Jeder Zehnte wurde 2025 Opfer einer Internetstraftat.

Sind Sie ausreichend geschützt?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Anfang 2026 zum achten Mal seinen Cybersicherheitsmonitor veröffentlicht. Für die Studie wurden über 3.000 Internetnutzerinnen und -nutzer in Deutschland befragt - Menschen wie Sie und Ihre Familie. Die Ergebnisse sind ein Weckruf: Cyberkriminalität ist längst keine abstrakte Bedrohung mehr, sondern alltägliche Realität.
Dieser Ratgeber fasst die wichtigsten Erkenntnisse zusammen und zeigt Ihnen, was Sie konkret tun können, um sich zu schützen. Der Bericht berücksichtig ausschließlich private IT- und Cyber-Struktuturen.

Das Wichtigste auf einen Blick

- 11 % der Befragten wurden 2025 Opfer einer Straftat im Internet - 2024 waren es noch 7 %.
- 27 % der Deutschen haben schon mindestens einmal Cyberkriminalität erlebt.
- 88 % der Betroffenen erlitten einen echten Schaden - finanziell, zeitlich oder emotional.
- Nur 14 % informieren sich regelmäßig über IT-Sicherheit.
- Im Schnitt werden nur 3,9 von 19 empfohlenen Schutzmaßnahmen genutzt

Was passiert genau - und könnte es auch Sie treffen?

Die häufigsten Straftaten, von denen Betroffene berichten, klingen vermutlich vertraut:

- **Betrug beim Onlineshopping (22 %):** Sie bestellen, bezahlen - und die Ware kommt nie an. Oder der Shop war von Anfang an gefälscht.
- **Fremdzugriff auf einen Account (14 %):** Jemand anderes loggt sich in Ihr E-Mail-Konto, Ihren Amazon-Account oder Ihre Social-Media-Profile ein.
- **Betrug beim Onlinebanking (13 %):** Manipulierte Überweisungen oder Missbrauch von Kontodaten.
- **Phishing (12 %):** Gefälschte E-Mails oder Nachrichten, die Sie zur Eingabe von Passwörtern oder Bankdaten verführen sollen.
- **Schadsoftware und Viren (7 %):** Programme, die sich unbemerkt auf Ihrem Gerät einnisten und Daten stehlen oder Ihr System schädigen.
- **Ransomware / Erpressersoftware (2 %):** Ihre Daten werden verschlüsselt, und Sie sollen Lösegeld zahlen, um sie wiederzubekommen.

Wichtig zu wissen: Diese Zahlen beziehen sich auf Privatpersonen - also auf Menschen, die zu Hause surfen, online einkaufen oder ihr Smartphone nutzen. Sie müssen kein Unternehmen sein, um ins Visier von Kriminellen zu geraten. Unternehmen wiederum müssen diesen Aspekt im Kontext Home-Office und Schatten-IT berücksichtigen aber das ist nochmal ein ganz eigenes Thema

Welche Schäden entstehen wirklich?

Viele unterschätzen, was nach einem solchen Vorfall auf sie zukommen kann. Der BSI-Report zeigt: Wer betroffen ist, bleibt selten ohne Folgen.

- **Finanzieller Schaden (33 %):** Geld weg, Rückbuchung schwierig oder unmöglich.
- **Vertrauensverlust (29 %):** Viele Betroffene trauen Onlinediensten danach nicht mehr - und schränken ihre digitale Teilhabe dauerhaft ein.

- **Zeitaufwand (23 %):** Passwörter ändern, Behörden kontaktieren, Bankkonten sperren - das kostet Stunden, manchmal Tage.
- **Emotionaler Schaden (20 %):** Angst, Stress, das Gefühl, ausgeliefert zu sein - das wird häufig unterschätzt.
- **Datenverlust (18 %):** Fotos, Dokumente, Kontakte - weg.

Nur 12 % der Betroffenen gaben an, keinen nennenswerten Schaden erlitten zu haben. Das bedeutet im Umkehrschluss: Bei fast 9 von 10 Fällen passiert etwas, das den Alltag **spürbar** belastet.

Warum schützen sich so wenige Menschen ausreichend?

Der Report zeigt eine ernüchternde Lücke: Den Befragten sind im Schnitt nur 6,2 der 19 empfohlenen Schutzmaßnahmen bekannt - und genutzt werden davon im Durchschnitt lediglich 3,9. Befragt nach dem Grund, antworten die meisten ehrlich:

- 27 % sagen: "Ich fühle mich eigentlich sicher."
- 23 % finden es zu kompliziert.
- 23 % fühlen sich überfordert.
- 20 % wissen nicht, was sie tun sollen, weil überall etwas anderes empfohlen wird.

Das subjektive Sicherheitsgefühl ist dabei besonders trügerisch: Mehr als die Hälfte der Befragten (55 %) hält ihr persönliches Risiko für gering oder ausgeschlossen - gleichzeitig steigt die Zahl der Betroffenen weiter. Sicherheit entsteht nicht durch das Gefühl, nichts zu haben, was Kriminelle interessiert. Sie entsteht durch konkrete Maßnahmen.

Was Sie jetzt konkret tun können
Die gute Nachricht: Die wirksamsten Schutzmaßnahmen sind weder teuer noch kompliziert. Die folgende Checkliste orientiert sich an den Empfehlungen des BSI:

Ihre persönliche Sicherheits-Checkliste

- ✓ Starke, einzigartige Passwörter: Verwenden Sie für jeden Dienst ein anderes Passwort. Ein Passwort-Manager hilft, den Überblick zu behalten.
- ✓ Zwei-Faktor-Authentisierung (2FA) aktivieren: Wo immer möglich - besonders bei E-Mail, Banking und Social Media. Selbst wenn Ihr Passwort gestohlen wird, kommt der Angreifer ohne den zweiten Faktor nicht rein.
- ✓ Updates immer zeitnah installieren: Sicherheitslücken in Betriebssystemen und Apps werden regelmäßig geschlossen - aber nur, wenn Sie die Updates auch einspielen. Aktivieren Sie automatische Updates.
- ✓ Antivirenprogramm und Firewall nutzen: Ein aktuelles Antivirenprogramm erkennt die meisten Schadsoftware-Varianten, bevor sie Schaden anrichten. Verlassen sie sich keinesfalls auf Windows Bordmittel wie den Defender o.ä.
- ✓ Regelmäßige Datensicherungen anlegen: Sichern Sie Fotos, Dokumente und wichtige Daten regelmäßig auf einer externen Festplatte oder einem Cloud-Dienst. Ransomware kann so kaum noch erpressen.
- ✓ Vorsicht bei E-Mails und Links: Klicken Sie nie auf Links in unerwarteten E-Mails, auch nicht, wenn der Absender vertraut wirkt. Banken, Paketdienste und Behörden fragen niemals per E-Mail nach Ihren Zugangsdaten.

Öffentliche WLAN-Netze meiden oder absichern: In Cafes, Bahnhöfen oder Hotels sind öffentliche Netzwerke ein Einfallstor. Nutzen Sie für sensible Vorgänge (Banking, E-Mail) lieber das Mobilfunknetz oder ein VPN.

Was tun, wenn es doch passiert?

Trotz aller Vorsicht kann es Sie treffen. Dann zahlt sich Besonnenheit aus. Laut BSI-Report reagieren Betroffene am häufigsten so - und das sind auch die richtigen Schritte:

- **Sofort handeln:** Ändern Sie alle betroffenen Passwörter - und alle anderen Konten, bei denen Sie dasselbe Passwort verwendet haben.
- **Den Dienstanbieter kontaktieren (35 % tun das):** Informieren Sie die Plattform, auf der der Betrug stattgefunden hat. Das hilft nicht nur Ihnen, sondern schützt auch andere.
- **Anzeige erstatten (32 % tun das):** Viele scheuen den Gang zur Polizei - dabei ist eine Anzeige oft die Voraussetzung, um Geld zurückzubekommen oder Fake-Shops löschen zu lassen. Sie können Anzeige auch online erstatten (Onlinewachen der Landespolizeien).
- **Bank sofort informieren:** Bei Betrug mit Kontodaten oder beim Onlinebanking zählt jede Minute. Manche Banken können Transaktionen noch stoppen, wenn Sie schnell reagieren.

Wichtig: Identitätsdiebstahl bleibt oft lange unbemerkt

Täterinnen und Täter bestellen unter Ihrem Namen Waren, schließen Verträge ab oder verkaufen illegale Produkte - manchmal erfahren Opfer davon erst, wenn eine Mahnung oder sogar eine Strafverfolgung ins Haus flattert. Regelmäßige Kontokontrollen, Kreditauskünfte und ein wachsames Auge auf unbekannte E-Mails können frühzeitig Alarm schlagen.

Gut informiert ist halb geschützt

Der BSI-Cybersicherheitsmonitor 2026 macht eines deutlich: Das Risiko steigt, aber die Bereitschaft, sich aktiv zu schützen, hält nicht Schritt. Der häufigste Grund dafür ist nicht Gleichgültigkeit - sondern das Gefühl, nicht zu wissen, wo man anfangen soll.
Fangen Sie mit der Checkliste in diesem Artikel an. Schon drei oder vier konsequent umgesetzte Maßnahmen reduzieren Ihr persönliches Risiko erheblich. IT-Sicherheit muss weder teuer noch zeitaufwändig sein - sie muss vor allem konsequent sein.

Link zum Report https://www.hmcplus.de/wp-content/uploads/CyMon-ProPK-BSI_2026_Kurzbericht.pdf

Hinweis: Wie oben bereits erwähnt bezieht sich die Studie des BSI weitgehend mit der Cybersicherheit für Verbraucherinnen und Verbraucher. Für Unternehmen stellen sich gänzlich andere Anforderungen und die Ergebnisse der Studie sind nur mittelbar relevant. Bei unserer Zusammenfassung haben wir Aspekte die ursächlich eher im Bereich Social-Engineering angesiedelt sind (bspw. Love Scam) unberücksichtigt gelassen.
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) - Cybersicherheitsmonitor (CyMon) 2026, Kurzbericht, Stand April 2026. Erhebung durch essentiq GmbH, Januar 2026, n = 3.060.
Zusammengefasst von HMC Systemhaus OHG, www.hmcplus.de