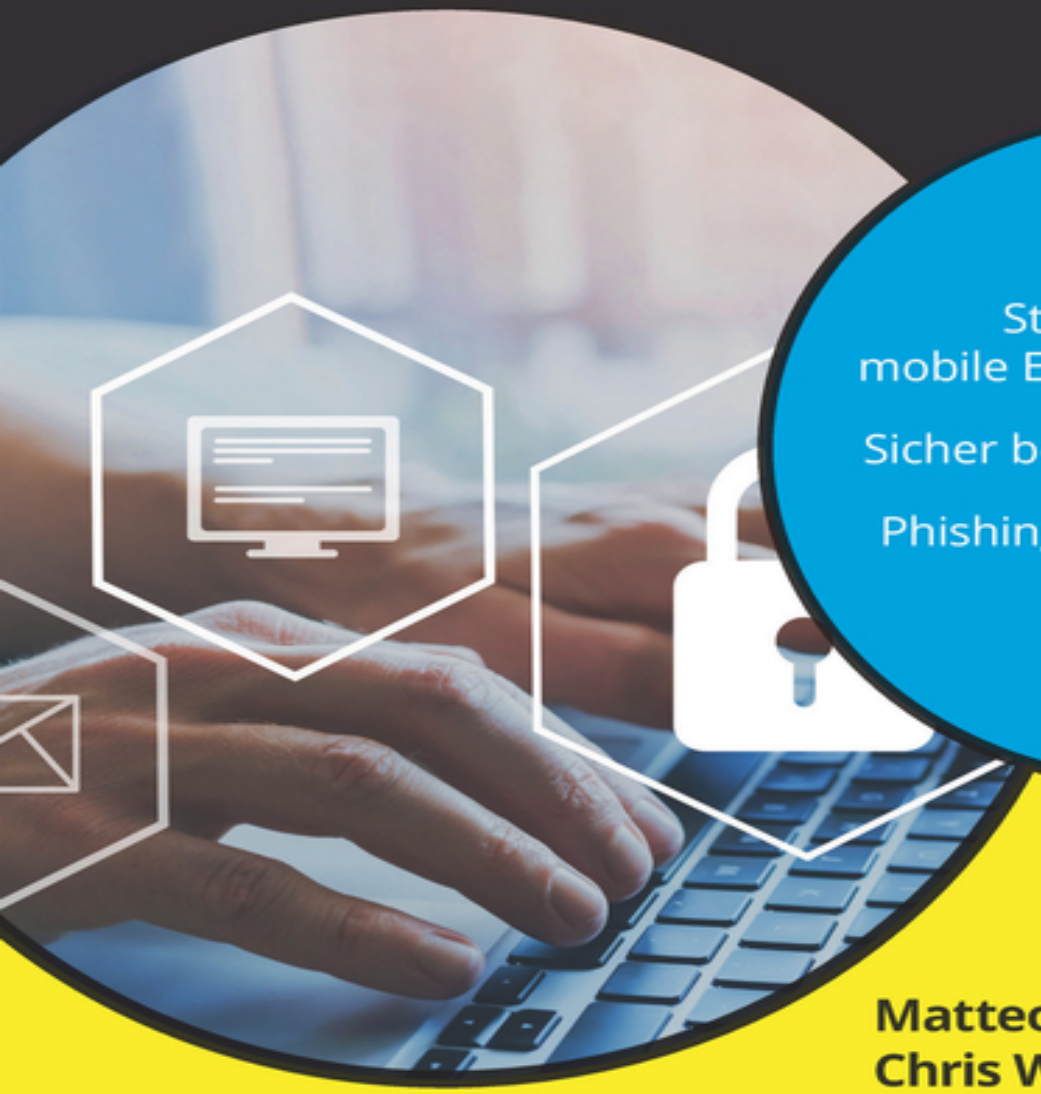
LERNEN EINFACH GEMACHT

Meine digitale Sicherheit

Tipps und Tricks

für dummies®



- Stationäre und mobile Endgeräte absichern
- Sicher bezahlen im Internet
- Phishing-Mails zuverlässig erkennen

Matteo Große-Kampmann
Chris Wojzechowski

Meine digitale Sicherheit Tipps und Tricks für Dummies

Schummelseite

QUICK WINS

Hier finden Sie Tipps für schnelle Siege im Kampf um ihre persönliche Informationssicherheit:

- ✔ Geben Sie Ihren Klarnamen nur dort an, wo Sie müssen! So viele Daten wie nötig und so wenige wie möglich sollte Ihre Devise sein.
- ✔ Sie haben einen Link in einer Mail geklickt und sollen nun etwas herunterladen oder Ihr Passwort eingeben? Überprüfen Sie die Seriosität der Mail!
- ✔ Nutzen Sie mehr als nur eine E-Mail-Adresse und stellen Sie sicher, dass Sie von allen Adressen zuverlässig das Passwort zurücksetzen können! Legen Sie außerdem eine Notfalladresse an, um eine Passwortwiederherstellung möglich zu machen.
- ✔ Lassen Sie sich nicht unter Druck setzen. Sie haben am Computer Zeit, insbesondere im Privatleben. Keiner zwingt Sie, sofort auf eine E-Mail oder einen Link zu klicken. Machen Sie sich das immer wieder bewusst.
- ✔ Jeder Account ist nur so gut wie sein Schutz. Verwenden Sie lange Passwörter (mehr als 12 Zeichen, kein Wort aus dem Wörterbuch) und aktivieren Sie die Zwei-Faktor-Authentifizierung, wo möglich. Wenn Sie diese aktivieren, speichern/drucken/schreiben Sie die Notfallcodes auf, für den Fall, dass Sie keinen Zugang mehr zu Ihrem Smartphone haben.
- ✔ Bereiten Sie sich vor: Nehmen Sie sich eine Stunde und spielen Sie durch, wie es wäre, wenn Sie Ihren Laptop oder Ihr Smartphone verlieren. Was brauchen Sie unbedingt, was ist nebensächlich? Schreiben Sie alles auf und sorgen Sie für den Notfall vor.
- ✔ Legen Sie auch Backups der wichtigsten Daten an. Gehen Sie auf Nummer sicher und archivieren Sie regelmäßig Ihre gesamte Festplatte. So vermeiden Sie Datenverlust.
- ✔ Suchen Sie regelmäßig nach Ihrem eigenen Namen. Sie finden Inhalte, die Sie nicht freigegeben haben? Dann beantragen Sie eine Löschung der Inhalte unter folgendem Link: https://aware.link/0801

BÖSARTIGE NACHRICHTEN UND LINKS ERKENNEN

Diese Liste soll Ihnen eine schnelle Hilfe beim Erkennen von bösartigen Nachrichten sein!

- ✔ Wenn Sie den Absender einer Nachricht nicht kennen, sollten Sie misstrauisch sein. Insbesondere wenn es um Rechnungen, Zahlungen, Gewinne oder um etwas geht, was schnell erledigt werden soll.
- ✔ Hinweise auf Rechnungen, Zahlungen und Gewinnbenachrichtungen im Betreff sind ein weiteres Alarmzeichen – gerade dann, wenn Sie sich weder an einen Kauf noch an eine Teilnahme erinnern können.
- ✔ Sind Sie unsicher, verschieben Sie die E-Mail in Ihren Junk-Ordner. Dann werden keine Bilder oder sonstigen Inhalte der Nachricht nachgeladen und Sie können die Mail gefahrlos weiter überprüfen.
- ✔ Bevor Sie von E-Mails ausgehend Dateien herunterladen, loggen Sie sich besser auf der Webseite des Anbieters ein. Da finden Sie die Dateien oft ebenfalls und können sie von dort sicher herunterladen.
- ✔ Halten Sie nach dem dritten Schrägstrich Ausschau. Die ersten beiden Schrägstriche finden sich direkt nach dem http(s). Wenn der dritte Schrägstrich kommt, ist die Internetadresse zu Ende. Der erste Punkt vor dem dritten Schrägstrich ist ebenfalls wichtig. Das, was links vom Punkt steht, ist die Domain - das was rechts vom Punkt steht, ist die Top-Level-Domain. Ausnahmen bestätigen allerdings die Regel: So wird in Großbritannien co.uk als Top-Level-Domain genutzt. In diesem Fall muss der zweite Punkt vor dem dritten Schrägstrich gesucht werden.
- ✔ Wenn Sie nach der Bewertung unsicher sind, ob die E-Mail bösartig ist oder nicht, sollten Sie auf gar keinen Fall den Anhang öffnen. Löschen Sie die E-Mail, wenn es sich bei dem Anhang um .zip- oder Office-Dateien (Endungen .docx, .xlsx oder .pptx) handelt.
- ✔ Um Täter zu ermitteln und dabei zu helfen, das Spam- und Phishingaufkommen zu reduzieren, können Sie die E-Mails an das Polizeilabor Niedersachsen weiterleiten. Dazu nehmen Sie die verdächtige Mail und leiten diese, ohne Kommentare oder Veränderungen, an trojaner@polizeilabor.de weiter. Sie erhalten eine automatisch erstellte Antwort. Sie erstatten dadurch keine Anzeige, unterstützen die Polizei aber bei der Bekämpfung von Internetkriminalität.

Matteo Große-Kampmann und
Chris Wojzechowski

Meine digitale Sicherheit Tipps und Tricks

für dummies®

WILEY
WILEY-VCH GmbH

Meine digitale Sicherheit Tipps und Tricks für Dummies

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Print ISBN: 978-3-527-71834-4
ePub ISBN: 978-3-527-83272-9

Coverfoto: © Song_about_summer – stock.adobe.com
Korrektur: Matthias Delbrück, Dossenheim/Bergstraße

Über die Autoren

Chris Wojzechowski absolvierte eine Ausbildung zum Bürokaufmann und studierte im Anschluss Wirtschaftsinformatik. Es schloss sich ein Studium der Internet-Sicherheit an. Er war im Institut für Internet-Sicherheit für den Bereich Live-Hacking und Awareness verantwortlich und leitete diverse wissenschaftliche Studien. Er ist seit dreizehn Jahren nebenberuflich selbstständig und hat im Jahr 2019 gemeinsam mit Matteo Große-Kampmann die AWARE7 GmbH gegründet und führt diese erfolgreich durch die Höhen und Tiefen der Geschäftswelt.

Matteo Große-Kampmann studierte im Master Internetsicherheit, nachdem er Medizintechnik im Bachelor studiert hatte. Er promoviert in der Arbeitsgruppe Systemsicherheit bei Prof. Dr. Thorsten Holz am Horst-Görtz-Institut der Ruhr-Universität Bochum und am Institut für Internet-Sicherheit von Prof. Dr. Norbert Pohlmann an der Westfälischen Hochschule Gelsenkirchen. Matteo Große-Kampmann ist zudem als Beiratsmitglied, Mentor, Juror und Coach in verschiedenen kommunalen, regionalen und internationalen Unternehmen und Veranstaltungen tätig.

Matteo Große-Kampmann und Chris Wojzechowski sind gemeinsam seit über 15 Jahren im Bereich IT-Sicherheit unterwegs. Die Faszination für digitale Sicherheit und das Aufdecken von Betrugsmaschen im digitalen Raum ist ihnen gemeinsam. Sie halten Fachvorträge auf Kongressen und bei Events von Firmen, Verbraucherzentralen und anderen Institutionen und Organisationen. Sie veröffentlichen regelmäßig Forschungsartikel und stehen immer wieder in Funk und

Fernsehen Rede und Antwort zu aktuellen Fragen der IT-Sicherheit.

Mehr Informationen finden Sie unter https://aware7.de

Vorworte

Die digitale Welt ist aus unserem Leben nicht mehr wegzudenken.

Surfen, E-Mails schreiben, Online-Banking und Einkaufen im Internet haben mittlerweile ebenso in unseren Alltag Einzug gehalten wie die sozialen Netzwerke LinkedIn, Xing, Facebook, Instagram oder Twitter.

Als Teil einer modernen Gesellschaft verlagern immer mehr Menschen ihr Berufs-, aber auch ihr Privatleben in den digitalen Raum. Die Risiken, denen sie dabei begegnen, sind vielen jedoch unbekannt. Der digitale Raum ist ein gewaltiger Datenspeicher, der begierig alles aufsaugt und nichts vergisst. Dazu gehören auch Informationen und Bilder, von denen wir nicht wollen, dass sie jedem Nutzer des World Wide Web zur Verfügung stehen. Insbesondere sicherheitskritische Daten geben wir im realen Leben nur ungern einem Fremden preis. Sollten wir dann nicht auch in der digitalen Welt Vorkehrungen treffen, um unsere Daten angemessen zu schützen? Die Bedeutung des Themas IT-Sicherheit hat im digitalen Raum in den letzten Jahren erheblich zugenommen, denn das Vertrauen der Nutzer in das Medium sinkt aufgrund negativer Erfahrungen und sich häufender Nachrichten über Datenmissbrauch sowie immer neue Betrugsmaschen zwangsläufig. Sicherheitslücken schließen und die eigene Kompetenz stärken – diese Herausforderungen gilt es zu meistern, um die vielfältigen Möglichkeiten der digitalen Welt sicher nutzen zu können.

Chris Wojzechowski und Matteo Große-Kampmann erläutern in ihrem Buch »Meine digitale Sicherheit –

Tipps und Tricks« kurz und bündig, wie es gelingt, selbstständig Maßnahmen zu ergreifen, um die private IT-Sicherheit zu erhöhen. Damit sind wir in der Lage, Gefahrensituationen aus dem Weg zu gehen und unsere Daten besser zu schützen. Ich bin mir sicher, dass das Lesen dieses Buches helfen wird, Risiken abzubauen, sodass wir mit mehr Freude die positiven Aspekte der digitalen Zukunft genießen können.

Daher wünsche ich Ihnen viel Spaß und Erkenntnisse beim Lesen dieses Buches.

Ihr

Norbert Pohlmann

Informatikprofessor für Informationssicherheit an der Westfälische Hochschule

Geschäftsführender Direktor des Forschungsinstituts für Internet-Sicherheit - if(is)

Geschäftsführer Beteiligungsgesellschaft - p-venture

Vorstandsvorsitzender des Bundesverbands IT-Sicherheit - TeleTrusT

Vorstandsmitglied des Verbandes der Internetwirtschaft - eco

Die Digitalisierung birgt Chancen und Risiken gleichermaßen. Für die Risikominimierung ist die IT-Sicherheit die elementare Basis. Doch wer kennt sich hier aus? Wer kann mit den ganzen Fachwörtern richtig arbeiten?

Die beiden Autoren dieses Buches sind nicht nur ausgewiesene Profis in der IT-Sicherheit, sondern sie verstehen es auch außerordentlich, die sprachliche Übersetzung zwischen IT-Nerds und IT-Nutzern zu leisten.

Mit dem vorliegenden Werk bekommt der IT-Neuling die Grundlagenkompetenz und der IT-Erfahrene noch ein paar Tipps für die sichere Nutzung der digitalen Welt.

Aus polizeilicher Sicht wird es niemals eine 100 Prozent sichere Welt geben, aber man bekommt eine Handlungsanleitung für ein deutlich sichereres Verhalten und gewinnt nicht nur an Handlungskompetenz, sondern auch an Schutz. Allein das rechtfertigt schon den Blick ins Buch und die Auseinandersetzung mit dem Thema.

Ihr

Peter Vahrenhorst

Kriminalhauptkommissar, Landeskriminalamt Nordrhein-Westfalen

Inhaltsverzeichnis

Tabellenverzeichnis

Kapitel 4

Kapitel 7

Illustrationsverzeichnis

Kapitel 2

Kapitel 3

Kapitel 4

Kapitel 5

Kapitel 6

Kapitel 7

Kapitel 9

Einleitung

Ich, Matteo, erinnere mich noch an meinen ersten Computer. Auf einer viel zu kleinen Holzkommode ohne Stuhl habe ich geflippert. Auch an den ersten Kontakt mit einem »Computervirus« in meinem Kinderzimmer erinnere ich mich gut: Ich hatte auf eine Datei geklickt und dann schob sich das CD-ROM-Laufwerk des Computers immer wieder auf und zu. Abgesehen von ein bisschen nervigem Gewackel kein größeres Ärgernis. Ein paar Jahre später gab es dann schon mal ein böseres Erwachen, denn im Zuge von Peer-to-Peer-Tauschbörsen wie Limewire oder Bearshare hielten auch schlimmere Viren auf dem heimischen PC Einzug, die ihn dann unter Umständen nahezu unbrauchbar machten.

Wir sind als Gesellschaft heute so weit in die digitale Welt eingetaucht und verlagern so viele Aspekte unseres Lebens ins Internet, dass die Bedrohungen immer größer werden. Musste früher lediglich der Familien-PC erneuert werden beziehungsweise gab es dann eine Zeit lang einfach keinen, kann ein Ausfall eines Computers heutzutage auch mit Lösegeldforderungen oder Erpressungen einhergehen. Ganz zu schweigen von der gelöschten oder gesperrten Erinnerung, hat ein Befall mit Schadsoftware heute auch finanzielle, gesundheitliche oder gesellschaftliche Auswirkungen. Als Gesellschaft müssen wir mit dieser neuen Gefahr umgehen lernen und unser Risiko überblicken können. Hierfür brauchen wir Erkenntnisse und ein Verständnis für das Problem.

Klar ist, dass kaum eine technische Erfindung unser Leben so nachhaltig verändert wie das Internet. Durch die zunehmende Vernetzung sind Informationen schnell geteilt und verfügbar gemacht. Gerade die Covid-19-

Pandemie hat uns vor Augen geführt, wie wichtig der digitale Austausch einerseits ist. Andererseits ist allerdings auch klar, dass digitaler Kontakt den normalen Kontakt nicht ersetzen kann. Er ist heute aber mindestens eine Alternative. Die Digitalisierung ist allumfassend auf der Erde, vom fernen Neuseeland bis nach Gelsenkirchen sind es in der digitalen Welt nur ein paar Millisekunden. Dies ist mit vielen Chancen und Möglichkeiten verbunden, aber auch mit einigen Risiken. Auf diese wollen wir uns in diesem Buch fokussieren und Ihnen als Leser:in ein paar Kniffe mit an die Hand geben, wie Sie sich schützen können. Damit Sie den Fokus auf die Chancen statt auf die Risiken lenken und sich auch digital optimal entfalten können!

Über dieses Buch

Betrugsmaschen, Einstellungen oder einfach ein kleiner Tipp am Rande – dieses Buch klärt auf, gibt Hilfestellungen und macht an zahlreichen Beispielen vor, wie Daten und die digitale Identität besser geschützt werden können.

Die digitale Sicherheit ist dabei ein ziemlich abstraktes Thema, das sich aber ganz schnell mit Leben füllt, wenn Kriminelle im Besitz Ihrer Daten sind, Sie einer Betrugsmasche auf den Leim gehen sind oder nicht feststellen können, ob der Online-Shop seriös ist oder nicht.

Die Digitalisierung bietet einiges an Chancen, den Herausforderungen müssen wir uns stellen. Ähnlich wie wir auch sonst mit neuen Situationen umgehen müssen, müssen wir dies auch in der Online-Welt. Da kann nicht alles auf Anhieb funktionieren, aber wir sollten uns und unsere Entscheidungen kritisch hinterfragen und darüber nachdenken, wie wir uns und unsere

Mitmenschen schützen können. Dieses Buch soll Ihnen diesbezüglich eine Orientierungshilfe sein, insbesondere wenn Sie auf diesem Gebiet noch nicht so bewandert sind. Sehen Sie das Buch als Ihren ersten Schritt in eine sicherere Zukunft online und vielleicht sogar offline!

Törichte Annahmen über den Leser

Dieses Buch ist geschrieben für all diejenigen, die ihre ersten Schritte in der Welt der digitalen Sicherheit machen. Diejenigen, die es bis jetzt nicht geschafft haben, denen sich die Informationen im Internet zu schnell ändern oder denen keiner beim sicheren Einrichten einer Online-Identität hilft, und auch all denen, die ein schnelles Nachschlagewerk für alltägliche Dinge benötigen. Wir hoffen, Sie finden hier, was Sie suchen, nämlich ein Buch mit praktischen Tipps und Tricks sowie ein wenig Hintergrundwissen.

Konventionen in diesem Buch

Bevor Sie sich auf die zahlreichen Tipps und Tricks in diesem Buch stürzen, sollten Sie folgende Hinweise lesen:

- ✔ Alle Links, die Sie in diesem Buch finden werden, sind nach dem gleichen Prinzip aufgebaut: https://aware.link/0000.

  Wir benutzen einen sogenannten Link-Verkürzungsdienst. Dieser hilft uns, alle Links im Buch aktuell zu halten – auch wenn das Buch bereits

gedruckt ist. Denn Webseiten ändern sich regelmäßig oder sind nicht mehr verfügbar. Alle Links sind durch uns manuell geprüft und stellen kein Risiko dar. Sollte ein Link wider Erwarten nicht funktionieren, schreiben Sie uns gerne eine E-Mail an info@aware7.de mit dem Betreff »MDSTT Link«.

- Sie können das Buch am Stück, kapitelweise oder nur bei Bedarf lesen. Und weil die folgenden Seiten sehr praktisch orientiert sind, benutzen wir nicht einfach Fantasienamen für unsere Beispiele: Wir verwenden die Firma »Franken Logistik« aus Bamberg. Frau Ann-Kathrin Boumann ist unsere beliebteste Mitarbeiterin in dem Unternehmen und hält in privaten und beruflichen Belangen für zahlreiche unserer Beispiele her. Weder Firma noch Person sind echt. Die Identitäten haben wir frei erfunden. Sie haben keinen Bezug zu echten Personen.

Symbole, die in diesem Buch verwendet werden

Bestimmte Arten von Informationen werden durch Symbole hervorgehoben:

 Bei der Glühbirne finden Sie kleine Tipps und Tricks, die wir als praktisch empfinden und die Ihnen weiterhelfen können. Serviert in kleinen Häppchen.

 Der Techniker liefert tiefergehende Informationen zu einem bestimmten Thema. Sie müssen diese Abschnitte nicht lesen, allerdings sind die meisten davon durchaus so interessant, dass es sich lohnt …

Aufpassen! Bei dem Warndreieck ist Vorsicht geboten und wir empfehlen Ihnen, an diesen Stellen besonders aufmerksam zu sein.

Bei dem Fernglas finden Sie Beispiele und mehr. Oft erzählen wir Ihnen dort zur Verdeutlichung eines Sachverhalts eine Geschichte, teilweise aus unserer beruflichen Praxis, teilweise aus privaten Erfahrungen.

Kapitel 1

Basiswissen und Softskills

Die Digitalisierung ist aus kaum einem Leben mehr wegzudenken. Der Blick auf das Smartphone direkt nach dem Aufstehen ist für viele Menschen alltäglich geworden. Und bereits vor dem Frühstück haben wir vielfältige Möglichkeiten, mit unserem Smartphone Informationen aufzunehmen, zu kommunizieren und Inhalte zu erstellen.

Digitale Technologie ist überall um uns herum, und damit diese intelligent wird, muss sie vernetzt werden. Diesen technologischen Fortschritt verdanken wir dem Internet. Es gibt jedoch wie so oft zwei Seiten der Medaille und neben den beeindruckenden Chancen eben auch ernstzunehmende Risiken bei der Nutzung des Internets.

Digitale Sicherheit bei digitalen Gefahren

Neue Geräte, neue Apps, neue Software, neue Möglichkeiten – mit der Nutzung nehmen auch die Risiken im Umgang mit modernen Technologien zu, da wir vermehrt Wertvolles im Internet hinterlassen: von unseren Urlaubsfotos bis hin zu getätigten Online-Zahlungen und anderen Bankdaten.

Die Gefahrenlage hat sich im Vergleich zu früher verändert. Menschen werden heute Opfer von realem Betrug im Internet. Gefälschte E-Mails, das Vortäuschen falscher Identitäten oder schlichtweg Schadsoftware