



*Online,
aber sicher!*

Zentrale Tipps für Ihre Sicherheit

Inhalt

1. Empfehlenswerte Webseiten.....	3
2. Tipps zur System-Sicherheit.....	4
3. Sichere Passwörter	5
4. Risiken im E-Mail-Postfach.....	6
5. Online-Banking	7
6. Riskante Kontaktaufnahmen	8
7. Einkaufen im Internet.....	8
8. Was tun, wenn... ..	10

Willkommen im Internet!

Egal ob Neuling oder „alter Hase“ – das Internet ist eine eigene Welt, die wir uns immer wieder neu erschließen müssen. Neben den unzähligen positiven Möglichkeiten, mit denen uns die Dienste des Internets das Leben erleichtern, begegnen uns in der Online-Welt aber unweigerlich Risiken und Gefahren, für die wir mit dieser Broschüre sensibilisieren wollen.

Das Internet bietet eben leider auch für Kriminelle ein erhebliches „Potential“ – abgesehen haben die es hier in erster Linie auf Daten, bspw. persönliche Zugangsdaten, aber auch auf Geld und Vermögen. Deshalb an dieser Stelle schon folgende grundlegende Tipps:

- 1 **Erst denken, dann klicken!**
- 2 **Lassen Sie sich nicht unter Druck setzen oder zu (vor-) schnellen Entscheidungen verleiten.**
- 3 **Holen Sie sich im Zweifel Rat bei Menschen, denen Sie vertrauen.**
- 4 **Gehen Sie sorgsam mit Ihren Daten um.**

Es würde den Rahmen dieser Broschüre bei Weitem sprengen, sämtliche Risiken im Zusammenhang mit der Nutzung des Internets anzusprechen – insofern beschränken wir uns auf die aus unserer (polizeilichen) Sicht wesentlichen.

Im Übrigen empfehlen wir, die an den Kapiteln platzierten Verweise auf Webseiten für weitere Informationen zum jeweiligen Thema zu nutzen.

Denn: Informiertes Verhalten reduziert das eigene Risiko erheblich!

1. Empfehlenswerte Webseiten

Unter den rund 1 Milliarde Webseiten, aus denen sich das Internet zusammensetzt, gibt es sehr viele empfehlenswerte. Um sich ausführlich über Ihre Sicherheit zu informieren, sollten Sie die nachfolgend genannten Seiten aber unbedingt besuchen:

▶ www.bsi.bund.de

Bei Fragen rund um das Thema „Sicherheit im Internet“ ist die Seite des Bundesamts für Sicherheit in der Informationstechnik die richtige Adresse: *Themen ▶ Verbraucherinnen und Verbraucher*

▶ www.polizei-beratung.de

Auf dieser gemeinschaftlich von den Polizeibehörden der Länder und des Bundes getragenen Webseite finden Sie Informationen zu den wichtigsten Kriminalitätsphänomenen – und wie Sie sich vor Kriminalität schützen.

Wir empfehlen: Abonnieren Sie den Bürger-Newsletter unter: <https://www.polizei-beratung.de/newsletter/>

▶ www.polizei.hamburg

Die zentrale Seite der Polizei Hamburg. Über www.polizei.hamburg/services/onlinewache-der-polizei-hamburg können Sie Strafanzeige erstatten und der Polizei Hinweise geben.

▶ www.verbraucherzentrale.de

Die zentrale Webseite des Verbraucherzentrale Bundesverband e.V. mit unabhängigen Informationen zu den wichtigsten Verbraucherthemen.

2. Tipps zur System-Sicherheit

▶ www.bsi.bund.de | **Stichwort: Basistipps zur IT-Sicherheit**

Bevor Sie mit Ihrem PC, Tablet oder Smartphone ins Internet gehen, sollten Sie sich mit der Frage der grundlegenden technischen Sicherheit beschäftigen. Wir raten Ihnen:

HALTEN SIE IHR SYSTEM AKTUELL

Software- und Hardware-Hersteller veröffentlichen regelmäßig Aktualisierungen, hier im Weiteren auch Updates genannt, mit denen u.a. kritische Sicherheitslücken des jeweiligen Systems geschlossen werden. Solche Updates sollten immer zügig installiert werden.

Im Normalfall erfolgt die Installation in einem automatisierten Prozess – im Einzelfall kann es aber erforderlich sein, dass Sie die Installation z.B. durch Eingabe Ihres Administrator-Passworts zulassen. In diesem Fall sollten Sie unbedingt darauf achten, dass die Aufforderung zur System-

Aktualisierung tatsächlich vom Hersteller des jeweiligen Produkts stammt. Dies wird im Normalfall in dem Fenster, das sich zur Bestätigung eines Updates öffnet, angezeigt.

GEHEN SIE NICHT MIT ADMINISTRATOR-RECHTEN ONLINE

Risiko: Im Falle eines Angriffs auf Ihren Rechner verfügt der Angreifer über die Möglichkeit, Software zu installieren bzw. auszuführen, wodurch Sie im schlimmsten Fall vom Zugriff auf Ihr eigenes Gerät ausgeschlossen werden.

Diese Problematik stellt sich in erster Linie bei Windows-basierten Endgeräten, da hier – anders als bei Geräten mit Android- bzw. iOS-Betriebssystem – für den ersten Nutzer standardmäßig ein Konto mit Administrator-Rechten angelegt wird.

Wir empfehlen, auf Geräten mit einem Windows-Betriebssystem – neben dem primär angelegten Nutzerkonto – immer ein Konto mit eingeschränkten Rechten (in Windows als „Standardnutzer“ bezeichnet) einzurichten und nur mit diesem Konto online zu gehen.

NUTZEN SIE EINE ANTI-VIREN-SOFTWARE

Grundsätzlich liefern die gängigen Betriebssysteme einen Basisschutz gegen Schadsoftware. Wir empfehlen jedoch, diesen Schutz durch Installation einer speziellen Anti-Viren-Software zu verstärken. Vor allem in diesem Bereich lohnt sich die Investition in ein kostenpflichtiges Produkt, mit dem Sie Ihr System umfassend vor Online-Risiken schützen können.

Achten Sie darauf, dass Sie Ihr Anti-Viren-Produkt entweder direkt beim Hersteller oder bei einem seriösen Anbieter kaufen. Und wie immer gilt: Die Software muss dauerhaft aktuell gehalten werden!

3. Starke Passwörter

► www.bsi.bund.de | **Stichwort: Passwörter**

Für die Nutzung vieler Angebote im Internet ist die Einrichtung eines personalisierten Kontos erforderlich. Hierfür wird in der Regel eine E-Mail-Adresse und ein selbst gewähltes Passwort benötigt.

Grundsätzlich gilt: Je länger, desto besser. Für ein gutes Passwort sind Länge und Komplexität entscheidend. Starke Passwörter bestehen aus **mindestens 8-stelligen Kombination von Buchstaben, Zahlen und**

Sonderzeichen. Ein weniger komplexes Passwort sollte mindestens **25 Zeichen** lang sein.

Verwenden Sie für **jedes Nutzerkonto ein anderes Passwort**. Denn wenn ein Konto gehackt wird, haben Angreifer Zugriff auf alle anderen Konten, für die Sie dasselbe Passwort verwenden.

Passwort-Manager helfen, individuelle und starke Passwörter für alle On-linekonten zu erstellen und an einem Ort zu speichern. Merken müssen Sie sich dann nur das sog. Masterpasswort, um Zugriff auf alle anderen im Passwort-Manager gespeicherten Zugangsdaten zu bekommen.

Die **2-Faktor-Authentisierung** (2FA) bietet zusätzliche Sicherheit, indem neben dem Passwort ein zweiter Bestätigungsweg, oft über ein zweites Gerät, gefordert wird. Dadurch wird es Hackern deutlich erschwert, auf Ihre Konten zuzugreifen.

Anstatt eines Passworts werden bei einer Anmeldung über einen sog. **Passkey** biometrische Daten wie Fingerabdrücke oder Gesichtserkennung genutzt. Wenn Ihnen also von einem vertrauten Diensteanbieter vorgeschlagen wird, Passkey einzurichten, können Sie die Technologie ohne weiteres verwenden und Ihr Passwort ersetzen.

4. Risiken im E-Mail-Postfach

► www.bsi.bund.de | **Stichwort: E-Mail**

Mit einer eigenen E-Mail-Adresse sind Sie in der Lage, über das Internet mit anderen Personen oder Organisationen (Unternehmen, Behörden) schriftlich zu kommunizieren. E-Mail-Adressen werden sehr häufig auch für die Einrichtung persönlicher Konten bei Anbietern im Internet benötigt.

Dabei ist zu bedenken:

- E-Mails werden im Normalfall unverschlüsselt im Internet übertragen. Die Sicherheit einer E-Mail ist vergleichbar mit einer Postkarte, die – jedenfalls theoretisch – von jemandem mit Zugang zum Übertragungsweg mitgelesen oder verändert werden kann.
- E-Mail-Adressen sind ein lukratives Handelsgut und werden massenhaft für die Bewerbung mehr oder weniger seriöser Angebote angeschrieben (man spricht dabei von „Spam“ oder „Junk“).

Aus diesem Grund empfehlen wir die **Einrichtung von wenigstens zwei E-Mail-Adressen**: eine für Ihre „seriöse“ Kommunikation, die ggf. auch Rückschlüsse auf Ihre Person zulässt und die Sie nicht für andere Zwecke nutzen sollten und eine zweite, die möglichst keinen Rückschluss auf Ihre Person zulässt, für alle anderen Zwecke (wie z.B. Konten bei Online-Shops).

- Von Betrügern werden E-Mails auch genutzt, um Sie als Empfänger mit den unterschiedlichsten Vorwänden auf Links zu locken, zum Antworten oder zum Öffnen von Dateianhängen zu bringen. So wird die Lieferung eines Pakets angekündigt, ein Gewinn in Aussicht gestellt oder behauptet, es gebe ein Problem mit Ihrem Online-Banking. Deshalb gilt: **Bei E-Mails von Ihnen unbekanntem Absendern sollten Sie weder Links anklicken noch angehängte Dateien öffnen oder auf solche Mails antworten!**

5. Online-Banking

► www.bsi.bund.de | **Stichwort: Onlinebanking**

Zwei Drittel der Deutschen nutzen das Internet auch für Bankgeschäfte – das ist praktisch, weil es in der Regel den Gang zu einer Filiale überflüssig macht und eine regelhafte Kontrolle der Kontobewegungen erleichtert. Solange Sie die zentralen Sicherheits-Tipps beherzigen, ist Online-Banking deshalb durchaus empfehlenswert.

ZENTRALE TIPPS:

- Lassen Sie sich von Ihrer Bank zum Online-Banking beraten. Fragen Sie auch danach, unter welcher Telefonnummer Ihnen bei der Einrichtung oder bei der Nutzung des Online-Bankings geholfen werden kann.
- Bewahren Sie Zugangsdaten an einem sicheren Ort auf.
- Ihre Bank wird Sie niemals per E-Mail oder auf anderem Weg zur Mitteilung von Zugangsdaten zum Online-Banking auffordern – solche E-Mails oder Nachrichten sollten Sie ignorieren und umgehend löschen.

6. Riskante Kontaktaufnahmen

► www.polizei-beratung.de | **Stichwort: Gefahren im Internet**

Die Dienste des Internets sind zu einem Großteil dafür gemacht, mit anderen Menschen in Kontakt zu kommen, sich in Echtzeit mit ihnen auszutauschen und digitale Inhalte (z.B. Fotos) zu teilen. Eine wirklich tolle Möglichkeit, am Leben Ihrer entfernt wohnenden Verwandten oder Freunde teilzuhaben.

Doch wie immer gilt: wo viel Licht, da auch viel Schatten. Und gerade ältere oder alleinstehende Menschen werden über die Kommunikationsmöglichkeiten des Internets von Betrügern ins Visier genommen.

Eine der wichtigsten Regeln im Internet lautet deshalb:

SEIEN SIE MISSTRAUISCH!

und dies vor allem, wenn Sie von Ihnen unbekanntem Personen – sei es per E-Mail oder über einen anderen Kanal – kontaktiert werden.

Sofern sich Kontaktaufnahmen nicht auf anderem Weg (bspw. durch einen Anruf bei dem angeblichen Bekannten unter der altbekannten Telefonnummer) als seriös bestätigen, ignorieren Sie Kontaktaufnahmen konsequent, reagieren Sie nicht auf E-Mails, sondern löschen Sie diese sofort.

7. Einkaufen im Internet

► www.verbraucherzentrale.de | **Stichwort: Onlinehandel**

Das Internet eignet sich hervorragend, um sich einen Überblick über bestimmte Warenangebote zu verschaffen, Preise zu vergleichen und Einkäufe zu tätigen. Wohl kaum ein Unternehmen, das Waren oder Dienstleistungen anbietet, kommt heute noch ohne den „Absatzkanal“ Internet aus.

Doch auch hier gilt es, sich bestimmte Risiken bewusst zu machen:

Bei Angeboten, die sich durch einen extrem günstigen Preis von anderen abheben, ist in jedem Fall Vorsicht geboten!

Vor allem mit besonders beliebten und hochpreisigen Waren versuchen Betrüger, potentielle Käufer in die Falle zu locken. Die „Falle“ besteht in der Regel darin, dass die Verkäufer zunächst die Zahlung verlangen (Vorkasse) – und anschließend die Ware nicht liefern.

PRÜFEN SIE ANGEBOTE SORGFÄLTIG

Anbieter und Angebote im Internet sollten Sie vor dem Kauf unter folgenden Aspekten prüfen:

Seriosität: Besonders günstige Angebote können unseriös sein. Zum Teil erstellen Betrüger eigens Webseiten, auf denen Käufer in die Falle gelockt werden sollen (sog. *Fakeshops*). Der Verbraucherzentrale Bundesverband bietet ein Werkzeug, mit dem Sie die Seriosität von Online-Shops selbst prüfen können: <https://www.verbraucherzentrale.de/fakeshopfinder>

Qualität: Auch auf grundsätzlich seriösen Plattformen finden sich immer wieder Angebote von zweifelhafter Qualität. Zum Teil helfen hier auch die zu den Produkten erstellten Bewertungen anderer Käufer nicht weiter, da nicht immer klar ist, ob es sich um echte oder gekaufte Bewertungen handelt. Sofern sich Zweifel an der Qualität nicht ausräumen lassen, sollten Sie vom Kauf Abstand nehmen oder auf das Produkt eines anerkannten Markenherstellers ausweichen.

Herkunft: Vor allem auf international tätigen Plattformen (wie Amazon oder eBay) werden Artikel angeboten, die aus Nicht-EU-Ländern an Sie versandt werden. Sofern diese Waren nicht verzollt wurden, sind Sie als Käufer verpflichtet, diese Zollanmeldung nachzuholen. Geschieht dies nicht, droht – neben einer Nachentrichtung der Einfuhrumsatzsteuer – ein Bußgeld- bzw. Strafverfahren.

NUTZEN SIE SICHERE ZAHLUNGSARTEN

Tätigen Sie Online-Käufe ausschließlich über „sichere“ Zahlungswege.

Überweisung: Wenn der Kauf auf Rechnung erfolgt, Sie also erst nach Erhalt der Ware zahlen, haben Sie Gelegenheit, die Qualität der Ware zu prüfen und ggf. bestehende Einwände gegenüber dem Verkäufer geltend zu machen.

Für Sie als Käufer riskant ist demgegenüber eine Überweisung vor Erhalt der Ware. Denn sollte die Ware nicht geliefert werden, ist das überwiesene Geld im Normalfall verloren.

Lastschriftinzug: Auch der Lastschriftinzug ist grundsätzlich eine sichere Zahlungsmethode, da Sie – anders als bei einer Überweisung – die Möglichkeit haben, dem Einzug innerhalb einer gewissen Frist zu widersprechen, also das Geld zurückbuchen zu lassen.

Nachnahme: Die Zahlung an den Paketzusteller kann im Prinzip auch als sicher bewertet werden. Allerdings händigt der Zusteller das Paket erst nach Zahlung aus. Sollte das gelieferte Paket keine oder nicht die bestellte Ware enthalten, ist ein Zurückholen des Geldes problematisch.

Zahlungsdienstleister: Die Zahlung über einen der etablierten Online-Bezahldienste (wie PayPal, Klarna, AmazonPay, Giropay, GooglePay, ApplePay) kann grundsätzlich als sichere Bezahlmethode bewertet werden. Bevor Sie die Dienste eines Online-Bezahldienstes in Anspruch nehmen, sollten Sie sich jedoch unbedingt mit dessen Geschäftsbedingungen (AGB) vertraut machen.

Kreditkarte: Bei Zahlung per Kreditkarte werden Sie im Normalfall zur Eingabe der Kreditkartennummer, des Gültigkeitsdatums der Karte sowie der Kartenprüfnummer aufgefordert. Diese Bezahlmethode sollten Sie ausschließlich bei seriösen Shops nutzen. Denn jeder, der diese Daten kennt, kann hiermit auf Ihren Namen (und auf Ihre Kosten) einkaufen.

8. Was tun, wenn...

► www.polizei.hamburg

Sollten Sie trotz aller Vorsicht Opfer geworden sein, **erstatten Sie Strafanzeige** bei der Polizei. Dies ist bei der Polizei Hamburg jederzeit auch online möglich über: www.polizei.hamburg/services/onlinewache-der-polizei-hamburg

Sofern Sie **Opfer eines Betrugs** beim Online-Shopping geworden sind, nehmen Sie umgehend Kontakt mit Ihrer Bank oder dem Zahlungsdienstleister auf, um evtl. noch Zahlungen rückgängig machen zu können.

Für Beweis Zwecke sollten Sie außerdem unbedingt die **Korrespondenz** mit dem „Verkäufer“ **aufbewahren**.

Unterstützungsangebote

Bundesamt für Sicherheit in der Informationstechnik



Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI unterstützt Sie dabei, Ihre Computer, Smartphones und Onlinekonten sicher zu nutzen. Bei Verständnisfragen oder aktuellen Ereignissen rund um das Thema IT-Sicherheit gibt es einen Newsletter oder es wird Ihnen hier weitergeholfen:

Erreichbarkeit: **Montag bis Freitag von 8-18 Uhr**

Telefon: **0800 274 1000**

E-Mail: service-center@bsi.bund.de

Webseite: <https://www.bsi.bund.de/>

SiBa – Das Sicherheitsbarometer
Die kostenfreie App für digitalen Selbstschutz!

Mit der SiBa-App sind Sie immer über aktuelle Bedrohungen im Netz informiert und wissen, wie Sie sich davor schützen können.

www.sicher-im-netz.de/sicherheitsbarometer

QR Code:

Laden im App Store

GET IT ON Google Play

Ein Angebot von **Deutschland sicher im Netz**

Digital dabei Hamburg



Das Projekt „Digital dabei Hamburg“ unterstützt Sie, digitale Geräte und das Internet sicher zu nutzen. Es bietet kostenlose Digitalschulungen an, die von ehrenamtlichen Digitalmentor*innen durchgeführt werden. Interessierte können sich für weitere Informationen oder eine Anmeldung hierhin wenden:

Telefon: **040 5581 4931**

E-Mail: digitalmentoren@albertinen.de

Webseite: <https://hamburg-digital-dabei.de/>

Impressum:

Landeskriminalamt Hamburg
Polizeiliche Kriminalprävention
Postfach 60 02 80 | 22202 Hamburg
Tel.: 040 4286-70707
kriminalpraevention@polizei.hamburg.de
<https://www.polizei.hamburg>

Stand: 04.2025

Titelbild: buqancreative/AdobeStock.de