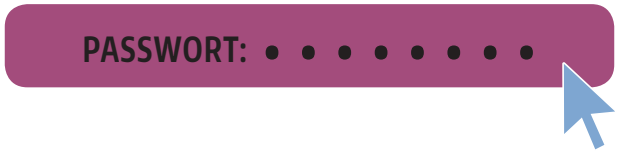
DER

# CYBER SURVIVAL GUIDE

NICK SELBY • HEATHER VESCENT

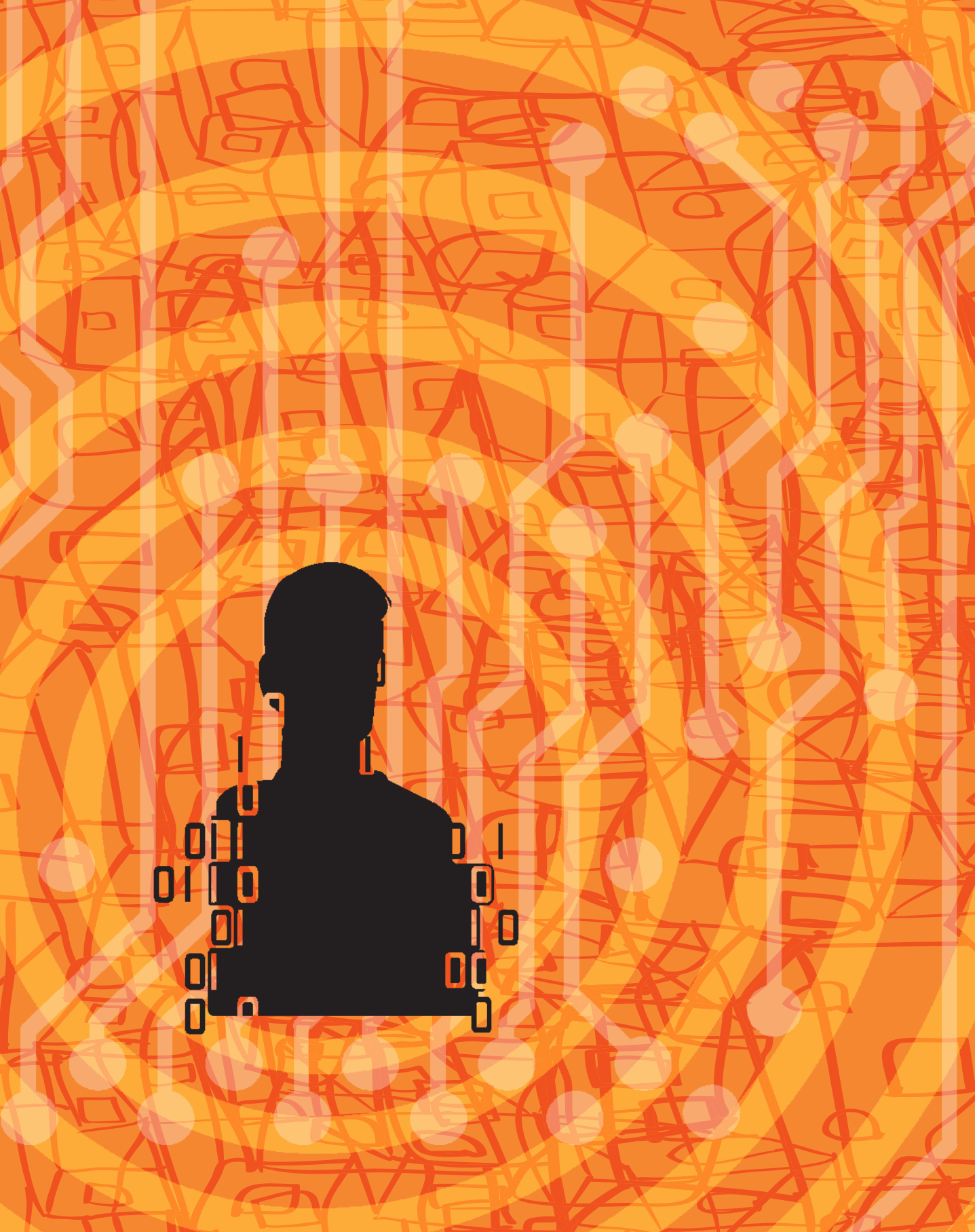
# DER CYBER SURVIVAL GUIDE

## SO WEHREN SIE SICH ERFOLGREICH GEGEN HACKER, STALKER UND ANDERE CYBER-GANGSTER




Illustriert von
ERIC CHOW
und Conor Buckley

FRANZIS



# INHALT

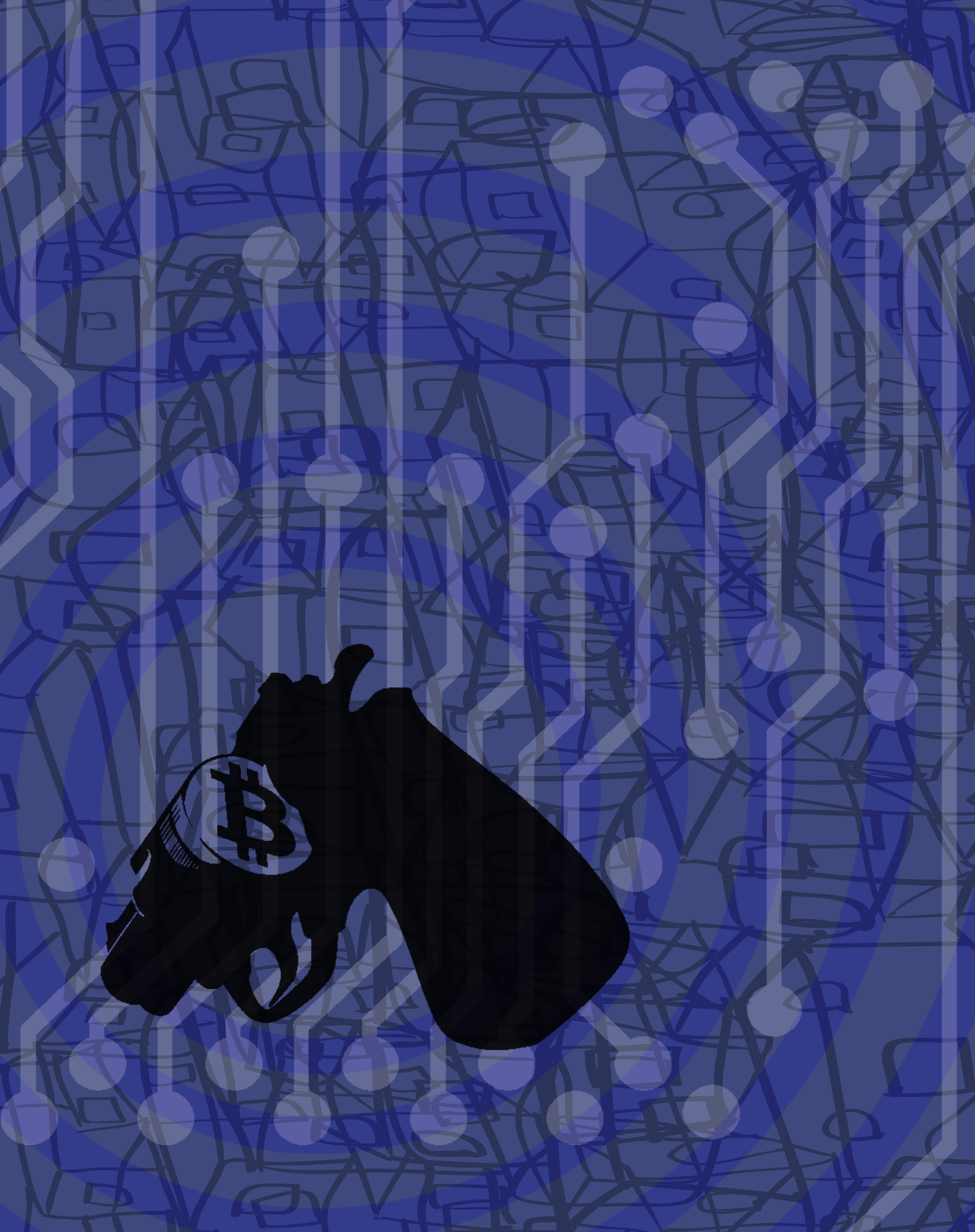


## IHR LEBEN HACKEN



# DIE GESELLSCHAFT HACKEN





# DIE WELT HACKEN



# DIESES BUCH IST JETZT SCHON VERALTET (UND DAS IST OKAY)

Fast jeden Tag gibt es eine neue Meldung über Cyberkriminalität: Millionen gestohlene Kreditkarten, private Star-Fotos geleakt, ausländische Agenten, die in höchsten Regierungskreisen mitmischen. Es ist selbst für den aufgeklärtesten Leser schwer zu wissen, wie viel davon wahr und wie viel Panikmache im Sinne von Clickbaiting ist. Wie soll man sich verhalten? Leider lassen sich viele Menschen von ihrer Angst so sehr lähmen, dass sie nichts unternehmen oder einfach alles ignorieren, weil es ihnen zu viel ist.

Der Punkt ist, dass jeder von uns ganz und gar auf Cyber-Sicherheit angewiesen ist, sowohl in offensichtlichen als auch in unerwarteten Fällen. Als Polizeibeamter klopfte ich bereits schroff an die Tür eines Verdächtigen in einem Cyber-Fall und stand plötzlich einem 78-jährigen Rentner gegenüber, der, abgesehen von seiner Vorliebe für spezielle, etwas schmierige, aber legale Pornos, völlig unschuldig war. Auf der Suche nach kostenlosen Legal-aber-schmierig-Pornos hatte der Mann einen Anfängerfehler begangen, weil er die oberste Regel im Netz nicht kannte: Wenn du nicht weißt, wie eine Seite Geld verdient, bist du selbst das Produkt. Kriminelle hatten in seinen Schmuddelfilmen Malware versteckt und vermieteten ohne sein Wissen den Fernzugriff auf seinen Computer an Internetbetrüger.

Manche der von uns hier beschriebenen Hacks sind bereits morgen ein alter Hut. Andere präsentieren sich in neuer und hinterhältigerer Form. Aber auch Neues wird dabei sein, auf jeder Seite. Das ist okay – dieses Buch gibt Ihnen das nötige Wissen, zu verstehen, wie Ihr digitaler Fußabdruck für Kriminelle, die Werbung, Ermittler und Regierungen aussieht und wie Sie Ihre eigenen Schwachstellen erkennen und beheben, auch wenn sich die spezifischen Schwachstellen ändern.

Wir können nicht alles vorhersehen, was Ihnen passieren könnte – die neuesten Bedrohungen werden gerade erst ausgedacht, in Kellern und Laboren von Missouri bis Moldawien. Aber wir können Ihnen zeigen, wie Sie das Risiko minimieren. Sicherheitsexperten sprechen gerne über OPSEC (Operations Security, dt.: Feind-hört-mit-Prinzip). Und OPSEC ist OPSEC – heute und morgen. Es geht nicht um spezifische Gefahren, es geht darum, auf gewisse Fälle vorbereitet zu sein.

Verstehen Sie das digitale Universum und die Konsequenzen Ihres Handelns, um sich nicht zum Opfer machen zu lassen, ohne auf all das, was das Internet zu bieten hat, verzichten zu müssen. Dieses Buch gibt Ihnen das nötige Wissen, die verschiedenen Bedrohungen da draußen besser zu verstehen, und zeigt Ihnen Mittel und Wege, sich selbst zu schützen. Der Rest liegt bei Ihnen.

NICK SELBY

# DIESES BUCH WIRD IHNEN AUCH ANGST MACHEN (UND DAS IST AUCH OKAY)

Einfach ausgedrückt: Sie sind in Gefahr, Ihre Identität, Ihre Bankkonten, Ihre Kinder. Selbst Ihre Regierung ist anfällig für Angriffe von Cyberkriminellen auf der ganzen Welt. Das sollte Ihnen Angst machen. Aber dieses Buch ist viel mehr als eine Sammlung furchteinflößender Geschichten (obwohl es auch das ist). Es ist auch ein Toolkit, mit dem Sie sich in einer immer gefährlicher werdenden Onlinewelt schützen können.

Das digitale Zeitalter hat uns wie auf dem Silbertablett eine große Bandbreite an Produkten und Services serviert, aber auch neue und oft unvorhergesehene Probleme verursacht. Die Sicherheitstechnologie wird sich ständig verbessern – und Verbrecher werden immer neue Wege finden, eben diese Technologie zu umgehen. Das ist unser Stichwort.

Wie funktioniert Sicherheit in der modernen Welt? Die meisten Leute wollen vor allem wissen, wie sie einen Hackangriff verhindern können. Das ist der falsche Ansatz. Es ist fast unvermeidlich, dass Sie irgendwann einmal gehackt werden.

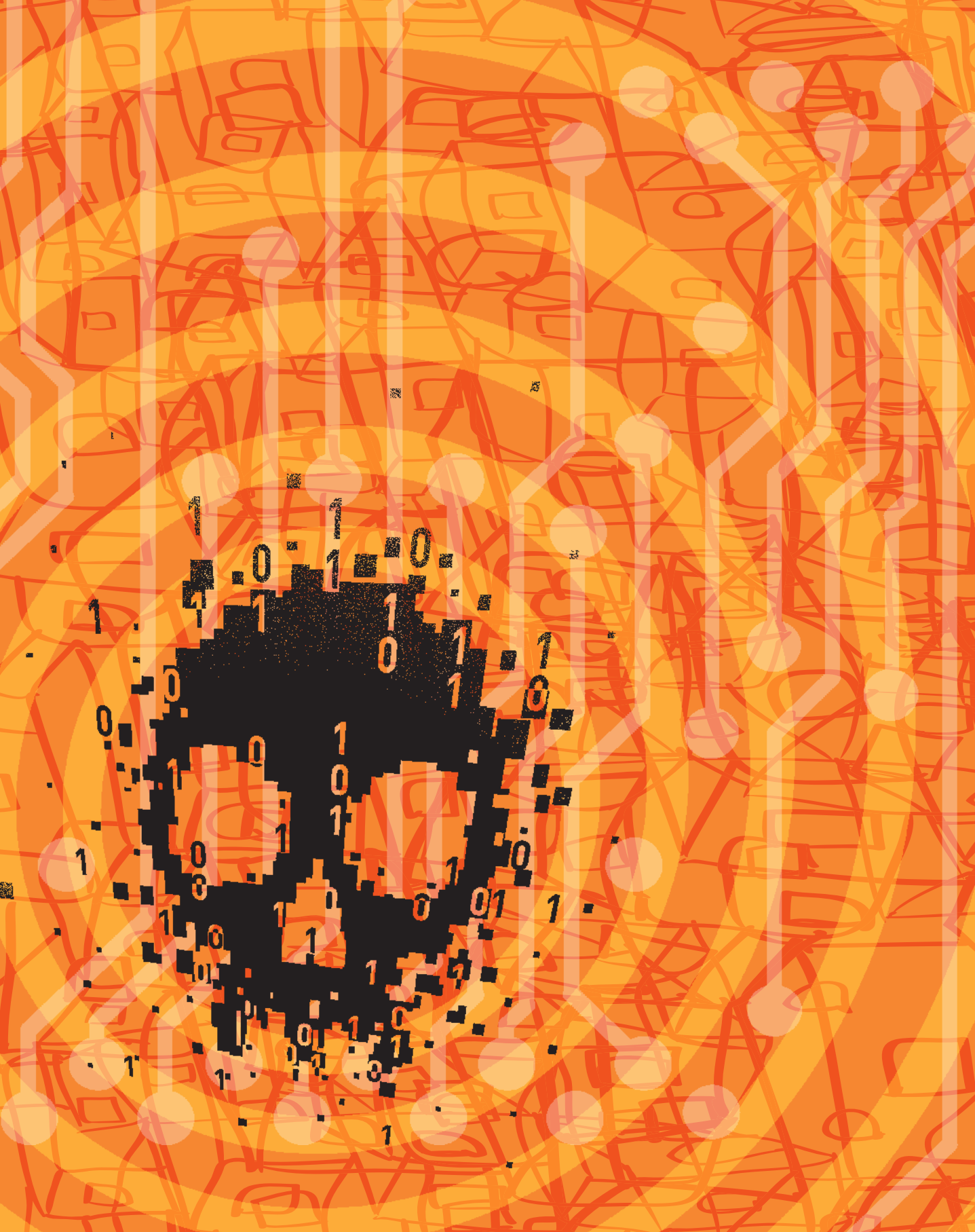
Beginnen wir damit, dass sogar die sichersten Technologien verwundbar sind. Es herrscht Krieg zwischen kriminellen Hackern und Sicherheits-

experten, und daran wird sich nichts ändern. Wir können nur „gewinnen", wenn wir davon ausgehen, gehackt zu werden, und Vorkehrungen treffen, um zu sichern, was uns wichtig ist. Wenn Sie mit dem unausweichlichen Hack Ihres Sicherheitssystems rechnen, werden Sie die Risikofaktoren erkennen und Ihre eigene Sicherheit kontinuierlich überwachen. Sie wissen, wo Sie verwundbar sind und wie Sie sich schützen können.

Wie treffe ich die nötigen Sicherheitsmaßnahmen? Das ist leicht. Lesen Sie dieses Buch! Viele der in diesem Buch aufgezeigten Schwachstellen können relativ leicht behoben werden, wenn Sie erst einmal das nötige Know-how besitzen. Sie brauchen nicht das sicherste aller Systeme, sondern nur das beste für Ihre Bedürfnisse. Sie sind nicht sicher, welche Anforderungen Sie haben? Wir helfen Ihnen dabei, das herauszufinden.

In gewisser Hinsicht helfen uns Hacker auf ihre eigene Art und Weise. Wann immer sie ein System knacken, lernen wir etwas Neues über dessen Schwachstellen und wie wir es sicherer machen können. Ich persönlich bin schon gespannt auf die neuen und aufregenden Tricks, mit denen Hacker die Grenzen jeder neuen Technologie aufzeigen werden. Ich will bloß nicht, dass sie diese Grenzen an Ihnen aufzeigen!

**HEATHER VESCENT**



# IHR LEBEN HACKEN

Ihr Bankkonto ist plötzlich und unerklärlicherweise überzogen. Ihre Freunde bekommen eine verzweifelte E-Mail von Ihnen mit der Bitte um Geld. Sie fallen bei einer Routine-Hintergrundüberprüfung durch. Ihr Fernseher bekommt auf einmal mysteriöse Fehlermeldungen. Was geht hier vor? Cyberkriminalität kann Sie daheim treffen – was immer alltäglicher wird, während sich unsere Welt vernetzt und Hacker immer schlauer werden. Die folgenden Kapitel erklären Ihnen, was zu tun ist, wenn die Internet-Bösewichte Sie persönlich angreifen – Ihre Identität oder Ihr Geld stehlen, in Ihre Privatsphäre eindringen, Ihre Kinder mobben und Ihre Familie bedrohen. Wir beleuchten auch einige weniger bekannte Schwachstellen auf Ihrem Smartphone, bei Ihren Browsing-Gewohnheiten und sogar Ihren Haushaltsgeräten und zeigen Ihnen, wie Ihre persönlichen Daten sicher bleiben.

# SCHÜTZEN SIE IHRE IDENTITÄT

**ID-DIEBE KAUFEN, VERKAUFEN UND MISSBRAUCHEN IHRE IDENTITÄT FÜR GELD ODER ANDERE LEISTUNGEN – ODER NUTZEN IHREN NAMEN, IHRE BONITÄT ODER IHRE VERSICHERUNG FÜR EINEN KREDIT ODER KOSTENLOSE MEDIZINISCHE VERSORGUNG.**

Es gibt unzählige Wege, wie die Bösewichte an Ihre Informationen kommen und sie zu allen möglichen Zwecken verwenden – vor allem, um Ihr Geld zu stehlen, doch auch für andere Betrügereien oder um Spuren von anderen Verbrechen zu verwischen. Das ist einer der Hauptgründe, warum Identitätsdiebstahl so verheerend ist. Wenn ein Verbrecher Ihre Kreditkarteninfos stiehlt, wird Ihre Bank wahrscheinlich das verlorene Geld rückerstatten. Wenn derselbe Kriminelle sich für Sie ausgibt, um einen internationalen Kinderpornografie-Ring zu betreiben, dann ist Ihr Problem um einiges größer ... vor allem, da viele Gesetzeshüter nicht auf dem neuesten Stand der Cyberkriminalität sind und „Das war ich nicht" somit nicht wirklich zählt.

Was passiert genau? Auf den folgenden Seiten sehen wir uns die vielen Methoden des ID-Diebstahls an und zeigen, wie Sie sich davor schützen oder dagegen ankämpfen, wenn Sie bereits Opfer geworden sind. Dies reicht von einfachen Methoden, wie dem Durchstöbern Ihres Müllcontainers nach ungeschredderten Finanzdokumenten oder dem Stehlen der neuen Kreditkarte, die die Bank Ihnen unerwarteterweise zugeschickt hat, bis hin zu ausgefeilten Einbrüchen in Datenbanken und anderen Hacks, ausgeführt von großen Verbrechersyndikaten vom anderen Ende der Welt aus, um Cyberterrorismus-Operationen zu finanzieren..

**AMERIKAS ERSTER ID-BETRUG**

Philip Hendrik Nering Bögel hatte finanzielle Probleme, doch er war ein kreativer Kopf. Also handelte der Holländer im Jahr 1793, als es ihm zu brenzlig wurde (zu der Zeit wurde er wegen Veruntreuung gesucht), wie jeder vorausdenkende Identitätsdieb heute: Er verließ die Niederlande auf schnellstem Weg und gründete auf dem amerikanischen Kontinent eine neue Stadt, ganz wirtschaftlich gedacht und davon überzeugt, dass ein Bögel mehr verdient hätte. Unter dem Namen „Felipe Enrique Neri, Baron von Bastrop" erwies sich Bögel für die frühen texanischen Anführer Moses und Stephen F. Austin bei der Beschaffung von Landzuweisungen als besonders hilfreich. Zum Oberbeauftragten in Grundangelegenheiten von Texas ernannt, gründete er dort eine Stadt und benannte sie nach sich selbst. Heute kann Bastrop, Texas, 5.340 Einwohner, feiern, dass Amerikas erster erfolgreicher ID-Betrug einem einzigen Menschen eine ganze Stadt einbrachte.

W/F

## „ICH BIN KEINEN DIEBSTAHL WERT!“

**FALSCH** Angreifer sind klug und auf schnellen Erfolg aus. Oft sind Sie der schnellste Weg zum Erfolg. Sie meinen vielleicht: „Ich habe doch nur Fotos von meinen Enkelkindern auf meinem Computer.“ Aber Ihr Rechner ist mit dem Internet verbunden, was ihn zu einem Angriffsziel macht. Hacker infizieren Computer und machen sie zu einem Teil eines globalen Netzwerkes von Spam, Angriffen auf andere Computer und anderen bösartigen Aktivitäten. Hacker, die Ihren Computer infizieren, können auch Ihre Finanzdaten abrufen, wenn Sie Onlinebanking machen. Es kommt auch vor, dass Hacker einen Computer zerstören und für Sie wichtige Fotos für immer verloren gehen.

**VIELE IDENTITÄTSDIEBE** geben sich online für Sie aus, und das aus vielen Gründen und auf viele Arten. Für Cyber-Stalker (siehe Amanda Nickersons Geschichte, Seite 50-51) ist die Imitation für gewöhnlich Teil eines größeren Cyber-Mobbing-Unterfangens. Doch meistens geht es um Geld. Ob Kriminelle Kontokarten oder Darlehen in Ihrem Namen bekommen, in Ihrem Namen anschreiben oder in Ihrem Namen Ihr Guthaben ausschöpfen, ID-Klau ist meistens ein erster Akt, auf den sich viele weitere kriminelle Vorhaben türmen. „Identitätsdiebstahl“ ist daher tatsächlich eine Kategorie in der Cyberkriminalität.

Obwohl die Opfer meist von der Bank oder der Kreditkartenfirma entschädigt werden, ist der Schaden des Identitätsdiebstahls über Jahre hinweg spürbar. Ihre Bonität und Ihre finanzielle Geschichte sind Banken, Autohändlern und anderen Anbietern von Darlehen wichtig und entscheidend dafür, ob Sie ein Risikokandidat sind. Solche Minuspunkte lassen sich nur schwer ausradieren.

**Der Trick mit den Steuern** Eines der am schnellsten wachsenden Verbrechen in Amerika ist Steuerbetrug: ein Betrug, der ID-Dieben Tausende Dollar beim Finanzamt einbringt. Die Verbrecher nehmen Ihre Sozialversicherungsnummer und Ihre persönlichen Informationen und erschaffen eine Steuererklärung in Ihrem Namen, mit einer kleinen Überzahlung auf Ihrer Seite. Die Erklärung wird über eine Software abgegeben, und ein paar Tage später überweist das Finanzamt eine Rückzahlung an „Sie“ – an die vom Dieb angegebene Adresse –, meist über Prepaid-Kreditkarten, die gegen Geld oder Güter getauscht werden können.

### ARTEN VON IDENTITÄTSKLAU

Betrüger stehlen nicht einfach nur Ihren Führerschein oder Ihre Kreditkarte. Sie nehmen Ihre gesamte Identität an und nutzen jeden kleinsten Teil für sich.

## FALLSTUDIE

**FREMDE MIT SÜSSIGKEITEN** 2004 führte InfoSec ein Experiment durch: Sie boten Passanten auf der Straße einen Schokoriegel an, im Austausch für ihre Login-Daten und ihr Passwort am Arbeitsplatz. Überraschenderweise gaben um die 70 Prozent diese Informationen preis – die Hälfte sogar ohne die Schokoladen-Bestechung. Man möchte meinen, das hätte so manchen wachgerüttelt. Und tatsächlich, staatliche Agenturen und private Firmen geben Millionen dafür aus, ihren Angestellten das richtige Sicherheitsverhalten beizubringen. Ob das fruchtet? Als das Experiment 2008 in London wiederholt wurde, war kein Unterschied zu bemerken.

Ob die Gründe nun kulturell oder technisch sind, Fakt ist, Menschen können Passwörter nicht gut für sich behalten. Sie nehmen das Thema einfach nicht ernst. Noch ärgerlicher für jene, die Unternehmen und ihren Angestellten ein besseres Sicherheitsverständnis näherbringen wollen, ist, dass „dein Passwort" immer noch wörtlich genommen wird. Die meisten benutzen immer noch ein einziges Passwort für viele oder alle ihre Konten – und noch dazu ein schwaches (siehe Seite 28 zum Erstellen eines sicheren Passworts).

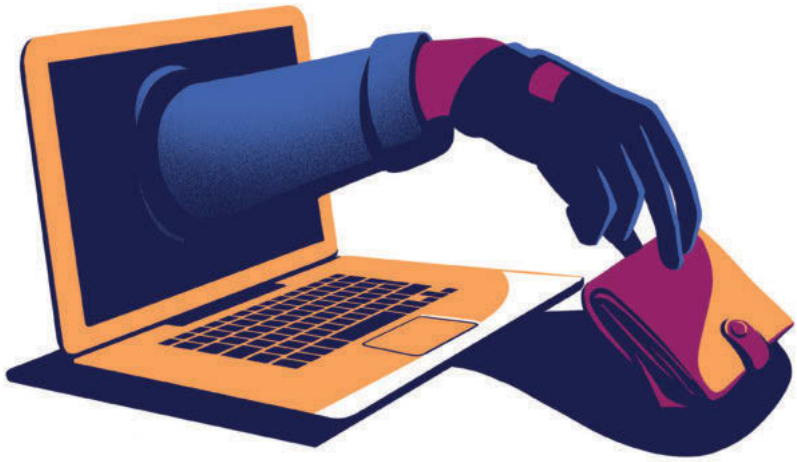
Sie glauben vielleicht, dieses Problem wäre mit Passwort-Manager-Apps gelöst worden, da diese das schwierige Erfinden (vom Erinnern gar nicht zu reden) eines starken Passworts, zum Beispiel das immer beliebte 98cLKd2rh29#36kasg!, wesentlich vereinfachen. Diese Programme sind noch dazu sehr benutzerfreundlich und können die Passwörter für alle ihre Onlinekonten automatisch ändern.

Als 2016 ein Sicherheitsberater den Schokoriegelversuch nochmals durchführte, doch dieses Mal das „beste" Passwort Preise gewann, von Süßigkeiten bis hin zu einer Flasche Champagner, war das Ergebnis endlich ein anderes: schlechter als je zuvor.

## SICHERHEITS-BASICS

### WICHTIGE ZAHLEN

Denken Sie dreimal darüber nach, bevor Sie Ausweis- oder Versicherungsnummern hergeben, selbst wenn eine rechtmäßige Stelle danach fragt. Anhand solcher Nummern sind Sie identifizierbar. Es zahlt sich immer aus, darüber nachzudenken, warum diese Information nötig ist, und nicht damit herauszurücken, wenn es nicht absolut notwendig ist. In den USA ist die Sozialversicherungsnummer ein universelles Identifizierungszeichen, und ich würde eher eine Kaution auf den Tisch legen, um Strom oder eine Telefonleitung zu bekommen, als dem Elektrizitätswerk meine Identifikationsnummer auszuhändigen. Schon viele Anschlüsse wurden ganz simpel gehackt, und ID-Diebstahl wächst auf dem Nährboden der Sozialversicherungsnummern. Wenn nicht notwendig, geben Sie die Nummer nicht her.



**WIE SIE ES TUN** Verbrecher stehlen auf verschiedene Arten die Identitäten, die sie missbrauchen wollen, von technisch einfachsten bis hin zu Geheimdienstmethoden. Einst die üblichste Art, ist der Diebstahl von Papieren oder der Geldbörse immer noch beliebt, doch heute eine Angelegenheit von Kleinkriminellen. Trotzdem kann immer noch einiger Schaden entstehen, wenn jemand Ihre Geldbörse stiehlt und Ihre Ausweise und Kreditkarten benutzt. Auf ähnliche Weise kann ID-Klau geschehen, wenn jemand Ihren Müll durchwühlt und Kontoauszüge mit Kontonummer, Kontostand und Datum findet. Solche Details ermöglichen es Dieben, Ihre Karten als verloren zu melden, Ihre Adresse zu ändern und Ersatzkarten zugeschickt zu bekommen.

Andere Möglichkeiten, Ihre Identität zu erbeuten, reichen vom physischen Diebstahl von persönlichen Schreiben von Dienstleistern bis zum Eindringen in ein Computernetzwerk, um Daten zu stehlen. Eine weitere populäre Vorgehensweise ist Phishing (siehe Seite 24).

Doch natürlich ist die am weitesten verbreitete Methode des massenhaften Identitätsdiebstahls die durch einen groß angelegten Einbruch in das Netzwerk eines Händlers, einer Bank, eines Versicherungsanbieters oder einer Regierungsbehörde. Das bringt den Dieben am meisten ein und liefert ihnen die meisten Angriffsziele. Die Grafik auf der nächsten Seite zeigt, wie so etwas funktioniert.

**Einen Schritt vor dem Gesetz** Für die Behörden ist es sehr schwierig, Identitätsdiebe aufzuhalten oder zu belangen. Da ein Großteil des Betrugs aus der Ferne und über Online-Tools passiert, ist das Fassen der Verbrecher schwer. Hinzu kommt die globale Natur des Internets, dank der die Diebe nicht einmal im jeweiligen Land sein müssen, um ihre Verbrechen auszuüben. Und ID-Diebstahl kann passieren, ohne dass sich das Opfer darüber im Klaren ist.

## WIRKLICH PASSIERT

**ALUHÜTE** Es ist ein bekanntes Phänomen, dass manche Menschen so paranoid sind, dass sie sich einen Hut aus Alufolie überziehen. Das Witzige daran: Vielleicht wäre das manchmal gar keine so schlechte Idee.

Es gibt viele Wege des Datenklaus, und einige beruhen auf heimlichen Übertragungen. Das beste (oder zumindest coolste) Beispiel dafür war der sowjetische Hack gegen die Schreibmaschinen IBM Selectric II und III in den 1970ern. An die fünfzehn dieser Schreibmaschinen standen in der US-Botschaft in Moskau und dem Konsulat in Leningrad und wurden von sowjetischen Spionen mit einem Gerät manipuliert, das die magnetischen Schwankungen des kleinen Selectric-Balls maß. Wie sich herausstellte, hatte jeder Buchstabe eine eigene Signatur. Durch einen Empfänger in der Wand (die Gebäude wurden von den Sowjets gebaut) konnten die Sowjets alles einsehen, noch während es von den Sekretärinnen geschrieben wurde.

**WAS MACHT SIE VERWUNDBAR?** Die riesige, multimilliardenschwere Industrie der Cyberkriminalität kann in drei Basiskategorien unterteilt werden, jede mit ihren eigenen Zielen, auch wenn es unterm Strich um das Gleiche geht: Sie wurden reingelegt. Die Unterschiede und was genau vor sich geht zu verstehen, ist für Ihre Sicherheit ausschlaggebend. Sehen Sie selbst, wie es läuft.

## SIE SIND

### DAS ZIEL

DAS BEDEUTET

ein Feind hat Sie auf hochpersönlicher Basis im Visier.

DER HACKER WILL VIELLEICHT

Geld aus Ihrem kleinen Onlinegeschäft abziehen.

ALSO WIRD ER ODER SIE

eine E-Mail mit spezifischen Details an Sie schreiben, um Sie zu überzeugen, dass er für Ihren Websiteanbieter arbeitet.

UND DANN

geben Sie Ihrem vermeintlichen Anbieter die Login-Daten für Ihr Konto.

DAS ERLEDIGT,

loggt sich der Hacker ein, löscht Ihre Seite und ändert Ihr Passwort.

UND AM ENDE

verlangt der Hacker eine 5000-Euro-Überweisung für die Wiederherstellung der Seite.

### EINES DER ZIELE

DAS BEDEUTET

Sie sind Teil einer Gruppe, alle im Visier eines Großangriffs.

DER HACKER WILL VIELLEICHT

PayPal-Konten hacken.

ALSO WIRD ER ODER SIE

eine Spamming-Liste mit zehn Millionen Mailadressen kaufen oder erstellen, eine davon Ihre.

UND DANN

versendet der Hacker eine falsche, doch realistische und überzeugende Phishing-Mail, die zur Herausgabe von Login-Daten für PayPal führt.

DAS ERLEDIGT,

erbeutet der Hacker alle Login-Daten von jenen, die hereingefallen sind.

UND AM ENDE

loggt sich der Hacker in Ihren Account und macht eine Überweisung an sich selbst.

### DAS OPFER, DOCH NICHT DAS ZIEL

DAS BEDEUTET

Sie sind Opfer des Fehlers eines anderen.

DER HACKER WILL VIELLEICHT

Zugriff auf Gesundheitsakten.

ALSO WIRD ER ODER SIE

eine Domain erstellen, die wie die echte aussieht, wie Gesund-Heit.de statt GesundHeit.de.

UND DANN

versendet der Hacker, sich als Führungsperson ausgebend, glaubwürdige E-Mails, damit Nutzer einen schadhaften Anhang öffnen.

DAS ERLEDIGT,

greift der Hacker auf das Netzwerk zu und hat in diesem Fall Zugriff auf Millionen private Krankenakte.

UND AM ENDE

wurde Ihre Akte gestohlen, obwohl nicht Sie die Malware geöffnet haben.

**SCHLÜSSEL-BEGRIFF**

**WARUM HEISST ES PHISHING?** Phishing ist eine Gruppe der meistverbreiteten und effektivsten Methoden, online an Informationen zu kommen. Der Terminus selbst ist ein Mix zweier Worte: „fishing" und „phreak". Fishing ist leicht zu erklären: das „Fischen" nach Opfern mit elektronischen Ködern – eine leicht verständliche und genaue Metapher. Die abgewandelte Schreibweise beruht auf „Phreaking", dem Hacken von Telefonsystemen durch „Phreaks" in Prä-Internet-Zeiten. Das wiederum bezieht sich auf eine andere Hacker-Routine: „1eet speak", in der Ziffern Buchstaben ersetzen und manche Buchstaben andere, was einen oft albernen Insider-Jargon kreiert. Heute klingt das seltsam, aber man findet immer noch Abwandlungen in Chatrooms, wenn Hacker einander im Spaß „133t H4x0r5" nennen, also „Elite Hackers".

**JEMANDEM DAS PHISHING BEIBRINGEN** Phishing ist keine spezielle Methode. Vielmehr gibt es eine Bandbreite an Möglichkeiten, um an Informationen zu kommen. Man muss diese Methoden und ihre Grundlagen verstehen, um viele der online lauernden Gefahren zu erkennen und zu vermeiden. Bevor wir uns weiter damit beschäftigen, schauen wir uns die verschiedenen Phish-Arten und wie sie anbeißen können an. Das sind die drei Vorgehensweisen, wenn Verbrecher versuchen, an Ihre Daten zu kommen:

**Freiwillige Auskunft** Die erste Methode ist teuflisch einfach: Angreifer wenden einen Mix an psychologischen Tricks an, gemeinhin bekannt als Social Engineering, um Sie zur Preisgabe Ihrer Daten zu bewegen. Menschen sind vertrauensselig und es ist unglaublich, wie viel sie im Schnitt preisgeben, nur weil sie jemand auf die richtige Art danach fragt.

**Schädliche Anhänge** Dabei werden Computernutzer durch eine überzeugende Nachricht dazu gebracht, einen vergifteten Mail-Anhang zu öffnen, der Schadsoftware auf ihrem Rechner installiert, sodass der Hacker Zugriff auf Computer oder Netzwerk erhält. Die Software tarnt sich als ein Dokument, das der User angeblich wollte, oder Fotos, die man „einfach gesehen haben muss", und dergleichen.

**Schädliche Links** Da viele Mailsysteme schädliche Anhänge heute bereits blockieren können, verwenden Angreifer stattdessen schädliche Links, die zu einer infizierten Seite führen. Die meisten Menschen klicken fast automatisch auf Links, was diese Vorgehensweise höchst effektiv macht. Die meisten Links geben sich als nützlich aus – ein Bild in der E-Mail mit einem Logo oder eine Textzeile mit der Adresse oder Website, wohinter sich eine schädliche Seite versteckt, die der Hacker allein zu seinem Zweck erstellt hat.

**PHISH-ARTEN** Es gibt viele Phishing-Methoden. Sie kennen wahrscheinlich bereits einige davon – und wurden hoffentlich nicht zum Opfer, aber falls doch, sind Sie eines von Millionen. Mit diesen Informationen können Sie die Gaunereien besser erkennen und ihnen ausweichen:

| BETRUGSMASCHEN | WIE ES LÄUFT |
|---|---|
| KLASSISCHES PHISHING  | Eine falsche Website sieht genauso aus wie eine reale – Nutzer geben ihre Login-Daten, vertrauliche oder andere private Informationen ein. |
| SPEAR PHISHING  | Hierbei handelt es sich um einen zielgerichteten Angriff, um eine kleine spezifische Gruppe oder ein Individuum mittels personalisierter Nachrichten, die oft auf stunden- oder wochenlangen Onlineausspähungen beruhen, zu betrügen. |
| WHALE PHISHING  | Spear Phishing nach einer wichtigen Persönlichkeit, etwa einem Geschäftsführer oder einer Celebrity, also einem „großen Fisch" oder Wal. |
| CAT PHISHING  | Wenn der Betrüger falsche Onlineprofile benutzt, mit denen er eine emotionale Bindung oder Liebe vortäuscht, um so an Geld oder persönliche Informationen zu kommen. |
| VISHEN/SMISHEN  | Ein Betrug oder Datenklau ähnlich dem Phishen, doch über Telefonanrufe oder SMS. |

**WENN SIE ONLINE PERSÖNLICHE DATEN EINGEBEN, TIPPEN SIE DIE ADRESSE SELBST, UND STELLEN SIE SICHER, DASS DER SEITE HTTPS UND EIN SCHLOSS-ICON VORANGESTELLT SIND.**

W/F

## PHISHING-MAILS SIND LEICHT ERKENNBAR

**FALSCH** Viele Menschen glauben, dass sie Phishing leicht erkennen können. Doch Betrüger basteln immer öfter vertrauenswürdig wirkende Nachrichten, als kämen sie von Ihrer Bank, Ihrem Amazon- oder eBay-Konto, mit all den Logos und Icons dieser Seiten, sodass die E-Mail wie echt aussieht – doch die Nutzer werden heimlich auf eine andere Seite geleitet. Manchmal kann man den Schwindel enttarnen, wenn man mit der Maus über den Link fährt (ohne zu klicken) und eine andere Adresse im Pop-up-Fenster sieht. Aber um auf Nummer sicher zu gehen, sollten Sie die Adresse immer selbst eingeben und nie auf Links klicken.

**WEHREN SIE SICH GEGEN PHISHING** Wenn also die Diebe schlau sind und nicht einmal die reichen Promis sicher sein können, haben Sie dann überhaupt eine Chance? Auf jeden Fall. Denn meistens wird man Opfer einen Angriffs nicht aufgrund mangelnder Ressourcen, sondern aufgrund mangelnder Vorsicht. Ein aufgeklärter User mit null Budget wird weniger leicht zum Opfer als ein leichtgläubiger unwissender mit allem Geld der Welt. In fünf Schritten machen Sie sich ab sofort zu einem viel schwierigeren Ziel für Phisher:

**Passen Sie auf** Achtsamkeit ist die beste Verteidigung. Seien Sie misstrauisch. Verstehen und glauben Sie, dass Sie im Visier sind. Jede Nachricht in elektronischer Form von einem Unbekannten sollte Ihnen höchst suspekt sein.

**Machen Sie den Schwebe-Test** Jedes moderne Mail-Programm zeigt Ihnen das Ziel eines Hyperlinks an, wenn Sie mit der Maus darüber fahren, ohne zu klicken. Dieser „Schwebe-Test" lässt Sie verdächtige Links in jeder E-Mail erkennen. Wenn Link und Ziel nicht völlig übereinstimmen, klicken Sie nicht darauf!


**Überprüfen Sie die URL** Lernen Sie, eine Webadresse richtig zu lesen. Der Name der Seite, die Sie besuchen, steht direkt vor der Domain (z. B. .de oder .com). Phisher nutzen das Unwissen gerne aus. Hier ein Beispiel:

**SICHER: https://www.amazon.de/**
**UNSICHER: http://www.amazon.phishingforyou.de/**

**HABEN SIE ANGST VOR ANHÄNGEN** Anhänge sind für Passwort-Diebe, Trojaner und andere Schädlinge der beliebteste Weg auf Ihren

Computer. Öffnen Sie nur Anhänge von Menschen, die Sie kennen, und auch dann nur, wenn Sie die Nachricht erwarten, etwa eine Rechnung für eine Dienstleistung, die tatsächlich stattfand.

**BESTÄTIGEN SIE EXTERN** Wenn eine verdächtige Nachricht zu vertrauliche Informationen verlangt, selbst wenn sie von Ihnen bekannten Menschen oder Unternehmen kommt, sollten Sie eine Bestätigung anfordern. Wenn zum Beispiel jemand in einer E-Mail möchte, dass Sie auf einen Link zu einer Website klicken, um einen Fehler zu beheben, suchen Sie die Website auf oder rufen Sie an. Und wie immer sollten Sie die Webadresse selbst eintippen und die Telefonnummer selbst heraussuchen. Vertrauen Sie nicht dem Link oder der Telefonnummer in der verdächtigen Nachricht. Beide könnten Fälschungen vom Phisher sein!

## HACKER-GESCHICHTE

**AM APPARAT** Das erste Mal im Netz kam der Begriff „Phishing" 1996 in der Onlinegruppe alt.2600 vor, einem Diskussionsforum für Telefon-Hacker. „2600" bezieht sich auf die Hertzfrequenz, die frühe Telefon-Hacker in einen Hörer spielten, so die Verteiler des Betreibers kontrollierten und gratis in der ganzen Welt herumtelefonieren konnten. Der Hack war einfach auszuführen und griff das System in seinen Grundlagen an, weshalb es einfach zu teuer war, ihn zu beheben. Das führte zu einer Subkultur rund um das Bauen von „Blue Boxes" oder Tongeneratoren, die den 2600-Hertz-Pfeifton spielten. Sogar die Apple-Gründer Steve Jobs und Steve Wozniak verkauften sie damals. Ein kühner Phreaker, John Draper, arbeitete mit blinden Phreakern, die logischerweise tonsensibler waren. Er fand heraus, dass die Plastikpfeifen, die in „Cap'n Crunch"-Schachteln gratis dabei waren, genau 2600 Hz erzeugten. Draper verwendete die Pfeife in großem Stil und wurde in Hacker-Kreisen Crunchman genannt. Er ist immer noch da: Sie können ihn auf Twitter unter @jdcrunchman oder auf Facebook unter John „Captain Crunch" Draper finden.

## GUT ZU WISSEN

**NICHT NUR SIE** Millionen normaler Bürger waren bereits Opfer des einen oder anderen Hacks. Das schließt auch die schlauen, mächtigen und reichen nicht aus. Die Raketenwissenschaftler der NASA fielen zum Beispiel chinesischen Hackern zum Opfer. Die US-Regierung ist zu der Erkenntnis gekommen, dass während der Wahl 2016 das Democratic National Committee von Russen und Donald Trump von Anonymous gehackt wurde. 2008 wurde das Mailkonto von Sarah Palin, Kandidatin für die Vizepräsidentschaft, von jemandem gehackt, der das Passwort der alaskischen Gouverneurin knackte. Andere bekannte Opfer waren Justizminister Eric Holder, FBI-Chef Robert Mueller, Jay Z und Beyoncé, Paris Hilton, Mel Gibson, Kim Kardashian – und Nick Selby, einer der beiden Autoren dieses Buchs; ganz zu schweigen von den Unmengen streng geheimer Regierungsdokumente, die WikiLeaks, Edward Snowden und andere preisgaben.

**KILLER-APP**

**KANN ICH IHREN MANAGER SPRECHEN?**

Die längsten, komplexesten Passwörter können Hacker in hundert Jahren nicht knacken, aber man scheint auch hundert Jahre zu brauchen, um sie auszuklügeln und dann auch noch jedes Mal neu einzugeben. Glücklicherweise gibt es Passwort-Manager-Programme, die all das übernehmen.

Passwort-Manager wie LastPass, Dashlane oder 1Password generieren, speichern und verschlüsseln seitenweise Passwörter für Sie, importieren vom Browser jedes Passwort, das Sie selbst kreiert haben, analysieren die Passwortstärke und mehr.

Sie dürfen nur nicht das Master-Passwort für das Konto selbst vergessen – und zum Glück haben viele Passwort-Manager Zwei-Faktor-Authentifizierung (siehe gegenüberliegende Seite) für einen noch stärkeren Passwort-Schutz.

**ERFINDEN SIE EIN STARKES PASSWORT** Jetzt wissen Sie, worauf Sie in E-Mails achten müssen, doch was ist der nächste Schritt? Nun, jedes Onlinekonto benötigt einen Benutzernamen (oft Ihr eigener Name oder Ihre Mailadresse) und ein Passwort. Die folgenden Regeln helfen Ihnen beim Erfinden praktisch unknackbarer Passwörter.

**Nicht eins für alle** Schauen Sie sich die Schlüssel an einem Bund an: Jeder sieht anders aus und hat eine andere Form. So wie jeder Schlüssel für ein bestimmtes Schloss passt, sollte jedes Passwort nur für einen Account benutzt werden. Ansonsten kann jemand, der es schafft, Ihre Daten zu klauen, auf jedes Ihrer Konten zugreifen.

**Länger ist besser** Manche Seiten begrenzen die Länge Ihres Passworts. Ein langes Passwort ist vielleicht schwerer zu merken, doch auch schwerer zu knacken, selbst mit brachialer Gewalt (mit Programmen, die jedmögliche Zeichenkombination ausprobieren).

**Machen Sie es kompliziert** Passphrasen wie „ichessegernepizza“ sind leicht zu merken, doch was aus echten Wörtern besteht, ist leicht zu hacken. Vermeiden Sie auch simple Auswechslungen wie „p4ssw0rt“ statt „passwort“. Machen Sie von allem Gebrauch: Klein- und Großbuchstaben, Ziffern, Sonderzeichen und was es sonst noch gibt. Eine Zahl zwischen 0 und 9 ist für einen Hacker oder ID-Dieb leicht zu finden; das richtige Zeichen in einem Mischmasch aus zweiundsechzig Ziffern, Klein- und Großbuchstaben zu finden, ist weitaus schwieriger – umso schwieriger, je länger das Passwort ist. Wenn Sie ein Passwort zur Erinnerung aufschreiben, verwahren Sie es sicher vor neugierigen Blicken und Dieben oder ziehen Sie einen Passwort-Manager in Erwägung.

**Veränderung ist gut** Erfinden Sie nicht einfach ein Passwort und lassen es dann gut sein. Ändern Sie es häufig, und benutzen Sie möglichst keines ein zweites Mal. Hacker könnten mit älteren gestohlenen Daten Erfolg haben, wenn Sie ein altes Passwort für einen neuen Account verwenden.

**SICHERHEITS-BASICS**

**BLOSS NICHT** Die zehn häufigsten – und damit schlechtesten – Passwörter haben sich seit den Anfängen des Passworts kaum geändert, nur ihre Beliebtheit ändert sich von Jahr zu Jahr. Momentan rangieren ganz oben:

| | |
|---|---|
| 1. 123456 | 6. password |
| 2. 123456789 | 7. 123123 |
| 3. 111111 | 8. 000000 |
| 4. qwertz | 9. 1234567 |
| 5. 12345678 | 10. 1234567890 |

**WER WILL DAS WISSEN?** Eine Extraportion Sicherheit bietet ein Passwort mit „wissensbasierter Authentifizierung", oft WBA genannt, entweder als Zusatz zu Nutzernamen und Passwort oder um Ihre Identität sicherzustellen, wenn Sie Ihr Passwort vergessen haben. Wie viele andere Verteidigungsstrategien kann auch diese gegen Sie verwendet werden.

**Statische WBA** Auch bekannt als „gemeinsames Geheimnis", also Fragen nach dem Mädchennamen Ihrer Mutter, Ihrem Geburtsort und so weiter, sind oft leicht öffentlich zugänglich. Ihre Angaben werden außerdem gespeichert, können also gestohlen werden – somit sind auch ausgefallenere Fragen, wie nach Ihrem Lieblingsdichter, nicht sicher.

**Dynamische WBA** Hier werden in Echtzeit Fragen von mehreren öffentlichen oder privaten Unterlagen generiert. Sie wissen nicht, welche Fragen gestellt werden, doch kennen hoffentlich die Antworten. Solche Fragen könnten sein: „Welche Farbe hatte Ihr Honda Accord?" oder „In welcher dieser Straßen haben Sie nie gewohnt?". Sie haben nur kurz Zeit zu antworten, die Chancen, dass jemand ohne Vorbereitung richtig antwortet, sind geringer.

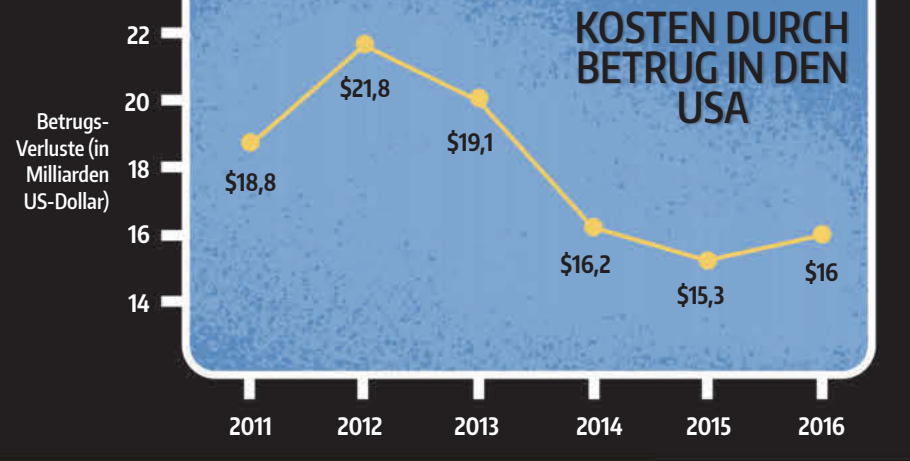
Leider kommen Sie vielleicht gar nicht in den Genuss solch protektiver Seiten mit guter dynamischer WBA, aber wenn Sie die Wahl haben, nutzen Sie sie. Eine simple Notlösung: lügen. Es ist leicht herauszufinden, wo jemand zur Schule ging. Doch wenn die „korrekte" Antwort ein Fantasieortsname wie Narnia oder Westeros ist, wird sie wohl kaum in alten Jahrbüchern aufscheinen. Leider nicht.

**SICHERHEITS-BASICS**

**DOPPELTE POWER** Zwei-Faktor-Authentifizierung, auch „2FA" genannt, funktioniert wie die aus Spionageromanen bekannte Parole („Die Amsel singt nachts"; „Doch nur bei Vollmond") oder wie wenn zwei Personen gleichzeitig einen Schlüssel drehen, um eine Rakete zu starten. 2FA benutzt einen verteilten Algorithmus, der an Ihren Account gebunden ist, und greift dazu oft noch auf eine Handy-App oder ein weiteres, nur für Sie zugängliches Gerät (z. B. einen Schlüsselanhänger) zurück. Nach der Passworteingabe öffnen Sie die App oder drücken einen Knopf auf Ihrem Anhänger, um den Authentifikationsschlüssel zu generieren, der auf dem Algorithmus basiert, meist eine zufällige kurze Ziffernfolge. Wenn ein Konto 2FA anbietet (wie Google Authenticator), nutzen Sie es. Sollten Sie den Anhänger oder das Telefon mit der App verlieren, ersetzen Sie beides sofort, um Ihr Konto zu sichern.

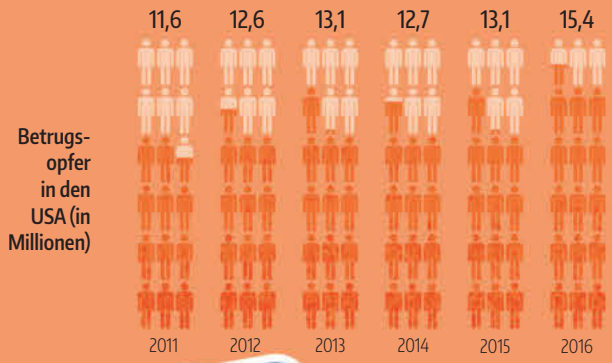
# IDENTITÄTS-DIEBSTAHL

## KOSTEN DURCH BETRUG IN DEN USA




**90%** ALLER OPFER BEMERKTEN DEN FREMDEN ZUGRIFF AUF IHRE DATEN ERST, NACHDEM DIE DIEBE SIE MISSBRÄUCHLICH VERWENDET HATTEN.

## FÄLLE VON IDENTITÄTSBETRUG




## GRÖSSTE ZIELGRUPPEN



## LÄNDER MIT DEN MEISTEN IDENTITÄTSDIEBSTÄHLEN PRO KOPF

1. MEXIKO
2. USA
3. INDIEN
4. VER. ARABISCHE EMIRATE
5. CHINA
6. VER. KÖNIGREICH
7. BRASILIEN
8. AUSTRALIEN
9. SINGAPUR
10. SÜDAFRIKA
11. KANADA

**64%** aller Kreditkarten wurden von Dieben versuchsweise oder erfolgreich benutzt.

## WIE LANGE DAUERT DIE AUFKLÄRUNG, WENN IHRE PERSONENDATEN GESTOHLEN WURDEN?

| | |
|---|---|
| 48% | 1 TAG ODER WENIGER |
| 16% | 2 BIS 7 TAGE |
| 18% | 8 TAGE BIS EINEN MONAT |
| 6% | 1 BIS 3 MONATE |
| 3% | 3 BIS 6 MONATE |
| 9% | 6 MONATE ODER LÄNGER |

## ANZEICHEN, DASS IHRE IDENTITÄT GESTOHLEN WURDE

- ERHÖHTE KREDITKARTENSPESEN
- SCHLECHTERE BONITÄT
- UNERKLÄRLICHE RECHNUNGEN
- TEURERE AUTOVERSICHERUNG
- KONTOAUSZÜGE EINGESTELLT
- STEUERRÜCKZAHLUNG ABGELEHNT
- ANTRAG AUF FÜHRERSCHEIN ABGELEHNT
- UNERKLÄRLICHE AUFFORDERUNGEN ZU MEDIZINISCHEN UNTERSUCHUNGEN
- ANRUFE VON GELDEINTREIBERN
- DARLEHEN ABGELEHNT
- NEGATIVES LEUMUNDSZEUGNIS

# 30 TAGE

im Schnitt, bis Verbrechen mit Identitätsklau behandelt werden.

## HÄUFIGSTE ARTEN VON IDENTITÄTSKLAU

| 49,2% | 15,8% | 9,9% | 5,9% | 3,5% | 3,3% | 22,9% |
|---|---|---|---|---|---|---|
| VERSUCHTER ZUGRIFF AUF OFFIZIELLE DOKUMENTE* | KREDITKARTEN-BETRUG | TELEFON- ODER NEBENKOSTEN-BETRUG | BANKBETRUG AUSSER KREDITKARTEN | DARLEHENSBETRUG | ARBEITSBETRUG | SONSTIGE |

**Ausweis, Sozialversicherungsnummer, Steuerrückzahlungen etc.*

# 30 STUNDEN

im Schnitt, bis angefochtene Kreditlast behandelt und aufgeklärt wird.

# REGISTER

# F



# G



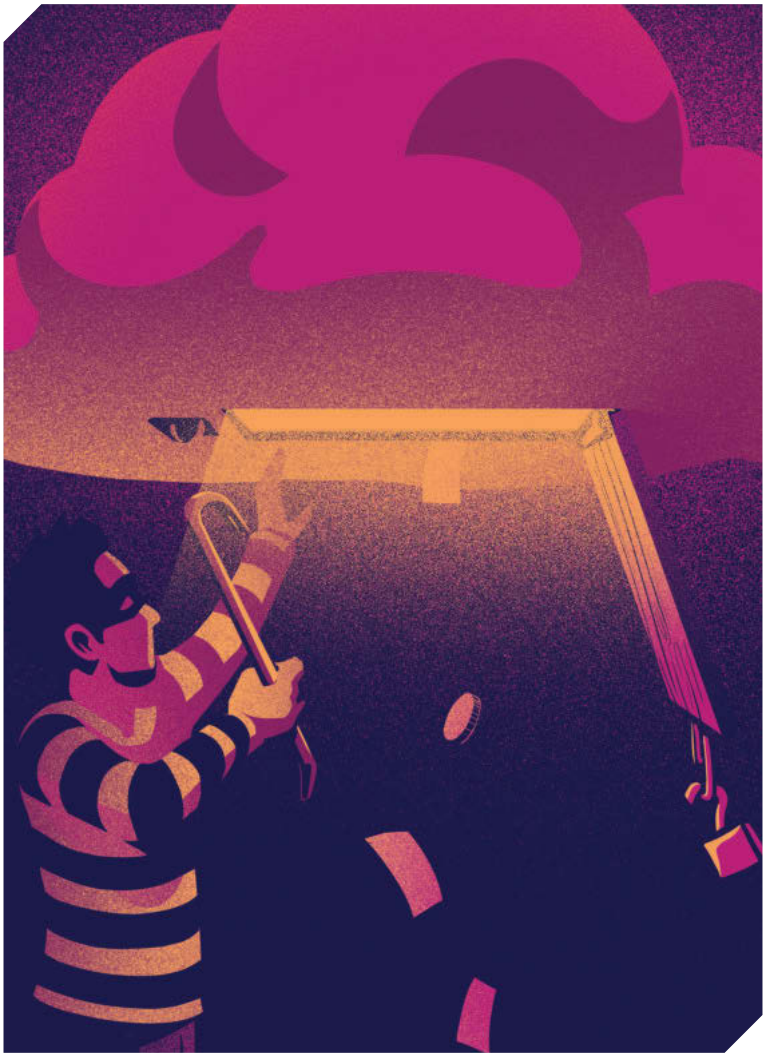
# H



# I

## P





## Q



## R



## S

## T



## U



## V



## W



## Y



## Z

# ÜBER DIE AUTOREN

**NICK SELBY** ist ein Kriminalbeamter aus Texas, der Computerkriminalität, Betrug und Ausbeutung von Kindern untersucht.. Er berät Strafverfolgungsbehörden zu Cyber-Intelligenz und -Ermittlungen. Er ist auch Cyber-Sicherheits-Berichterstatter beim Team von Secure Ideas Response. Nick begründete die Informationssicherheitspraxis bei der Industrieanalysefirma 451 Research. Als Analyst für Informationssicherheit führte Nick fachliche Interviews mit mehr als 1.000 Start-ups und baute Sicherheits- und Nachrichtendienstfirmen auf, schrieb Hunderte strategischer Schriftsätze, beriet US- und europäische Regierungsbehörden in Fragen der Sicherheit und der Aufklärung und wurde regelmäßig als Experte in den weltweit führenden Wirtschafts- und Branchenzeitungen genannt.

Er schreibt häufig Beiträge für Zeitungen, u. a. die *Washington Post* und *New York Times*, er war Co-Autor von *Blackhatonomics: Understanding the Economics of Cybercrime* und Fachlektor von *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Er schrieb auch an *In Context: Understanding Police Killings of Unarmed Civilians* mit.

**HEATHER VESCENT** ist Futuristin und vor allem als Expertin für Cyber-Wirtschaft und Kryptowährung bekannt. Ihre weitreichende Forschung, veröffentlicht von *New York Times*, *CNN*, *American Banker*, CNBC, Fox und *Atlantic*, untersucht Trends bezüglich der Zukunft von Geld, Wirtschaftssystemen, Identität, Wearable Technology, Beziehungen, Erweiterter Intelligenz, IoT, Cyber-Sicherheit und Menschheit.

Sie hielt auf zahlreichen Konferenzen und Veranstaltungen Reden, darunter SXSW, TEDxZwolle und Cyber Security Summit. Sie wurde von *Wired,* der *New York Times*, dem *Atlantic*, *American Banker*, der italienischen *Elle* und vielen mehr porträtiert und zitiert. Sie ist mehrfach als Technik-Expertin für Fox News aufgetreten.

Seit mehr als einem Jahrzehnt produziert ihre Firma The Purple Tornado Medien, die „die Zukunft im Präsens visualisieren", darunter zehn Kurzfilme und Dokumentationen über die Zukunft und mehr als dreißig Podcasts zu Themen wie Geld, Wearable Technology und selbstfahrende Autos. Heather teilt ihre Zeit zwischen Los Angeles und der Mojave-Wüste auf.

## ANDERE BEITRAGENDE

**ERIC OLSON** arbeitet im Bereich Cyberkriminalität und Bedrohungsanalyse, einschließlich der Entwicklung von Software und Systemen zur Bekämpfung von Phishing, Identitätsdiebstahl und Cyberkriminalität. Derzeit ist er Vizepräsident der Aufklärungsmaßnahmen bei LookingGlass Cyber Solutions und arbeitet ehrenamtlich für eine Non-Profit-Kampagne gegen Online-Ausbeutung von Kindern. Eric hat einen BA in Russisch vom Hamilton College und einen MBA der Georgetown University.

**MOEED SIDDIQUI** bekam seinen ersten IT-Job in der Stadtverwaltung im Alter von fünfzehn (zwei Jahre, bevor er Eagle Scout wurde). Während seines Studiums leitete er sein eigenes IT-Dienstleistungsunternehmen, das auf Netzwerke, Sicherheitsregeln im Gesundheitsbereich, bei Behörden und in der Finanzdienstleistungsbranche und Projektmanagement spezialisiert war. Er hat mit kleinen Unternehmen, Stufe-4-Rechenzentren und allem dazwischen gearbeitet.

**JOHN BEAR, PH.D.** verfasste 1974 sein erstes Buch über Fernunterricht, *Bear's Guide to Earning Degrees by Distance Learning*, noch vor der Geburt des Internets. Er beriet ein Jahrzehnt lang die FBI-Operation DipScam, half dabei, betrügerische Schulen zu entlarven und zu schließen, und ist gemeinsam mit dem pensionierten FBI-Agenten Allen Ezell Autor von *Diploma Mills: The Billion-Dollar Industry That Sold a Million Fake Degrees*.

## DANKSAGUNG DER AUTOREN

**NICK SELBY** Dank an Mariah Bear, Ian Cannon, Jan Hughes, Allister Fein, Suzi Hutsell und den Rest des Teams von Weldon Owen und Cameron für ihre unglaubliche Unterstützung und an Rob James dafür, dass er mir Beine gemacht hat. Einen speziellen Dank an Ben Singleton und Moeed Siddiqui bei SIRT. Ich bedanke mich auch bei Aaron Barr, Daniel Clemens, Kevin Branzetti, Dave Marcus, Ryan Lackey, Rhett Greenhagen, Lance James, Allison Nixon, Mike Kearn, Will Gragido und anderen auf dem Informationssicherheitsgebiet, die mir ihre Zeit und Expertise gewidmet haben. Die Fehler sind alle meine. Und ich bedanke mich bei meinen Co-Autoren Heather Vescent, Eric Olson, Moeed Siddiqui, Amanda Nickerson und John Bear.

**HEATHER VESCENT** Danke an meine Eltern, Pam Phillips, Rick Schlegel, und Donna Dee. An Ruth Waytz, Sarafina Rodrigeuz, und Rosie Pongracz für ihre Unterstützung, ihre Freundschaft und ihre Liebe. Für die Recherche, Sicherheitstipps und persönliche Geschichten bedanke ich mich bei Monica Anderson, Ian Danskin, Scott Froschauer, Ashish Gupta, Alex Kawas, Jennifer Ramsey, Rob Ryel, Tamara Struminger, Corwin Weskamp und meinen anonymen Dark-Web-Schutzpatronen. Und danke an die Böcke und Trolle auf Reddit. Ihr wisst, wer ihr seid, aber vermutlich nicht, wer ich bin. Ich habe spätabends viel zu viele Kommentar-Threads gelesen.

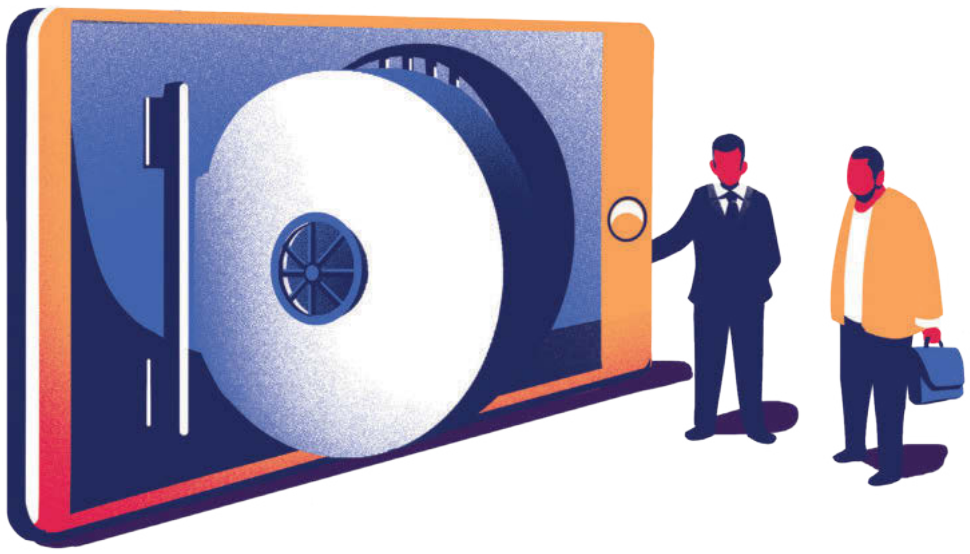
Vielen Dank an meinen Co-Autor Nick Selby und an das Team bei Weldon und andere: Mariah Bear, Ian Cannon, Jan Hughes und alle anderen. Verzeihung, wenn ich jemanden irrtümlich ausgelassen habe.

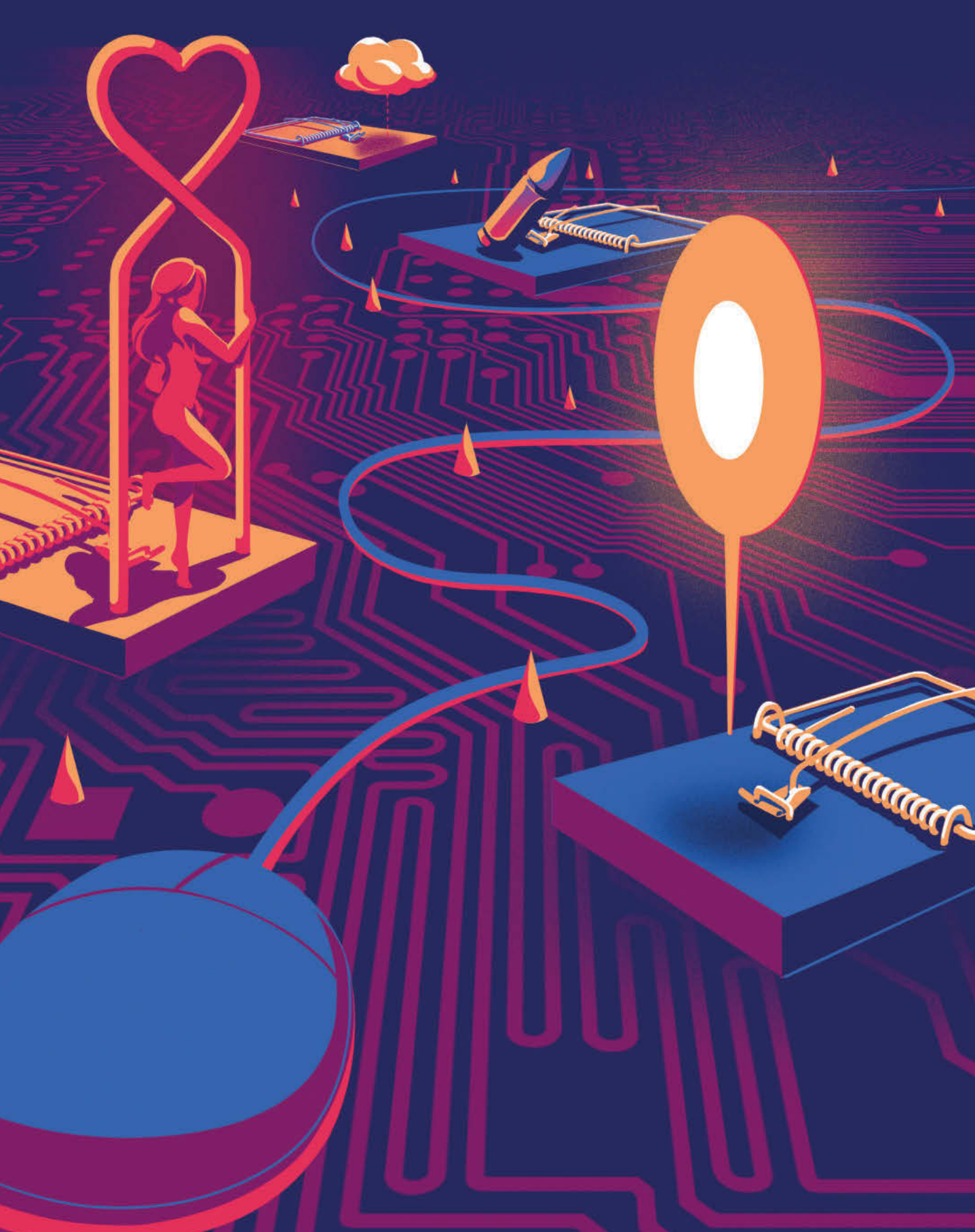
Dieses Buch hätte ohne meine spätabendlichen Begleiter, Kaffee von Peet's und Wein von Ravenswood und Bonny Doon nicht geschrieben werden können. Und am Schluss Dank an Mr. Dog, der sich noch nicht um Cybersicherheit kümmern muss, da das Internet für Hunde noch einige Jahre entfernt ist.

## BILDNACHWEIS

**Eric Chow:** Vordercover, 1, 2, 4, 8, 14–15, 16, 18, 22, 24, 28, 34, 36, 40 (unten), 42, 46, 50, 52, 53, 58, 60, 64, 68, 69, 70, 72, 74, 76, .84, 86, 88, 92, 94, 96, 98, 100–101, 102–103, 104, 110, 112, 116, 122, 123, 124, 126, 128, 130, 132, 134, 136, 150, 152, 155, 156, 158 (oben), 160–161, 164–165,174,178, 180, 182, 186, 188, 196, 198, 200–201, 207, 209, 210,211, 212, 216, 218, 221, 222, 224

**Conor Buckley:** 20, 25, 26, 30–31, 32–33, 38, 39, 40 (oben), 44, 49, 56, 57, 62, 66–67, 75, 78–79, 80, 81, 82, 90, 91, 106, 108, 114, 119, 120, 125, 133, 138, 140, 144–145, 146, 148, 154, 158 (unten), 159, 160, 166, 169, 170, 172–173, 181, 190, 192, 194, 197





Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.



**Autoren:** Nick Selby, Heather Vescent
**Mit Beiträgen von:** Eric Olson, Moeed Siddiqui, John Bear (Ph. D.)
**Illustrationen:** Eric Chow, Conor Buckley
**Schriftart „Hacked“:** David Libeau (CC BY 4.0)
**Satz und Übersetzung:** Print Company Verlagsgesellschaft m.b.H., Wien
**Übersetzung:** Lilo Bolen, Laura Kühbauch, Anita Weinberger-Schwendenwein
**Programmleitung Franzis Verlag:** Benjamin Hartlmaier

**ISBN 978-3-645-20593-1**

**„Ich wünschte, dieses clevere Handbuch wäre gar nicht nötig, aber für die meisten Menschen ist es unverzichtbar. Und das Lesen macht Spaß – eine Seltenheit in Cybersicherheitskreisen."**

**DAVID BIRCH**
Direktor für Innovation, Consult Hyperion

**„Ein Muss für jeden: Experten und n00bs, Profis und Eltern. Ich habe noch nie gesehen, dass so komplexe Cyber-Themen auf so unterhaltsame Weise behandelt wurden."**

**CHRIS ROCK**
CEO und Gründer, Cybersicherheitsfirma Kustodian

---

Identitätsdiebstahl. E-Mail-Hacks. Angriffe auf die Infrastruktur. Kreditkartenbetrug. Sogar Auftragsmord. All diese Verbrechen können mit nur wenigen Mausklicks begangen werden. Cyberkriminelle können Sie jederzeit angreifen: über den Laptop, das Smartphone, den Fernseher - sogar über Ihre Türklingel oder Ihr Thermostat. Die gute Nachricht? Sie müssen kein Opfer sein. In diesem umfassenden, praktischen und fundierten Handbuch geben Ihnen der Sicherheitsexperte Nick Selby und die Zukunftsforscherin Heather Vescent die nötigen Tools an die Hand, um Ihre Familie, Ihre Privatsphäre, Ihre Finanzen und Ihren Ruf zu schützen. Gehen Sie nicht ohne es online.

---

**NICK SELBY** ist ein texanischer Strafverfolger und bekannter Cybersicherheitsberater, dessen Artikel in der New York Times, der Washington Post und vielen anderen Publikationen erschienen sind. Er schreibt zu Themen wie Hacking, Online-Kriminalität und Polizeiarbeit.

**HEATHER VESCENT** ist Schriftstellerin, Filmemacherin und Zukunftsforscherin. Sie ist bekannt aus Wired, The Atlantic und der New York Times, hatte Auftritte bei CNN, CNBC und Fox News und hat unter anderem auf den Konferenzen South by Southwest und TEDx gesprochen.

FRANZIS