edv-buchversand.de

Digitale Selbstverteidigung für Dummies

» Hier geht's direkt zum Buch

DAS VORWORT

Dieses Vorwort wird Ihnen von www.edv-buchversand.de zur Verfügung gestellt.

Einführung

Digitale Selbstverteidigung – was ist das überhaupt?

Wenn Sie dieses Buch zur Hand genommen haben, dann haben Sie selbst wahrscheinlich vage – oder auch ganz konkrete – Gefahren im Hinterkopf.

Vielleicht ist Ihnen (oder jemandem aus Ihrer Familie oder aus Ihrem Freundeskreis) schon einmal Folgendes passiert:

- ✔ Sie sind im Netz auf eine Betrugsmasche hereingefallen. Sie haben zum Beispiel auf den Link in einer Phishingmail geklickt und dabei Ihren Computer mit einem Virus infiziert oder ein geheimes Passwort preisgegeben.
- ✔ Sie sind Opfer von digitaler Sabotage oder Erpressung geworden – beispielsweise sind Sie von einem Kryptotrojaner befallen worden.
- ✔ Sie werden in sozialen Medien beleidigt, bedroht oder gestalkt – von Bekannten oder Unbekannten.
- ✔ Sie sind ehrenamtlich engagiert oder in einem Verein oder einer Initiative organisiert und fürchten Manipulation Ihrer digitalen Kommunikation durch »Trolle« und andere Störenfriede.
- ✔ Oder Sie haben bemerkt, wie die digitale Durchdringung des Alltags Ihre Gewohnheiten verändert, Ihre Konzentration und Aufmerksamkeit pulverisiert und zwischenmenschliche Kontakte verdrängt. Vielleicht sind Sie es auch einfach leid, von Ihren Apps subtil bevormundet zu werden.

In diesem Buch werden Sie Gegenmaßnahmen kennenlernen.

Zwei Einschränkungen müssen Sie dabei beachten:

- ✔ Dieses Buch ersetzt keine Rechtsberatung.
- ✔ In einer digitalisierten Welt kann es keine hundertprozentige Sicherheit gegenüber digitalen Angriffen geben. Selbst, wenn Sie sich sorgfältig in alle Richtungen absichern, kann es immer einen Angreifer geben, der mehr Ressourcen hat als Sie oder eine bisher unbekannte Sicherheitslücke ausnutzt.

Aber wenn Sie zumindest ein paar der in diesem Buch vorgebrachten Vorschläge befolgen, dann werden Sie Ihre persönliche Sicherheit im Netz deutlich verbessern.

Warum ist es häufig so schwer, einfache Sicherheitsmaßnahmen langfristig durchzuhalten? Das liegt daran, dass eine erfolgreiche Vorbeugung dazu führt, dass im Prinzip gar nichts passiert. Und »gar nichts« ist nun mal völlig unspektakulär.

Ein Beispiel: Wenn Sie für Ihr E-Mail-Konto ein langes und kompliziertes (also sicheres) Passwort wählen, dann denken Sie nicht jeden Abend zufrieden darüber

nach, dass auch heute wieder niemand in Ihr E-Mail-Konto eingebrochen ist. Im Gegenteil, Sie erinnern sich vielleicht nur daran, dass Sie sich beim Eingeben dreimal vertippt haben oder Sie Ihren Passwortmanager neu installieren mussten. Solche kleinen Ärgernisse bleiben eher im Bewusstsein als das Ausbleiben einer Katastrophe.

Törichte Annahmen über die Leser

Sie als Leserin oder Leser dieses Buchs müssen keine technischen Vorkenntnisse mitbringen, um es zu verstehen, und schon gar keine Berufserfahrung in einem technologischen Feld.

Dieses Buch wird für Sie nützlich und verständlich sein, wenn Sie digitale Tools in ganz normalem Umfang einsetzen, wenn Sie also gelegentlich E-Mails oder WhatsApp-Nachrichten verschicken, wenn Sie im Internet surfen und dabei zum Beispiel soziale Netzwerke nutzen oder mal in einem Onlineshop einkaufen.

Aber auch wenn Sie schon etwas fortgeschritten im Bereich der digitalen Privatsphäre sind – wenn Sie zum Beispiel schon Ihre E-Mails signieren oder sich über datenschutzfreundliche Messenger schlaugemacht haben –, finden Sie in diesem Buch bestimmt noch interessante neue Informationen und Anregungen.

Wie dieses Buch aufgebaut ist

Dieses Buch besteht aus sechs Teilen. Jeder Teil ist auch für sich allein verständlich, Sie müssen das Buch also nicht von vorn bis hinten lesen.

Überall im Buch finden Sie auch Verweise auf andere Buchstellen, wenn diese zum Verständnis hilfreich sind.

Teil I: Wer ist hier der Boss? Digitale Souveränität

In Teil I erfahren Sie, warum Sie sich überhaupt mit dem Thema digitale Selbstverteidigung beschäftigen sollten und was das Ganze mit digitaler Souveränität zu tun hat.

Sie erfahren, dass Sie selbst darüber bestimmen können, welche Daten Sie online teilen wollen – auch ohne Ihr Leben komplett offline zu führen.

Und Sie lernen einige Organisationen kennen, die auf Ihrer Seite sind.

Teil II: Spurensuche – diese Daten hinterlassen wir im Netz

In diesem Teil erfahren Sie, welche Spuren Sie freiwillig und unfreiwillig im Netz hinterlassen. Sie lernen etwas über den Unterschied zwischen Anonymität und Pseudonymität, und dass echte Anonymität sehr schwer herzustellen ist.

Und schließlich schauen wir uns die wichtigsten digitalen Fußabdrücke im Detail an: von der IP-Adresse über Cookies und Standortdaten bis hin zu Ihren Social-Media-Konten, und weitere.

Teil III: Sicher kommunizieren

In Teil III dieses Buchs befassen wir uns mit der Frage, ob es in der digitalen Welt eigentlich auch ein Briefgeheimnis gibt. (Spoiler: Ja!)

Sie lernen, was Verschlüsselung ist und wie Sie damit Ihre Privatsphäre schützen, und wie symmetrische, asymmetrische und hybride Verschlüsselung funktioniert.

Und außerdem erfahren Sie, was das alles mit der digitalen Signatur zu tun hat, und wozu Sie sie gebrauchen können.

So weit die Theorie, und dann wird es praktisch: Sie erfahren, was PGP und S/MIME sind, mit denen Sie Verschlüsselung und digitale Signatur umsetzen können. Und auch, wie beide Verfahren sich unterscheiden und wie Sie entscheiden können, was für Sie besser geeignet ist.

Und schließlich lernen Sie auch etwas darüber, wie Sie nicht nur über E-Mail, sondern auch per Instant Messaging und mit anderen Medien sicher kommunizieren können.

Teil IV: Sicher im Web unterwegs

Hier geht es um Ihre Privatsphäre im Web: Wir schauen uns zunächst an, was ein Browser ist und was Ihr Browser alles über Sie weiß.

Am Beispiel von Mozilla Firefox lernen Sie, welche Einstellungen Sie im Browser treffen können, um Ihre Privatsphäre zu schützen, und wie Sie mit Erweiterungen Ihre Browser-Sicherheit noch weiter verbessern können.

Und schließlich erfahren Sie noch, wie Sie mit dem Tor-Netzwerk (fast) anonym browsen können, und Sie lernen ein kleines Betriebssystem kennen, mit dem Sie sogar mit einem öffentlichen oder fremden Rechner sicher ins Internet können: nämlich Tails.

Teil V: Top-Ten-Teil

Mit diesem Teil schließen alle Bücher der Dummies-Reihe ab. In diesem hier finden Sie im Top-Ten-Teil zehn gute Gewohnheiten, die Ihnen helfen, Ihre digitale Privatsphäre wiederzugewinnen.

Symbole, die in diesem Buch verwendet werden

Mit diesem Symbol sind Definitionen gekennzeichnet.

Hier finden Sie konkrete Beispiele, die die Aussagen aus dem Haupttext mit Leben füllen.

Als Tipp sind Infos und Hintergründe gekennzeichnet, die besonders wichtig oder interessant sind und die Sie sich vielleicht merken möchten.

Unter dem Techniker-Symbol finden Sie Exkurse, die ein technisches Thema vertiefen, aber nicht unbedingt zum weiteren Verständnis des Textes notwendig sind.

Mit diesem Symbol werden Sie vor gängigen Missverständnissen oder Fallgruben gewarnt.

Wie es weitergeht

Haben Sie Fragen oder Anmerkungen zu diesem Buch? Sie erreichen mich unter der E-Mail-Adresse czeschik@serapion.de. Ich freue mich auf Ihre Rückmeldungen!