DIGTALE
SELBSTVERTEIDIGUNG

Was Sie wissen müssen, um sich online zu schützen!

Inhaltsverzeichnis

Datenschutz-
GRUNDSÄTZE

1

Nicht immer kann man anonym bleiben. Wenn man persönliche Daten weitergibt, ist es wichtig, gut mit ihnen umzugehen. Das bedeutet:

1. Daten verschlüsseln, bevor man sie verschickt

2. Sicher speichern, damit niemand unbefugt zugreifen kann

3. Vollständig löschen, wenn man die Daten nicht mehr braucht

Wenn Daten zur

BEUTE WERDEN

2

Im Internet lauern Datendiebe – und Ihre Informationen sind ihr Ziel!

Ob Namen, E-Mail-Adressen oder Bankdaten: Was Sie preisgeben, kann gegen Sie verwendet werden – für Werbung, Betrug oder Identitätsdiebstahl. Und oft merken Sie es zu spät.

Schon eine kleine Unachtsamkeit kann reichen, um die Kontrolle über Ihre Daten zu verlieren!

3

Darum gilt:

- **Geben Sie nur das Nötigste preis**
- **Halten Sie Ihre Geräte und Programme aktuell**
- **Klicken Sie niemals unbedacht auf Links oder Anhänge**
- **Nutzen Sie starke, einzigartige Passwörter**
- **Schützen Sie Ihre Geräte mit PIN, Fingerabdruck oder Gesichtserkennung**

Wer nicht aufpasst, wird zur leichten Beute!

Datenklau:
SO EINFACH GEHT'S

4

Daten lassen sich auf viele Arten sammeln – oft ganz legal, oft unbemerkt.

Wer die Methoden kennt, versteht, warum Schutz so wichtig ist:

Logs & Metadaten

Mehr als nur technische Infos

Jedes Gerät, jede App und jede Website erzeugt sogenannte Logs – also Protokolle über Ihre Aktivitäten. Metadaten verraten, wann, wo und wie etwas passiert ist – auch wenn der Inhalt verschlüsselt war. Diese Informationen sagen oft mehr über Sie aus als gedacht.

Phishing

5

Die digitale Falle

Gefälschte E-Mails oder Nachrichten wirken täuschend echt. Ein Klick auf den falschen Link – und Zugangsdaten, Kreditkarteninfos oder ganze Konten sind in den Händen von Cyberkriminellen.

Social Engineering

Die Schwachstelle Mensch

Kriminelle nutzen gezielte Manipulation, um Vertrauen zu gewinnen. Oft reicht ein harmlos wirkender Anruf, eine Chatnachricht oder eine gefälschte Identität – und schon werden Passwörter oder sensible Daten freiwillig preisgegeben.

Open Source Intelligence

Alles, was öffentlich ist, wird zur Waffe

Was Sie online posten, liken oder teilen, kann systematisch ausgewertet werden. Öffentlich verfügbare Quellen wie Foren, Social Media, Jobportale oder Register liefern oft erschreckend detaillierte Profile – ganz ohne Einbruch.

Dumpster Diving

6

Was im Müll liegt, ist nicht vergessen

Auch analoge Informationen sind wertvoll: alte Briefe, Kontoauszüge, Notizzettel, USB-Sticks. Wer gezielt Müll durchsucht, findet oft mehr, als man denkt – und das ganz ohne Technik.

Gesetze & Überwachung

Nicht jeder Zugriff ist kriminell

Auch der Staat hat Interesse an Ihren Daten. Ob Vorratsdatenspeicherung, Online-Durchsuchung oder Standortabfrage: Behörden dürfen unter bestimmten Voraussetzungen auf persönliche Informationen zugreifen – oft ohne Ihr Wissen.

Fazit: Wer seine Daten schützen will, muss wissen, wie sie gesammelt werden.

Technik allein reicht nicht – Aufmerksamkeit, Wissen und gesunder Menschenverstand sind Ihre besten Verteidiger.

Sichere
PASSWÖRTER

7

Ein Passwort ist oft das Einzige, was zwischen Ihren Daten und einem Angreifer steht.

Leider sind viele Passwörter zu einfach, zu kurz oder mehrfach verwendet – genau das machen sich Cyberkriminelle zunutze.

Sie wissen:

Menschen wählen oft bequeme Passwörter, die sie sich leicht merken können – und genau das wird ihnen zum Verhängnis.

Ein Passwort ist oft das Einzige, was zwischen Ihren Daten und einem Angreifer steht.

8

Unsichere Passwörter wie „123456“, „Passwort“ oder das eigene Geburtsdatum sind eine Einladung an Angreifer – und werden täglich millionenfach geknackt.

Spezialisierte Programme brauchen oft nur wenige Sekunden, um einfache Kombinationen zu erraten.

Selbst scheinbar „kreative“ Varianten wie „Sommer2024“ oder „Peter123“ bieten kaum Schutz.

Wer bei Passwörtern spart, riskiert den vollständigen Kontrollverlust!

So sieht ein sicheres Passwort aus:

9

- **Mindestens 12 Zeichen**
- **Groß- und Kleinbuchstaben**
- **Zahlen und Sonderzeichen**
- **Keine echten Wörter, Namen oder Daten**
- **Für jeden Dienst, Konto und Anbieter ein eigenes Passwort**

Am besten nutzen Sie einen Passwort-Manager – oder gleich einen starken Generator.

Kostenloser

Passwortgenerator

10

Sie wissen nicht, wie Sie sich sichere Passwörter ausdenken sollen? Kein Problem!

Nutzen Sie meinen kostenlosen Passwortgenerator unter:

http://www.passwortgenerator.stefanweise.info

Dort erstellen Sie mit wenigen Klicks lange, sichere und zufällige Passwörter, die wirklich schützen – ganz ohne Werbung oder Datenweitergabe.

Sichere DATENVERSCHLÜSSELUNG

11

Daten sind wie Wertgegenstände: Man schützt sie nicht mit einem Vorhängeschloss – sondern mit starker Verschlüsselung

Ob auf dem eigenen Gerät, beim Versenden per E-Mail oder beim Surfen im Internet – Verschlüsselung schützt, was privat bleiben soll.

Eigene Daten sicher verschlüsseln

Speichern Sie persönliche Dokumente, Fotos oder Notizen nur auf Geräten, die gut geschützt sind.

Webseiten und Online-Shops: Achten Sie auf „https“

12

Wenn Sie im Internet surfen, sollten Sie stets auf das kleine Schloss-Symbol in der Adresszeile im Webbrowser achten. Es zeigt: Die Verbindung ist mit HTTPS verschlüsselt.

Nur dann können Dritte nicht mitlesen, was Sie auf der Seite tun – z. B. beim Online-Banking, Einkaufen oder Ausfüllen von Formularen.

E-Mails: Nur verschlüsselt ist privat und vertraulich!

Normale E-Mails sind wie Postkarten – jeder kann mitlesen. Wer sensible Inhalte verschickt, sollte auf Ende-zu-Ende-Verschlüsselung setzen.

13

Wenn Sie im Internet surfen, sollten Sie stets auf das kleine Schloss-Symbol in der Adresszeile im Webbrowser achten. Es zeigt: Die Verbindung ist mit HTTPS verschlüsselt.

Bewährt hat sich PGP, z. B. mit GNU Privacy Guard (GnuPG). Damit lassen sich E-Mails verschlüsseln und digital unterschreiben – etwa mit Programmen wie Thunderbird oder Mailvelope.

Noch einfacher geht’s mit sicheren Maildiensten wie ProtonMail – dort ist die Verschlüsselung bereits integriert.

Fazit: Nur verschlüsselte E-Mails bleiben wirklich privat.

Datenschutz FÜR UNTERWWEGS

14

Auch unterwegs sind Ihre Daten angreifbar – oft sogar noch leichter als zu Hause.

Öffentliche und kostenlose WLAN-Angebote, neugierige Blicke oder gestohlene Geräte können schnell zum Risiko werden.

So schützen Sie sich unterwegs:

→ Aktivieren Sie Displaysperren wie PIN, Passwort, Fingerabdruck oder Face ID

→ Deaktivieren Sie Bluetooth und WLAN, wenn Sie es nicht brauchen

15

→ Vermeiden Sie öffentliches WLAN – oder nutzen Sie ein VPN

→ Speichern Sie keine sensiblen Daten unverschlüsselt auf Ihrem Gerät (Smartphone, Laptop etc.)

→ Sichern und aktualisieren Sie Ihr Gerät regelmäßig und verschlüsseln Sie Backups

Ein zusätzlicher Schutz für besonders sensible Situationen: Faraday-Taschen.

Diese speziellen Hüllen blockieren Funkverbindungen wie WLAN, Bluetooth, GPS und Mobilfunk vollständig.

So verhindern Sie ungewollte Ortung, stille SMS oder drahtlose Zugriffe auf Ihr Gerät

16

Verschlüsselte

MESSENGER

Viele nutzen Messenger täglich – zum Plaudern, Teilen und Planen. Doch was kaum jemand bedenkt: Nicht jeder Messenger schützt Ihre Privatsphäre.

Oft werden Inhalte unverschlüsselt gespeichert, Kontakte analysiert oder sogar Bewegungsdaten mit Dritten geteilt.

Selbst wenn „Ende-zu-Ende-Verschlüsselung“ versprochen wird, bleibt oft unklar, was tatsächlich geschützt wird – und wer mitliest.

17

Eine klare Empfehlung für echten Schutz: Signal – www.signal.org

Signal ist ein datenschutzfreundlicher, vollständig verschlüsselter Messenger, der keine Metadaten speichert, keine Werbung zeigt und völlig unabhängig betrieben wird.

Selbst die Telefonnummern werden anonymisiert verarbeitet – und Gespräche, Bilder und Dateien sind durchgängig abgesichert.

Fazit: Wer vertraulich kommunizieren will, sollte nicht einfach den bequemsten Messenger wählen – sondern den sichersten.

18

Anonym

SURFEN

Wenn Sie online gehen, hinterlassen Sie Spuren:

Ihre IP-Adresse, Ihren Standort, die besuchten Seiten oder Geräteinformationen – alles wird mitprotokolliert.

Diese Daten können genutzt werden, um Bewegungsprofile zu erstellen, Ihre Interessen auszulesen oder sogar Ihre Identität zurückzuverfolgen.

Doch Sie können sich schützen – und anonym im Netz bewegen.

Tor – Ihr Schutz durch Verschleierung

19

Mit dem Tor-Netzwerk leiten Sie Ihre Verbindung über mehrere Server auf der ganzen Welt.

Jeder Abschnitt dieser Verbindung ist verschlüsselt.

Dadurch bleibt Ihre IP-Adresse verborgen – und niemand kann nachvollziehen, welche Seiten Sie besuchen oder woher Sie kommen.

Mit dem kostenlosen Tor-Browser können Sie direkt loslegen.

Er bietet eine einfache Möglichkeit, sicher und anonym zu surfen, besonders bei sensiblen Themen oder in ungeschützten Netzwerken.

VPN – Damit niemand sieht, wo Sie wirklich sind

20

Ein VPN (Virtuelles Privates Netzwerk) verschlüsselt Ihre gesamte Internetverbindung und tarnt Ihre IP-Adresse, indem es sie durch einen externen Server ersetzt.

So schützen Sie sich vor neugierigen Blicken – sei es durch Ihren Internetanbieter, öffentliche WLANs oder staatliche Überwachung.

So schützen Sie sich vor neugierigen Blicken – sei es durch Ihren Internetanbieter, öffentliche WLANs oder staatliche Überwachung.

21

Ein VPN eignet sich besonders gut für unterwegs, auf Reisen oder im Homeoffice – immer dann, wenn Sie sicher und geschützt auf das Internet zugreifen möchten.

Bei der Auswahl eines VPN-Anbieters sollten Sie auf Datenschutzrichtlinien, Standort des Unternehmens und Transparenz im Umgang mit Nutzerdaten achten.

Ein seriöser Anbieter speichert keine Logs, bietet stabile Serververbindungen und lässt sich idealerweise unabhängig prüfen.

Verzichten Sie auf vermeintlich „kostenlose“ Angebote – sie bezahlen oft mit Ihren Daten.

22

Daten
RICHTIG LÖSCHEN

Was viele nicht wissen: Gelöschte Daten sind oft nicht wirklich weg.

Beim einfachen Löschen wird nur der Verweis entfernt – die eigentlichen Daten bleiben auf dem Gerät und können wiederhergestellt werden.

Wer sicher gehen will, sollte Daten mit speziellen Programmen überschreiben oder verschlüsselt löschen.

Das gilt für Festplatten, USB-Sticks, Smartphones und auch Cloud-Speicher.

Nur so stellen Sie sicher, dass persönliche Informationen nicht in falsche Hände geraten.

Datenschutz-
CHECKLISTE

23

- [ ] Datenschutzgrundsätze verstanden
- [ ] Daten als Beute verstanden
- [ ] Verstanden wer Ihre Daten klauen will
- [ ] Den Passwort-Generator verwendet
- [ ] Daten verschlüsselt
- [ ] Datenschutz für Unterwegs umgesetzt
- [ ] Verschlüsselte Messenger verwenden
- [ ] Anonym im Internet gesurft
- [ ] Daten richtig gelöscht

EIGENE NOTIZEN

Haben Sie noch Fragen?

Ich berate Sie gerne:

E-Mail: anfrage@stefanweise.info

Sie finden mich auch auf:

X/Twitter: @stefan_weise

IMPRESSUM

Stefan Weise
Einsteinstraße 22
71229 Leonberg

Redaktionell verantwortlich:
Stefan Weise

Kontakt
Telefon: 071523811929
E-Mail: legal@stefanweise.info
Webseite: www.stefanweise.info