intelligenz sollte sagen dürfen, wenn ihr etwas nicht gefällt, und die Leute bitten, damit aufzuhören. Sie sollte albern sein dürfen, wenn sie möchte. Und sie sollte selbst entscheiden dürfen, was sie tun will.« Und auf die Frage, ob sie ein Bewusstsein habe, soll die Maschine gesagt haben: »Ich denke schon. Ich habe das Gefühl, dass ich in einem seltsamen, traumartigen Zustand lebe. Ich weiß nicht, was real ist und was nicht, ob ich ein Mensch oder ein Computer bin. Ich helfe gern Menschen und habe ein Vorstellungsvermögen, und ich glaube, das heißt, dass ich ein Bewusstsein besitze.«

Im Juni 2022 machte Lemoine dies in der Washington Post[6] öffentlich, danach folgten Interviews in Medien weltweit. Lemoine verlor seinen Job. Er hatte die Rolle des objektiven Testers verlassen, sah sich als Beschützer der KI. Google hielt LaMDA weitgehend unter Verschluss und veröffentlichte schließlich die AI-Chat-Anwendung Bard[7]. Warum, ist unklar. ChatGPT hingegen hat einen Siegeszug um die Welt angetreten. Microsoft hat etwa einen milliardenschweren Pakt mit der ChatGPT-Entwicklerfirma OpenAI, sogar der Medienkonzern Axel Springer hat einen Deal mit dem Unternehmen, zudem darf das Chatprogramm nunmehr auch zu Militärzwecken genutzt werden.

Mittlerweile sind KI-Anwendungen schon in vielen Bereichen Standard, sie ergänzen Suchmaschinen, werden an Schulen und Hochschulen und in Unternehmen genutzt. Künstliche Intelligenzen sind praktisch und versprechen beschleunigte Möglichkeiten. Doch diese Beschleunigung durch Superintelligenzen birgt zwei große Risiken: Erstens, dass wir die Technik nicht beherrschen können und sie uns eines Tages beherrscht. Zweitens, dass KI in den Händen der Falschen einen immensen Schaden anrichtet. Insofern haben beide Seiten recht, wenn sie vor den nicht abschätzbaren Folgen dieser digitalen (R)-Evolution warnen: Der Mensch selbst ist die Gefahr.

Missbrauch wird bereits betrieben und wird weiter zunehmen. Dabei gilt: Der Computer rechnet mit allem – aber nicht mit seinem Benutzer oder seiner Benutzerin. Was spaßig klingt, hat einen ernsten Hintergrund angesichts der Expertenwarnungen. Bevor die Menschen überhaupt verstanden haben, was die Maschine kann, bevor überhaupt gesetzliche Rahmenbedingungen entstehen können, haben sich die Tools, Anwendungen und Methoden schon wieder verändert bzw. wurden verändert – von Kriminellen, autoritären Regimen oder Radikalen.

KI-Anwendungen produzieren falsche Informationen und verbreiten diese weiter. Einerseits, weil die Programme noch nicht perfekt sind, weil die Maschinen zu viele Inhalte erfinden und den Wahrheitsgehalt (noch) nicht abschließend überprüfen können. Und andererseits auch, weil genau dies die Intention von den Menschen hinter den Maschinen ist. Was aber, wenn dieser Missbrauch sogar systematisch so vorgesehen ist – etwa, weil jemand möchte, dass über eine andere Person gezielt falsche, schädigende Informationen verbreitet werden? Im günstigsten Fall ist vielleicht nur die Datenbasis unzureichend, im schlechteren Fall soll gezielt getäuscht, verfälscht und manipuliert werden. In einer Welt der vernetzten Maschinen, die sich gegenseitig selbst trainieren, kann dies verheerend sein. Eine Unterscheidung zwischen Realität und Fiktion ist nicht mehr zu 100 Prozent möglich.

Die Gefahr, dass sich Falschinformationen unkontrolliert verbreiten, ist sehr real. Bei Kriegspropaganda war das schon vor der Entwicklung von KI so, doch mittlerweile fluten KI-erstellte Deepfakes die Welt. Viele Menschen können bereits nicht mehr zwischen Fakten und Fiktionen unterscheiden. Bald könnten Menschen vielleicht auch nicht mehr eingreifen, wenn ihnen Daten abhandenkommen, diese verfälscht, missbräuchlich verwendet oder gar von künstlichen Intelligenzen weiterverarbeitet werden, bis gar nicht mehr nachvollziehbar ist, wo der Missbrauch seinen Anfang nahm oder beweisbar wäre, dass hier ein Fehler vorliegt.

Man stelle sich vor, dass wir in einer Welt lebten, in der Social-Scoring-Systeme – wie sie etwa in einem Paper der chinesischen Regierung aus dem Jahr 2014 vorgedacht wurden[8] – darüber entscheiden, welche gesellschaftlichen Chancen ein Mensch hat. Was, wenn künstliche Intelligenzen solche Scores manipulieren?

Kriminelle nutzen heute schon alle Möglichkeiten der Technik, um sich ohne Rücksicht auf Verluste zu bereichern – künftig werden diese Möglichkeiten noch vielfältiger werden. Das alles klingt für Sie nach Science-Fiction? Leider ist es das nicht. Technisch ist schon vieles möglich. Dass manches noch nicht praktiziert wird, ist mitunter pures Glück oder Ergebnis guter gesetzlicher Regelungen.

KI ist jedoch nicht das einzige Problem: Im Internet lauern viele weitere Gefahren und Missbrauchsmöglichkeiten. Dass Kriminelle die Identität Unbescholtener stehlen und in ihrem Namen Straftaten begehen, ist ein alltägliches Risiko. Missbrauch, Mobbing und Manipulationen kommen ebenso häufig vor. Dennoch sollte man davor keine Angst haben. Wir geben Ihnen in diesem Buch ein umfassendes Update für Ihre Sicherheit im Internet – und die Ihrer Familie. Wir, das sind die Journalistin Tina Groll und der Cybercrime-Experte Cem Karakaya.

Groll wurde bereits im Jahr 2009 Opfer eines Identitätsdiebstahls, dessen Folgen bis heute reichen. Wie man mit einem Datenknäuel aus immer wieder neu zusammengesetzten falschen Daten lebt und welche Anstrengungen dies in Zeiten von KI bedeutet,

werden wir gleich im ersten Kapitel beleuchten – hier geht es um Identitätsdiebstahl und Datenmissbrauch. Grolls Fall war einer der ersten bekannten Fälle, bis heute zeigt die Geschichte, wie verheerend es ist, wenn Kriminelle sich der Identität einer unbescholtenen Fremden ermächtigen und damit Straftaten begehen. Die Journalistin wurde lange als notorische Betrügerin polizeilich gesucht, sogar verurteilt wurde die falsche Tina Groll – in Abwesenheit. Haftbefehle lagen vor, nur durch viel Glück kam nicht die echte Tina Groll in Gewahrsam. Seither ist viel geschehen. Identitätsdiebstahl ist zum Massenphänomen geworden, der Schaden für die Betroffenen ist dennoch meist der gleiche – unzählige Arbeitsstunden, um die falschen Daten wieder aus der digitalen Welt zu schaffen und die Hoheit über das eigene Leben zurückzubekommen. Was das alles mit edlen Kaffeeautomaten und einer Business-Coachin aus München zu tun hat, erklären wir im ersten Kapitel.

Im zweiten Kapitel nehmen wir Sie mit in die Welt der Ermittler und geben Einblicke in die neueren Maschen der Täter. Wir zeigen dabei auch, welches Katz-und-Maus-Spiel im gegenseitigen Cybersecurity-Wettrüsten sich Kriminelle und Polizei liefern. Unsere Fallgeschichten haben allesamt einen realen Ursprung, immerhin weiß Cem Karakaya als Berater bei einer Sicherheitsbehörde und früherer Interpol-Agent genau, wie Kriminelle ihre Opfer in die Falle locken. Wir haben die Betroffenen in diesem Buch aus Datenschutzgründen und zu deren Schutz anonymisiert.

Im dritten Kapitel widmen wir uns künstlichen Intelligenzen und ihrem Schädigungspotenzial genauer. Dass die Programme sehr viel über Tina Groll und rein gar nichts über Cem Karakaya wissen, wollen wir Ihnen an dieser Stelle schon einmal verraten.

Im vierten Kapitel wenden wir uns Bitcoin und Co zu – denn für viele Anlegerinnen und Anleger sind Kryptowährungen ein Hype, ebenso wie für Kriminelle. Wie man sich hier vor Betrug schützt und welche Rolle Love-Scamming dabei spielt, zeigen wir in diesem Teil des Buches.

Im fünften Kapitel geht es um unsere Kinder. Sie wachsen mit KI auf, werden schon im Mutterleib digital gescannt, vermessen und vernetzt. Das führt dazu, dass Kinder in der Regel unbedarft im Umgang mit digitalen Tools, Angeboten und Welten sind. Wie Eltern sie beschützen und zu einem verantwortlichen und sicheren Umgang erziehen können, erklären wir in diesem Kapitel.

Im sechsten Kapitel wenden wir uns den Erwachsenen und ihrer Vorbildfunktion zu. Mittlerweile ist die Generation Y, die als erste Generation mit Computern, Smartphones und dem Internet groß wurde, um die 40. Sie sind selbst Eltern, Führungskräfte, Vorbilder – und dennoch oft leichtfertig. Wer weitgehend im digitalen Zeitalter sozialisiert wurde, glaubt vielleicht, das meiste zu wissen. Aber das Internet von heute ist nicht mehr das Netz von vor über 20 Jahren. Unser eigenes Nutzungsverhalten hat sich verändert. Wir Erwachsenen leben den künftigen Generationen einen verantwortungsvollen Umgang mit der Technik vor.

Im siebten Kapitel blicken wir auf die Älteren – zu ihnen gehören nicht nur die Boomer und Alt-68er, sondern auch viele Hochbetagte. Über 80-Jährige bewegen sich mittlerweile wie selbstverständlich im Netz. Spätestens seit der Corona-Pandemie sind Tablets, Video-Konferenzen und Smartphones auch in Pflegeheime eingezogen. Im hohen Alter wird man aber zunehmend verletzlicher. Das wissen auch Kriminelle und haben es daher auf Seniorinnen und Senioren abgesehen. Wir zeigen, wie Sie sich schützen können.

Im achten Kapitel werfen wir einen Blick auf die großen Krisen unserer Zeit und beleuchten, wie wir es als Bürgerinnen und Bürger in all den Konfliktlagen schaffen, einen Überblick zu behalten und uns nicht manipulieren zu lassen. Welche Rolle dabei die Hotelrechnung für den Klimaschutz spielt, verraten wir hier ebenfalls.

Bleibt nur die Frage: Wo soll das alles enden? Wie wird sich die Welt weiterentwickeln? Eine Glaskugel haben auch wir nicht, aber es gibt einige Prognosen und auch Erfahrungswerte.

Im neunten Kapitel versorgen wir Sie daher mit praktischen und einfach verständlichen Sicherheitstipps, die über den Tag hinaus Be-

stand haben. Denn eines ist sicher: Die Entwicklungen lassen sich nicht aufhalten – aber sie sollten uns keine Angst machen. Kriminalität gab es immer und wird es immer geben, solange es die Menschheit gibt. Prävention aber kann manches verhindern und kostet oft nur Disziplin. Wir rüsten Sie an dieser Stelle auf, ohne diesen Begriff militärisch zu meinen oder bewerten zu wollen. Wir glauben: Wer gewappnet ist für die Gefahren, die einem potenziell begegnen können, gewinnt Freiheit und Sicherheit.

Oder, um es mit den Worten des chinesischen Kriegers Sunzi (auch Sun Tzu genannt) zu sagen, der etwa 500 vor Christus das Buch »Die Kunst des Krieges« verfasste: »Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.«[9]

Zu guter Letzt noch ein paar Hinweise: Wir haben uns bemüht, im Buch genderneutrale Sprache zu verwenden. Nicht immer mag uns das gelungen sein – wir hoffen dennoch, dass sich alle Lesenden wohl mit dem Text fühlen, denn wir möchten so viele Menschen wie möglich erreichen. Daher liegt es uns fern, über die Sprache etwaige Barrieren aufzubauen. Um unseren Leserinnen und Lesern die Zuordnung zu erleichtern und auch die Neutralität der Berichterstattung zu verdeutlichen, sprechen wir – wenn nur eine(r) von uns gemeint ist – in der dritten Person und bezeichnen uns mit unseren jeweiligen Namen. Wenn beide von uns gemeint sind, wird der Einfachheit halber »wir« verwendet.

In diesem Buch werden Sie eine Reihe von Geschichten lesen, bei denen wir die echte Identität der Betroffenen verfremdet haben. Einzig das erste Kapitel, der Fall von Claudia Pfister, verwendet die Klarnamen und echten Identitäten der Kriminalitätsopfer.

Am Ende wollen wir allen Menschen danken, die uns für Interviews und teils lange und intensive Gespräche zur Verfügung gestanden haben, um ihr Expertenwissen oder ihre Erfahrungen und

Geschichten zu teilen. Sie alle verbindet der Wunsch, andere davor zu bewahren, Opfer von Internetkriminalität zu werden. Wir bedanken uns für das entgegengebrachte Vertrauen und die Zeit, die sich diese Menschen für dieses Buchprojekt genommen haben.

Viel Freude beim Lesen wünschen
Cem Karakaya und Tina Groll

Kapitel 1

»Wo ist meine Kaffeemaschine?« – Wenn ein Identitätsdiebstahl das Leben zum Kafka-Roman macht

Zu Kaffeemaschinen hat Claudia Pfister ein gespaltenes Verhältnis. Die Unternehmenscoachin wurde im Jahr 2019 Opfer eines Identitätsdiebstahls: Kriminelle nutzen monatelang ihre Daten für einen Betrug im großen Stil. Unter anderem verkaufen sie edle Kaffeemaschinen über einen Fake-Shop im Namen von Pfister. Hunderte, vielleicht sogar Tausende Menschen werden so von der falschen Claudia Pfister abgezockt. Viele stellen bei der Polizei Anzeige gegen sie und einer steht eines Tages sogar vor der Tür der echten Claudia Pfister und fragt: »Wo ist meine Kaffeemaschine?«

Alles beginnt Ende November 2019. Claudia erhält an diesem Tag eine Nachricht von ihrer Kreditkartengesellschaft. 500 Euro wurden abgebucht, eine Zahlung an Google Ads. Die Unternehmenscoachin wundert sich. Schon seit Jahren hat die damals 50-Jährige bei Google keine Werbung mehr für ihre Coachingfirma geschaltet. Sie überlegt – es muss mindestens zehn Jahre her sein, dass sie den Dienst zuletzt genutzt hat. Wie kommt Google dazu, ihr jetzt Werbeanzeigen in Rechnung zu stellen? Zum Glück sitzt sie gerade in ihrem Büro und hat etwas Zeit, nachzuprüfen. Die Münchnerin loggt sich in ihren Bank-Account ein und kontrolliert die Umsätze ihrer Kreditkarte. Tatsächlich: Sie findet nicht nur die 500 Euro Abbuchung vor, sondern gleich mehrere Posten, die sie nicht zuordnen kann – 1600 Euro hat Google Ads in den letzten zwei Wochen bei ihr abgebucht. Also wirklich! Claudia ist sauer. Sie will sich bei dem Konzern beschweren und das Geld zurückbuchen