
# Datenschutz: Ein Leitfaden für Einzelpersonen und Familiens

Schützen Sie Ihre Online-Informationen und Ihren digitalen Fußabdruck.

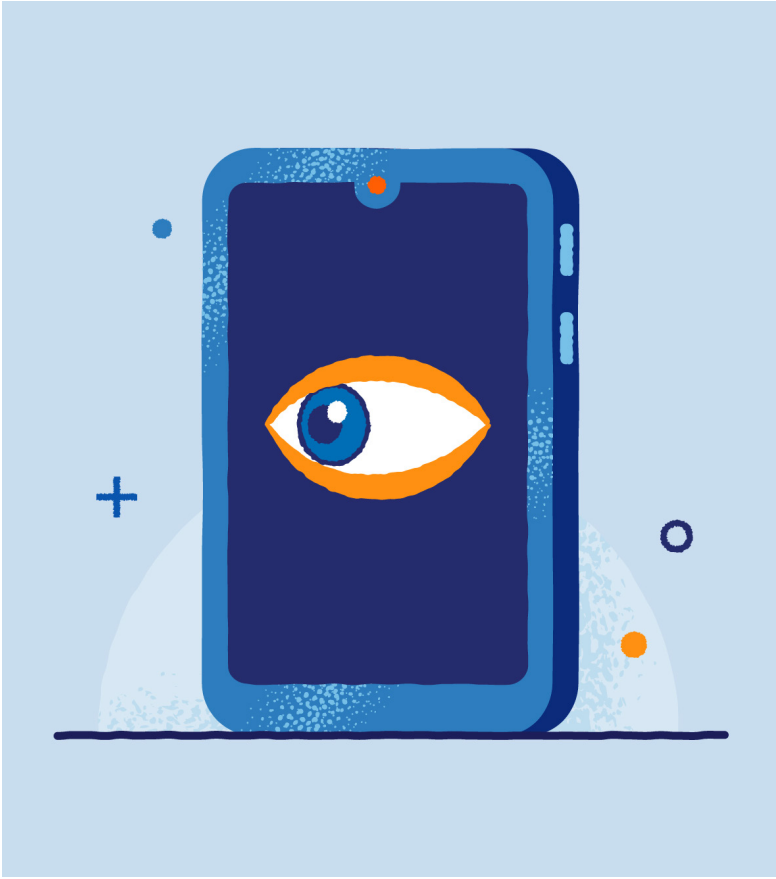
panda

# Inhalt

# 01.
# Grundlagen des Datenschutzes

Im digitalen Zeitalter ist der Datenschutz zu einem unscheinbaren Hauptdarsteller geworden. Er ist die geheimnisvolle Gestalt, die hinter jeder gesendeten E-Mail, jeder getätigten Transaktion und jeder besuchten Website lauert. Dennoch ist vielen der Datenschutz fremd und wird nicht selten übersehen, bis es zu spät ist.

Beim Datenschutz geht es darum, Ihre personenbezogenen Daten sicher unter Verschluss zu halten. Unternehmen, Regierungen und Cyberkriminelle sind aus verschiedenen Gründen auf der Suche nach diesen Daten. Aus diesem Grund ist es wichtig zu wissen, wie man Daten schützt. Glücklicherweise gibt Ihnen dieses umfassende E-Book zum Datenschutz die Informationen an die Hand, die Sie benötigen, um die Kontrolle über Ihren digitalen Fußabdruck zu erlangen.



## Was ist Datenschutz?

**Datenschutz** ist die Kontrolle, die eine Person oder ein Unternehmen über ihre bzw. seine gespeicherten oder erfassten sensiblen Daten hat. Er umfasst die Fähigkeit zu bestimmen, wer Zugriff auf diese Daten hat, wie sie verwendet werden und welche Sicherheitsvorkehrungen getroffen werden, um sie vor unbefugtem Zugriff zu schützen.

Personenbezogene Daten im Zusammenhang mit dem Datenschutz enthalten sensible Informationen wie Namen, Adressen, Sozialversicherungsnummern und Finanzdaten. Sie erstrecken sich zudem auf weniger offensichtliche personenbezogene Daten wie den Browserverlauf, Standortdaten, IP-Adressen und Online-Einkäufe. Darüber hinaus können sie biometrische Daten, Daten aus Patientenakten und Angaben zur Beschäftigung umfassen.

Das Konzept des Datenschutzes geht auf die Anfänge der Computertechnik zurück, als personenbezogene Daten für verschiedene Zwecke elektronisch gespeichert wurden. Mit der Ausweitung der digitalen Landschaft haben auch die Bedenken um Datenmissbrauch und Datenschutzverletzungen rapide zugenommen.

Durch die Entwicklung der sozialen Medien wurden diese Bedenken noch verstärkt. Da Nutzer personenbezogene Daten auf Plattformen wie Facebook und Twitter bereitwillig veröffentlichen, hat die Menge der erzeugten Daten ein noch nie dagewesenes Ausmaß angenommen.

# Warum Datenschutz wichtig ist

Angesichts des rasanten technologischen Fortschritts ist der Datenschutz und Schutz der Privatsphäre nicht mehr nur eine Option, sondern ein Muss. Der Datenschutz hängt davon ab, dass Einzelpersonen die Möglichkeit haben, die Kontrolle über ihren digitalen Fußabdruck zu übernehmen.

Jedes Mal, wenn wir uns mit dem Internet verbinden, erzeugen wir eine große Menge an Daten. Von einfachen Likes in sozialen Medien bis hin zu unseren Einkaufsgewohnheiten zeichnen diese scheinbar harmlosen Daten ein lebendiges Porträt von uns.

**Wenn diese privaten Daten in die falschen Hände geraten, kann das Folgen haben wie:**

### Identitätsdiebstahl

Persönliche Daten könnten in die falschen Hände geraten, was zu Identitätsbetrug führen könnte, bei dem Einzelpersonen mit unbefugten Transaktionen oder kriminellen Aktivitäten in ihrem Namen konfrontiert werden könnten.

### Finanzbetrug

Mit dem Zugriff auf sensible Finanzdaten könnten Cyberkriminelle betrügerische Transaktionen durchführen, die zu schweren finanziellen Verlusten führen.

### Vertrauensverlust

Unternehmen könnten das Vertrauen ihrer Kunden verlieren, was sich auf die Kundentreue auswirkt und zu Geschäftseinbußen führt.

### Rechtliche Auswirkungen

Bei Nichteinhaltung der Datenschutzgesetze und -vorschriften drohen Unternehmen hohe Geldstrafen und rechtliche Schritte, die ihren Ruf und ihre Finanzen schädigen können.

### Zunahme der Cyberkriminalität

Das Risiko von Cyberangriffen könnte steigen, da immer mehr wertvolle Daten für Hacker leicht zugänglich sind.

### Verlust der Privatsphäre

Ohne Datenschutz könnte unser Privatleben zu einem offenen Buch werden, das für jeden einsehbar ist.

### Manipulation und Ausbeutung

Daten könnten dazu verwendet werden, Verhalten und Entscheidungen zu manipulieren, oft ohne das Wissen oder die Zustimmung von Einzelpersonen

# Datenschutz, Privatheit von Daten und Datensicherheit im Vergleich

Datenschutz, Privatheit von Daten und Datensicherheit sind drei miteinander verwobene und doch unterschiedliche Konzepte in der Welt der digitalen Daten.


Datenschutz, Privatheit von Daten und Datensicherheit sind aufeinander abgestimmt. Jedes Konzept hat seine eigene Rolle, aber zusammen schaffen sie eine sichere digitale Umgebung.

# 02.
# Personenbezogene und sensible per-sonenbezogene Daten

Auf dem weitreichenden Gebiet des Datenschutzes ist es von entscheidender Bedeutung, den Unterschied zwischen personenbezogenen und sensiblen personenbezogenen Daten für die Einhaltung rechtlicher Vorschriften, das Risikomanagement und ethische Überlegungen zu kennen. Dies dient als Grundlage für den Umgang mit Daten, als Leitfaden für Sicherheitsmaßnahmen und trägt dazu bei, den potenziellen Schaden für Einzelpersonen zu minimieren, wenn Daten kompromittiert sind.

In diesem Abschnitt werden die verschiedenen Ebenen der Datenklassifizierung aufgeschlüsselt und es wird erläutert, wie Sie die intimsten Details Ihrer digitalen Identität schützen können.

## Was sind personenbezogene Daten?

Personenbezogene Daten, oft auch personenbezogene Informationen genannt, sind alle Informationen, die zur Identifizierung einer bestimmten Person verwendet werden können. Sie umfassen ein breites Spektrum von Daten, die mit einer bestimmten Person in Verbindung gebracht werden können. Je nach Kontext können sie Namen, Adressen, Telefonnummern usw. enthalten.

## Wie können Sie die Kontrolle über Ihre personenbezogenen Daten übernehmen?

Damit Sie wirklich die Kontrolle über Ihre personenbezogenen Daten haben, müssen Sie unbedingt proaktive Maßnahmen ergreifen, die Ihre Online-Privatsphäre und -Sicherheit verbessern. Im Folgenden finden Sie einige wichtige Tipps, die Sie im Hinterkopf behalten sollten.

### Halten Sie Ihre Präsenz in den sozialen Medien in Grenzen

Überprüfen Sie Ihre Privatsphäre-Einstellungen auf Social-Media-Plattformen und passen Sie sie an, um festzulegen, wer Ihre Beiträge und persönlichen Informationen sehen kann.

### Denken Sie nach, bevor Sie etwas posten

Bevor Sie personenbezogene Daten online veröffentlichen, sollten Sie die möglichen Folgen bedenken und überlegen, ob die Veröffentlichung dieser Informationen notwendig ist.

### Lesen Sie die Datenschutzrichtlinien

Nehmen Sie sich die Zeit, die Datenschutzrichtlinien der von Ihnen genutzten Websites und Apps zu lesen und zu verstehen, damit Sie wissen, wie Ihre Daten erfasst, gespeichert und weitergegeben werden.

### Lehnen Sie die Datenerfassung ab

Lehnen Sie die Datenerfassung ab, wann immer dies möglich ist, und wählen Sie Dienste, die nur die wichtigsten Informationen abfragen.

## Was sind sensible personenbezogene Daten?

Sensible personenbezogene Daten bilden eine Kategorie personenbezogener Daten, die als kritischer angesehen werden und ein höheres Maß an Schutz erfordern. Sie enthalten Details, deren Offenlegung zu schwerwiegenden Folgen wie Identitätsdiebstahl, Cyberstalking oder Diskriminierung führen könnte.

# Wie können Sie die Kontrolle über Ihre sensiblen personenbezogenen Daten übernehmen?

Heutzutage ist es wichtiger denn je, die Kontrolle über Ihre sensiblen personenbezogenen Daten zu haben. Angesichts der zunehmenden Anzahl an Datenschutzverletzungen und anderen Cyberbedrohungen ist es unerlässlich, proaktive Maßnahmen zum Schutz dieser wertvollen Daten zu ergreifen.

## Reichen Sie als betroffene Person einen Antrag auf Auskunft über personenbezogene Daten ein

- **Sie sollten Ihre Rechte kennen:** Under the General Data Protection Regulation (GDPR), you have the right to ask an organization whether or not it is processing your data.

- **Ersuchen Sie Auskunft über Ihre Daten:** Mit einem Antrag auf Auskunft über Ihre Daten können Sie Auskunft über Ihre gespeicherten Daten erhalten und deren Verwendung nachvollziehen.

- **Beantragen Sie die Berichtigung Ihrer Daten:** Beantragen Sie die Berichtigung unrichtiger Daten oder deren Löschung. Unternehmen müssen Ihrem Antrag gemäß DSGVO innerhalb eines Kalendermonats und gemäß dem California Consumer Privacy Act (CCPA) innerhalb von 45 Tagen nachkommen.

## Verwenden Sie die Links „Meine personenbezogenen Daten nicht verkaufen oder weitergeben“

- **Überprüfen Sie die Websites von Unternehmen:** Achten Sie auf erweiterte Optionen wie „Meine personenbezogenen Daten nicht verkaufen oder weitergeben“ im Rahmen des California Privacy Rights Act (CPRA) auf den Homepages und Seiten mit Datenschutzrichtlinien von Unternehmen.

- **Lehnen Sie Folgendes ab:** Den Verkauf oder die Weitergabe Ihrer personenbezogenen oder sensiblen Daten an Dritte. Unternehmen sind gesetzlich verpflichtet, Ihrem Antrag nachzukommen

## Lehnen Sie die Datenerfassung auf Websites oder in Browsern ab

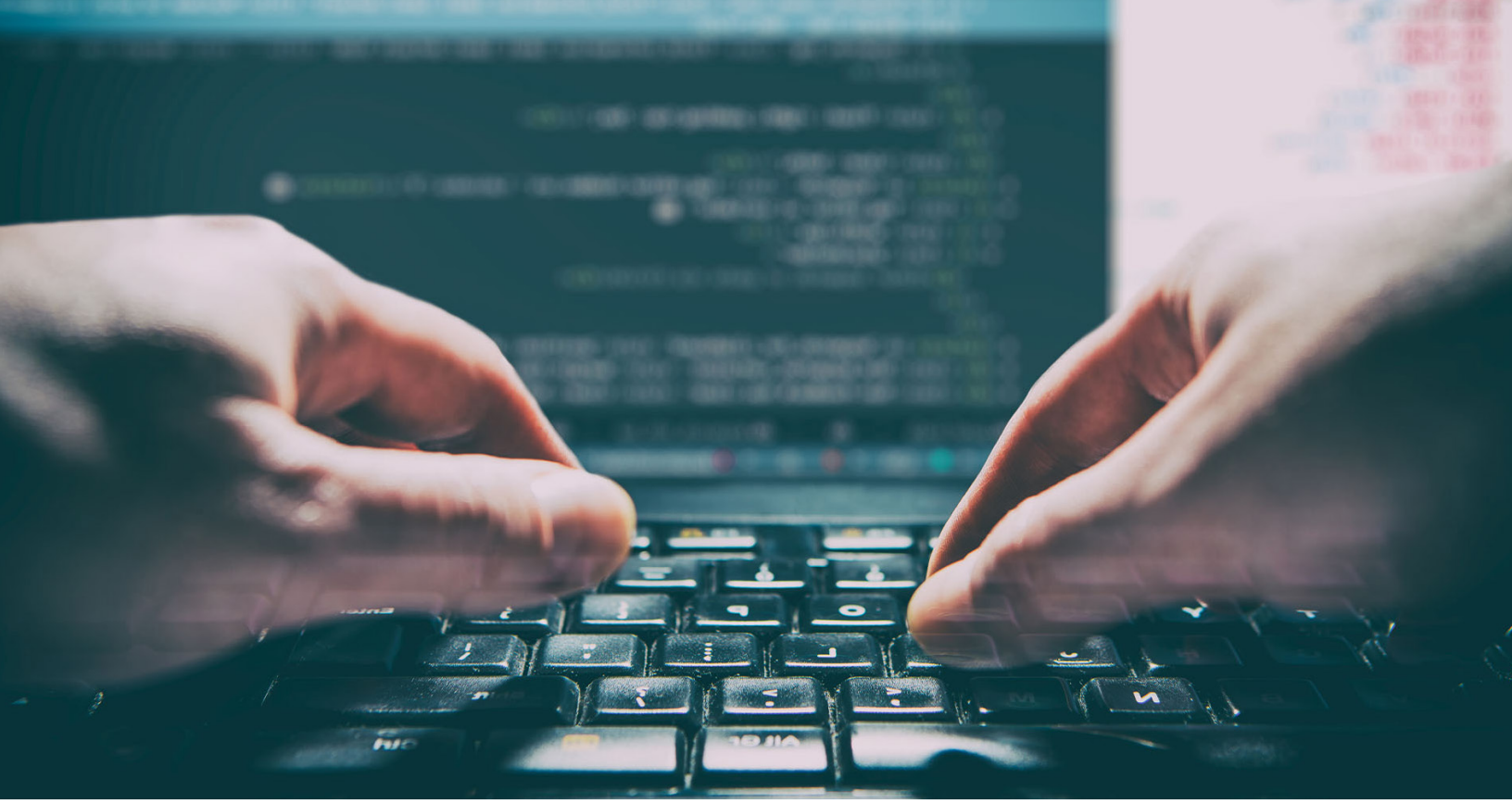
- **Führen Sie eine Online-Suche durch:** Führen Sie eine Online-Suche nach Ihrem Namen durch, um Datenbroker-Websites wie Radaris, Pipl, Spokeo und Whitepages zu finden, die Ihre Informationen auflisten.

- **Beantragen Sie die Löschung Ihrer Daten:** Besuchen Sie die Seiten dieser Plattformen, auf denen Sie die Datenerfassung ablehnen können, oder senden Sie eine E-Mail-Anfrage, um Ihre Daten löschen zu lassen.

- **Nutzen Sie Ressourcen:** Nutzen Sie Ressourcen wie Privacy Rights Clearinghouse für ein umfassendes Verzeichnis von Websites und deren Optionen zum Ablehnen der Datenerfassung.

- **Überprüfung Sie die Datenschutzrichtlinien:** Überprüfen Sie die Datenschutzrichtlinien Ihrer Finanzinstitute, um die Weitergabe von Daten an Datenbroker zu unterbinden.

# 03.
# Verständnis von Datenschutzverletzungen



Wahrscheinlich haben Sie schon von massiven Datenschutzverletzungen bei Unternehmen gehört und sich gefragt: „Wie konnte das passieren?“ oder „Was wäre, wenn ich betroffen gewesen wäre?“ Eine Datenschutzverletzung kann beängstigend sein und auch schwerwiegende Folgen wie Zahlungskartenbetrug oder sogar Identitätsdiebstahl nach sich ziehen.

Im Folgenden erfahren Sie mehr darüber, wie sich Datenschutzverletzungen auf Sie auswirken können, wie sie entstehen und wie man sie verhindern kann.

## Was ist eine Datenschutzverletzung?

Eine Datenschutzverletzung ist ein Sicherheitsvorfall, bei dem private, vertrauliche oder sensible Daten von jemandem unbefugt offengelegt oder gestohlen werden. Die Gründe dafür sind vielfältig und reichen von menschlichem Versagen bis hin zu bösartigen Angriffen und die Folgen können verheerend sein. Jeder ist dem Risiko einer Datenschutzverletzung ausgesetzt, insbesondere wenn seine Konten nicht geschützt sind.

## Datenschutzverletzungen können zu Folgendem führen:

**Gestohlenen Anmeldeinformationen**
**Beispiel:** Hacker haben sich unbefugten Zugriff auf eine Datenbank mit den Benutzernamen und Passwörtern der Nutzer einer Social-Media-Plattform verschafft, was zu einer weitreichenden Übernahme von Konten und dem Missbrauch personenbezogener Daten geführt hat.

**Identitätsdiebstahl**
**Beispiel:** Ein Cyberkrimineller hat gestohlene personenbezogene Daten wie Sozialversicherungsnummern und Adressen verwendet, um in betrügerischer Absicht Darlehen und Kreditkarten im Namen der Opfer zu beantragen, was zu finanziellen Schäden und identitätsbezogenen Problemen geführt hat.

**Kompromittierten Vermögenswerten**
**Beispiel:** Malware hat das Netzwerk eines Unternehmens infiziert und Angreifern ermöglicht, die Kontrolle über kritische Systeme und sensible Daten zu übernehmen, was zu einer Unterbrechung des Betriebs und zu erheblichen finanziellen Verlusten geführt hat.

**Zugriff auf Konten durch Dritte**
**Beispiel:** Bei einem Anbieter von Cloud-Diensten ist es zu einer Datenschutzverletzung gekommen, die es unbefugten Dritten ermöglicht hat, auf sensible Dateien und Informationen seiner Kunden zuzugreifen, was zu potenziellen Datenlecks und Verletzungen der Privatsphäre geführt hat.

**Zahlungskartenbetrug**
**Beispiel:** Ein Cyberangriff auf das Zahlungsverarbeitungssystem eines Online-Händlers hat zum Diebstahl von Kreditkartendaten der Kunden geführt, die dann für nicht autorisierte Einkäufe verwendet wurden.

# Wie kommt es dazu?

Datenschutzverletzungen können in die Kategorie der Cyberkriminalität fallen, wenn sie böswillig erfolgen, aber sie können auch durch einen unbeabsichtigten Fehler einer Person mit autorisiertem Zugriff auf die Daten entstehen.

**Zu den Ursachen von Datenschutzverletzungen gehören:**

### Böswillige Zugehörige
Personen mit Zugriff auf die Datenbank missbrauchen ihre Zugriffsrechte absichtlich, um sensible Daten zu stehlen oder weiterzugeben.

### Böswillige Außenstehende
Ein Außenstehender des Unternehmens greift eine Datenbank durch Phishing, Malware, über Schwachstellen oder Denial-of-Service-Angriffe (DoS) an.

### Versehen seitens Zugehöriger
Personen mit Zugriffsberechtigung legen aufgrund von Fehlern oder mangelnden Sicherheitsmaßnahmen versehentlich Daten offen. Technisch gesehen handelt es sich zwar um ein Datenleck, da es sich um einen internen Fehler handelt, doch es hat für die Betroffenen dieselben Folgen und das Unternehmen muss möglicherweise auch mit rechtlichen Konsequenzen rechnen.

# Phasen einer Datenschutzverletzung

Im Gegensatz zu dem, was Sie sich vielleicht vorstellen, sieht eine böswillige Datenschutzverletzung weniger danach aus, dass sich jemand komplett in Schwarz gekleidet mit einem Flash-Laufwerk in ein Gebäude schleicht, sondern eher danach, dass Personen an einem entfernten Ort darüber nachdenken, wie sie sich in eine Datenbank hacken können.

Doch nicht jede Datenschutzverletzung erfolgt böswillig. Einige sind auf menschliches Versagen oder Fahrlässigkeit zurückzuführen, aber darauf gehen wir im nächsten Abschnitt näher ein.

**Im Folgenden werden die drei Phasen einer vorsätzlichen Datenschutzverletzung beschrieben.**

## 1. Recherche

Zu Beginn einer Datenschutzverletzung wählt ein Angreifer ein Ziel aus – in der Regel ein Unternehmen oder eine Organisation mit Zugriff auf persönliche Daten – und recherchiert, wie er in die Datenbank des Opfers eindringen kann.

Der Angreifer erfasst Details wie Mitarbeiterinformationen, Finanzdaten und Daten zu Sicherheitsbudgets. Er macht zudem Schwachstellen wie schwache Passwörter, veraltete Software oder ungeschützte Netzwerkverbindungen ausfindig.

## 2. Angriff

Der Angreifer kann nun mit den Erkenntnissen aus seiner Recherche das Datensystem angreifen. Im Folgenden werden einige gängige Methoden vorgestellt, mit denen sich Angreifer Zugriff auf Unternehmenssysteme oder -netzwerke verschaffen:

- **Gestohlene Anmeldeinformationen:**
  Sie können kompromittierte Benutzernamen und Passwörter über das Dark Web, Phishing, Brute-Force-Angriffe oder sogar physischen Diebstahl von Geräten erfassen, um sich als legitime Benutzer auszugeben und Zugriff auf Systeme zu erhalten.

- **Phishing-E-Mails**
  Angreifer verwenden auch personenbezogene Daten aus ihren Recherchen, z. B. Berufsbezeichnungen oder Namen von Kollegen, um ihre Opfer dazu zu bringen, Anmeldeinformationen anzugeben oder auf einen schädlichen Link zu klicken, über den Malware auf ihren Computer heruntergeladen wird.

- **Malware**
  Hacker verwenden bösartige Software, um heimlich den Computer oder das Netzwerk eines Opfers zu infizieren und die Kontrolle darüber zu übernehmen, um Daten zu stehlen.
- **Ausnutzung von Schwachstellen**
  Der Angreifer macht sich Schwachstellen wie schwache Passwörter, Fehlkonfigurationen oder nicht gepatchte Systeme im Computersystem eines Unternehmens zunutze, um sich Zugriff zu verschaffen.

- **Denial-of-Service-Angriffe (DoS)**
  Bei derartigen Angriffen wird eine Website mit übermäßigem gefälschten Datenverkehr überflutet, bis sie für tatsächliche Benutzer nicht mehr erreichbar ist. Sie lenken von anderen Sicherheitslücken ab, so dass Angreifer Datenschutzverletzungen durchführen können.

## 3. Daten extrahieren

Sobald sich die Angreifer Zugriff auf das System oder Netzwerk des Opfers verschafft haben, können sie wertvolle oder sensible Daten ausfindig machen und extrahieren, darunter personenbezogene Daten, Finanzdaten oder andere Daten, die sie im Dark Web verkaufen können.

Die extrahierten Daten werden dann auf die eigenen Server der Angreifer kopiert oder übertragen, wo sie die Kontrolle darüber haben und sie nutzen können. Oft weiß ein Unternehmen erst dann, dass seine Daten gestohlen wurden, wenn ein Dritter, z. B. Strafverfolgungsbehörden, Dienstanbieter oder Kunden, die Sicherheitsverletzung meldet.

# 04.
# Schutz Ihrer Person und Ihrer Daten

Es gibt einige einfache Möglichkeiten, um online sicher zu bleiben. Panda Dome bietet einen Schutzplan für jeden Lebensstil, damit Sie unbesorgt surfen können.

## Netzwerksicherheit

Die Netzwerksicherheit umfasst die Umsetzung von Maßnahmen zum Schutz von Computernetzwerken vor unbefugtem Zugriff, Cyberangriffen und Datenschutzverletzungen. Dazu gehören die Sicherung der Netzwerkinfrastruktur, die Überwachung des Datenverkehrs und die Implementierung robuster Verschlüsselungsprotokolle.

### Verwenden Sie öffentliche WLANs auf sichere Weise

Seien Sie vorsichtig, wenn Sie sich mit öffentlichen WLANs verbinden, um unbefugten Zugriff auf sensible Daten zu verhindern.

### Verwenden Sie ein VPN

Verbessern Sie den Online-Datenschutz und die Online-Sicherheit, indem Sie den Internetverkehr beim Zugriff auf öffentliche Netze verschlüsseln.

### Installieren Sie eine Firewall

Implementieren Sie eine Barriere gegen unbefugten Zugriff auf Ihr Netzwerk, um eine zusätzliche Sicherheitsstufe gegen Cyberbedrohungen zu schaffen.

## Authentifizierung und Zugriffskontrolle

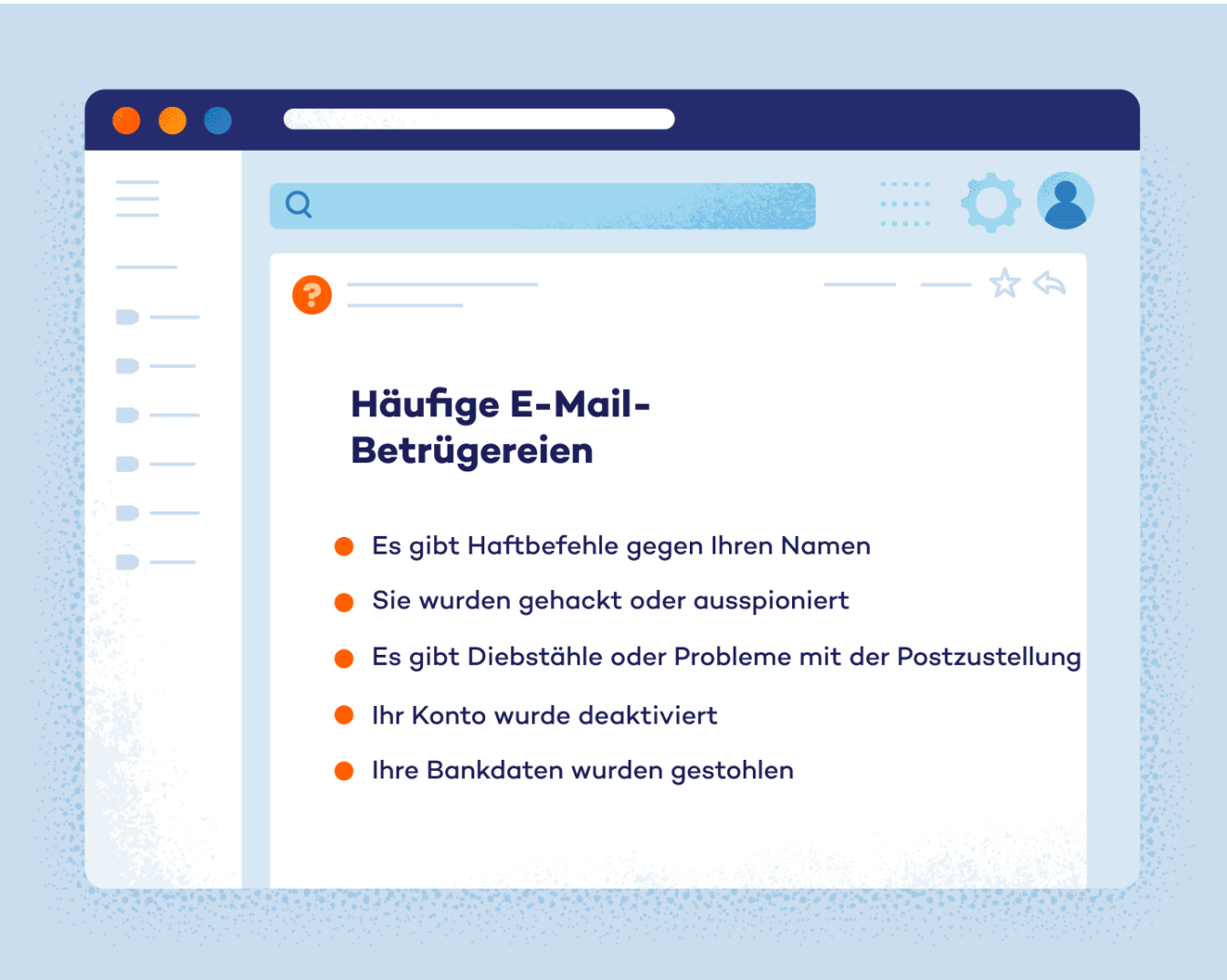
Authentifizierung und Zugriffskontrolle sind wesentliche Komponenten des Datenschutzes, die sicherstellen, dass nur autorisierte Personen oder Systeme auf sensible Daten oder Ressourcen zugreifen können. Durch diese Maßnahmen werden die Identität der Benutzer überprüft und Beschränkungen ihrer Aktionen innerhalb eines Netzwerks oder Systems durchgesetzt.

- **Wählen Sie sichere und einzigartige Passwörter**
  Erhöhen Sie die Kontosicherheit, indem Sie komplexe Passwörter erstellen, die für jedes Konto einzigartig sind, um das Risiko von unbefugtem Zugriff zu verringern.

- **Richten Sie eine Zwei-Faktor-Authentifizierung ein**
  Fügen Sie eine zusätzliche Sicherheitsstufe hinzu, indem Sie neben dem Passwort eine zweite Form der Authentifizierung verlangen, z. B. einen Code, der an ein vertrauenswürdiges Gerät gesendet wird.

- **Überwachen Sie Kontoinformationen**
  Überprüfen Sie regelmäßig die Kontoaktivitäten, um verdächtiges Verhalten oder unbefugte Zugriffsversuche zu erkennen. Melden Sie verdächtige Aktivitäten oder unbefugte Zugriffsversuche unverzüglich den zuständigen Behörden oder Dienstanbietern.

- **Geben Sie niemals Codes weiter, die Sie per SMS oder E-Mail erhalten haben**
  Vermeiden Sie die Weitergabe von Verifizierungscodes, die Sie per SMS oder E-Mail erhalten haben, da diese von Angreifern abgefangen werden könnten, die versuchen, sich unbefugt Zugriff zu verschaffen.




## Datenschutz und -wiederherstellung

Datenschutz und -wiederherstellung beziehen sich auf die Strategien und Technologien, die zum Schutz und zur Wiederherstellung von Daten im Falle von versehentlicher Löschung, Beschädigung oder Cyberangriffen eingesetzt werden. Dazu gehört die Implementierung von Datensicherungslösungen, Verschlüsselung und Disaster-Recovery-Plänen, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.

### Sichern Sie Ihre Daten

Schützen Sie sich vor Datenverlusten durch Cyberangriffe oder Hardwareausfälle, indem Sie regelmäßig Sicherungskopien wichtiger Dateien und Dokumente erstellen.

### Installieren Sie eine Virenschutz-Software

Schützen Sie sich vor Malware und anderen Cyberbedrohungen, indem Sie eine seriöse Virenschutz-Software installieren, die bösartige Software erkennt und von Ihren Geräten entfernt. malicious software from your devices.

## Allgemeines Wissen zur Cybersicherheit

Es ist wichtig, gängige Anzeichen für Hackerangriffe zu kennen, damit Sie so schnell wie möglich Maßnahmen ergreifen und Ihre Konten wiederherstellen können.

**Hier sind einige Warnzeichen, die darauf hinweisen, dass Sie Opfer eines Hackerangriffs geworden sein könnten:**

- Die Internetnutzung eines Geräts steigt erheblich an
- Die Betriebsgeschwindigkeit eines Geräts verlangsamt sich
- Der Akku entlädt sich schnell und ohne Erklärung
- Sie erhalten unbefugte Aufforderungen, Passwörter zu ändern
- Neue Software oder Anwendungen werden automatisch heruntergeladen

# 05.
# Häufig gestellte Fragen zum Datenschutz

In diesem Abschnitt beantworten wir einige häufig gestellte Fragen zum Datenschutz

## Was ist der Zweck eines Datenschutzgesetzes?

Zweck eines Datenschutzgesetzes ist es, die personenbezogenen Daten von Personen zu schützen, indem es die Erhebung, Verarbeitung und Speicherung dieser Daten regelt und so Transparenz und Datenschutz fördert.

## Was sind die 4 Arten des Datenschutzes?

**Die vier Arten des Datenschutzes entsprechen verschiedenen Zugriffs- und Sensibilitätsstufen:**

### Schutz öffentlicher Daten

Bezieht sich auf Informationen, die für die Öffentlichkeit bestimmt sind, z. B. allgemeine Kontaktinformationen eines Unternehmens, und erfordert im Allgemeinen keinen hohen Datenschutz.

### Schutz von Daten nur für interne Zwecke

Bezieht sich auf Daten, die nur innerhalb eines Unternehmens zugänglich sind, und erfordert in der Regel Sicherheitsvorkehrungen, um einen unbefugten Zugriff durch Außenstehende zu verhindern.

### Schutz vertraulicher Daten

Bezieht sich auf sensible Informationen, die verstärkte Datenschutzmaßnahmen erfordern, um den Zugriff auf autorisierte Personen innerhalb eines Unternehmens zu beschränken.

### Schutz geheimer Daten

Bezieht sich auf hochsensible Daten, die strengen Datenschutzkontrollen unterliegen und oft besondere Zugriffs- und Bearbeitungsberechtigungen erfordern, um das Risiko einer unbefugten Offenlegung oder eines Missbrauchs zu minimieren.

## Was versteht man unter personenbezogenen Daten?

Personenbezogene Daten, auch bekannt als Angaben zur Identität umfassen alle Daten, anhand derer eine Person persönlich identifiziert werden kann. Dazu gehören grundlegende Identitätsangaben wie Name und Geburtsdatum, Kontaktinformationen wie E-Mail-Adressen und Telefonnummern, Finanzdaten wie Kreditkartennummern und sensible Informationen wie Daten aus Patientenakten.