

Cybersecurity im Alltag

Typische Online-Gefahren verstehen und die wichtigsten Schutzmaßnahmen kennen — für Links, Phishing, Passwörter, 2FA, DNS, öffentliche WLANs und Notfälle.

THEMEN IM ÜBERBLICK

Links & Domains prüfen

Phishing erkennen

Passwörter & 2FA

DNS-Schutzfilter

Updates & Backups

Öffentliche WLANs & VPN

Erpressung & falscher Support

Notfallplan

Die Broschüre lässt sich von vorne nach hinten lesen oder kapitelweise nachschlagen. Kapitel 19 ist ein Spickzettel zum Heraustrennen.

01	Die wichtigsten Regeln auf einen Blick	3
02	Webadressen richtig prüfen	4
03	Tarnung durch ähnliche Zeichen	5
04	Phishing erkennen	6
05	Konto absichern: vom Minimum zum starken Schutz	7
06	Passwörter ohne Kopfschmerzen	8
07	Passwortmanager richtig nutzen	9
08	2FA, Passkeys und Hardwarekeys	10
09	Abmelden nicht vergessen — auch mit 2FA	11
10	DNS verstehen: das Telefonbuch des Internets	12
11	DNS-Anbieter im Vergleich	13
12	Schutz-DNS: Quad9 und DNS4EU	14
13	DNS einrichten: einfache Wege	15
14	Geräte, Updates, WLAN und Backups	16
15	Öffentliche WLANs und unterwegs	17
16	Erpressung, Schockanrufe und falscher Support	18
17	Wenn doch etwas passiert	19
18	Karten und Zugänge sperren	20
19	Spickzettel zum Ausdrucken	21
20	Erste Hilfe bei verdächtigen Nachrichten	22
21	Quellen und weiterführende Hinweise	23
22	Impressum und Weitergabe	24



Wie aktuell ist das hier?

Menüpfade, DNS-Adressen und Anbieterfunktionen ändern sich. Alle Angaben wurden zum genannten Stand geprüft. Vor der Einrichtung immer die offizielle Anbieterseite gegenlesen.

Die wichtigsten Regeln auf einen Blick

Stop vor dem Klick

Bei E-Mail, SMS, Messenger oder QR-Code erst prüfen: Absender, Domain, Tonfall, Anlass.

Jedes Konto einzeln schützen

Ein Passwort pro Konto. Für wichtige Konten zusätzlich 2FA, Passkey oder Hardwarekey.

Updates schnell einspielen

Betriebssystem, Browser, Apps und Router aktuell halten. Automatische Updates einschalten.

Misstrauen bei Forderungen

Drohungen, Zeitdruck, Gutscheine und angebliche Sperren sind häufige Phishing-Muster.

GOLDENE SICHERHEITSREGEL

Wenn eine Nachricht Druck macht, Geld fordert, Zugangsdaten verlangt oder Sie auf eine Login-Seite schickt: **nicht über den Link einloggen**. Öffnen Sie die bekannte App oder tippen Sie die Adresse selbst ein.

Mini-Checkliste

- ? Ist die Website wirklich die richtige?
- ? Stimmt die Domain exakt, nicht nur ungefähr?
- ? Passt der Anlass der Nachricht?
- ? Fragt jemand nach Passwort, TAN, 2FA-Code oder Fernzugriff?

Webadressen richtig prüfen

Gefälschte Links sehen oft vertraut aus. Entscheidend ist nicht der blaue Linktext, sondern die echte Adresse dahinter.

`https:// beispielbank.de /login?ref=mail`

■ Protokoll



Echte Domain —
entscheidend!



Pfad
(egal)

Merksatz: Entscheidend ist die Domain direkt vor .de, .com, .org usw. — nicht der Text im Link.

✓ GUT

`https://www.beispielbank.de/login`

Die Domain ist klar und endet wie erwartet.

× VERDÄCHTIG

`https://beispielbank.de.login-sicher.info`

Die echte Domain ist hier **login-sicher.info**.



Das Schloss beweist nichts

Das Schloss im Browser zeigt nur, dass die Verbindung verschlüsselt ist. Auch Betrüger können ein Schloss für ihre Fake-Webseite bekommen. Es beweist nicht, dass die Webseite echt ist.



Sicherer Weg

Öffnen Sie immer die App oder tippen Sie die Adresse von Hand ein, statt einem Link aus einer Nachricht zu folgen.

Tarnung durch ähnliche Zeichen

Kriminelle nutzen Zeichen aus anderen Alphabeten oder kleine Tippfehler. Die Domains sehen identisch aus, sind es aber nicht.

ECHT	GEFÄHRLICH ÄHNLICH	WORAUF ACHTEN?
paypal.com	paypal.com	Einige Zeichen sind kyrillisch. Im Zweifel Adresse selbst eintippen.
google.com	google.com	Die beiden „o“ können andere Zeichen sein als normale lateinische.
microsoft.com	micros0ft.com	Null statt Buchstabe O. Auch Bindestriche, Zusätze und Subdomains prüfen.

Typische Tricks

! **Subdomain-Trick:** bank.de.login-sicher.info — die echte Domain ist login-sicher.info.

! **Tippfehler-Domain:** paypaI.com mit großem I statt kleinem L.

! Linktext passt nicht zur echten Adresse, die beim Darüberfahren angezeigt wird.

! QR-Codes können ebenfalls auf Fake-Seiten führen.

SCHNELLER SCHUTZ-TRICK

Nutzen Sie Lesezeichen für wichtige Seiten wie Bank, E-Mail und Cloud. Klicken Sie nicht aus Nachrichten auf Login-Links. Ein Passwortmanager hilft zusätzlich, weil er auf Fake-Domains meist nicht automatisch ausfüllt.

Phishing erkennen

Phishing bedeutet: Eine Nachricht soll Sie dazu bringen, Zugangsdaten, Zahlungsdaten oder Sicherheitscodes preiszugeben.

DRUCK

„Ihr Konto wird gesperrt. Reagieren Sie sofort.“

Künstliche Dringlichkeit soll Sie zum Handeln ohne Nachdenken bringen.

BELOHNUNG

„Sie haben gewonnen. Melden Sie sich an.“

Unerwartete Gewinne oder Preise, für die Sie sich anmelden müssen.

UNGEWÖHNLICHE ANFRAGE

„Chef, Bank oder Support fragt plötzlich nach Daten.“

Anfragen, die außerhalb des normalen Kontexts auftreten.

UNERWARTETER ANHANG

„Rechnung, Bewerbung oder Office-Datei ohne Anlass.“

Anhänge, die Sie nicht erwartet haben, immer mit Vorsicht öffnen.



Merke

Keine seriöse Bank und kein seriöser Dienst fragt per E-Mail, SMS oder Chat nach Ihrem Passwort, einer TAN, einem 2FA-Code oder fordert Fernzugriff auf Ihr Gerät.

Besser reagieren

- ✓ Nicht antworten, keine Links öffnen, keine Anhänge öffnen.
- ✓ Über offizielle App oder bekannte Adresse anmelden.
- ✓ Unerwartete Forderungen über eine bekannte Telefonnummer prüfen.
- ✓ Bei Konten mit Geld oder wichtigen Daten sofort Passwort ändern und Sitzungen abmelden.

Konto absichern: vom Minimum zum starken Schutz

BASIS	Passwort	Mindestanforderung — einzigartiges, langes Passwort pro Konto.
BESSER	Passwortmanager	Einzigartige Passwörter für alle Konten automatisch generieren und verwalten.
GUT	2FA-App / Passkey	Zweite Hürde beim Login — verhindert die meisten Kontoübernahmen.
STARK	Hardwarekey	Physischer Sicherheitsschlüssel für E-Mail, Bank und wichtige Konten.

Empfohlene Reihenfolge

1. E-Mail zuerst

Die E-Mail ist oft der Schlüssel zum Zurücksetzen anderer Konten. Zuerst absichern.

2. Finanzkonten

Bank, PayPal, Shopping, Steuerportale und Versicherungen besonders absichern.

3. Cloud & Social

Cloud-Speicher, Fotos, Chats und soziale Netzwerke enthalten oft sensible Daten.

4. Recovery sichern

Wiederherstellungs-E-Mail, Telefonnummer und Recovery-Codes aktuell halten.

Passend dazu

Wie die Einstellungen bei Instagram, Facebook, X, TikTok und WhatsApp konkret heißen, steht in der Schwesterbroschüre „**Social Media Sicherheit**“ — dort auch zu Privatsphäre, Fake-Profilen und Kontoübernahme.

Wenn die Zeit knapp ist

Nur ein Schritt möglich? Dann 2FA für das E-Mail-Konto. Wer die E-Mail kontrolliert, kann bei fast allen anderen Diensten das Passwort zurücksetzen.

Passwörter ohne Kopfschmerzen

BEISPIEL	BEWERTUNG	WARUM?
Sommer2026	× Schlecht	Kurz, erratbar, Muster aus Wort + Jahreszahl.
Kater!Auto?Lampe	~ Mittel	Besser — aber wiederverwendbar?
heute-berg-lampe-pizza-92	✓ Gut	Lang, gut merkbar, zufällig kombiniert.
Tj8#mL!kPq2\$nXvR...	✓✓ Ideal	Vom Passwortmanager: 24+ Zeichen, einzigartig je Konto.

Lang schlägt kompliziert

Eine lange Kombination aus Wörtern ist oft besser merkbar als kurze Sonderzeichen-Kunst.

Einzigartig je Konto

Dasselbe Passwort bei mehreren Diensten ist gefährlich — ein Datenleck betrifft dann alle Konten.



Nicht verwenden

Namen, Geburtsdaten, Haustiere, Lieblingsverein, Tastaturmuster (qwertz), Passwort mit Jahreszahl oder Passwörter aus bekannten Datenlecks.



Für wenige wirklich wichtige Konten: eine lange Passphrase nutzen.



Für alles andere: Passwortmanager zufällige Passwörter erzeugen lassen.



Nie Passwörter per Chat, E-Mail oder Telefon weitergeben.



Keine KI zum Passwörter generieren nutzen

KI-Chatbots sind keine echten Zufallsgeneratoren. Die erzeugten Passwörter folgen statistischen Mustern aus Trainingsdaten und sind damit leichter vorhersagbar, als sie erscheinen. Hinzu kommt: Eingaben in KI-Systeme können für Training oder Logging genutzt werden — ein eingegebenes oder generiertes Passwort könnte so dauerhaft gespeichert sein. Nutzen Sie stattdessen den eingebauten Generator Ihres Passwortmanagers oder systemnahe Werkzeuge wie pwgen. Diese arbeiten mit echten kryptografischen Zufallsquellen.

Passwortmanager richtig nutzen

Ein Passwortmanager ist ein digitaler Tresor. Er speichert Passwörter verschlüsselt und hilft, für jeden Dienst ein eigenes Passwort zu verwenden.

✓ Einzigartige Passwörter

Sie müssen sich nicht jedes Passwort merken und nutzen trotzdem starke Kombinationen.

✓ Phishing-Bremse

Der Manager füllt auf einer falschen Domain oft nicht automatisch aus.

✓ Weniger Zettelchaos

Passwörter liegen nicht offen auf dem Schreibtisch oder in ungeschützten Dateien.

Vorsicht

Der Tresor braucht ein sehr gutes Masterpasswort und Schutz durch 2FA oder Passkey.

Sicher einrichten

- ✓ Starkes Masterpasswort wählen und sicher merken.
- ✓ 2FA für den Passwortmanager aktivieren.
- ✓ Wiederherstellungs- und Notfalloptionen prüfen.
- ✓ Updates für den Passwortmanager installieren.
- ✓ Passwörter nicht als unverschlüsselte Datei exportieren.

Bin ich schon betroffen? Datenlecks selbst prüfen

Bei Datenpannen landen oft Millionen E-Mail-Adressen und Passwörter in öffentlichen Listen. Das kostenlose Werkzeug Have I Been Pwned durchsucht diese — ohne selbst Daten zu speichern.

E-Mail-Adresse prüfen

Gibt an, bei welchen bekannten Datenpannen die Adresse aufgetaucht ist und welche Daten betroffen waren. Kein Konto nötig.

Passwort prüfen

Prüft, ob ein Passwort in Leaks vorkommt. Nur ein Hash-Ausschnitt wird übertragen — das Passwort verlässt Ihr Gerät nie (k-Anonymität). Unter „Passwords“ erreichbar.

haveibeenpwned.com

Unabhängig betrieben von Sicherheitsforscher Troy Hunt. Kostenlos, werbefrei, von vielen Passwortmanagern direkt eingebunden.

2FA, Passkeys und Hardwarekeys

Eine zweite Anmeldehürde verhindert viele Kontoübernahmen. Passkeys und Hardwarekeys schützen besser gegen Phishing als einfache SMS-Codes.

METHODE	STÄRKE	ALLTAG	HINWEIS
SMS-Code	Mittel	Einfach	Besser als nur Passwort, aber anfällig für SIM-Tausch und Weitergabe.
Authenticator-App	Gut	Gut	Codes nie an andere weitergeben. Backup und Gerätewechsel vorab prüfen.
Passkey	Hoch	Sehr gut	Login per PIN, Fingerabdruck oder Gesichtserkennung. Sehr bequem.
Hardwarekey	Sehr hoch	Gut	Für E-Mail, Admin-, Finanz- und sehr wichtige Konten. Phishing-resistent.

i Hardwarekey oder Passkey?

Passkeys sind für die meisten Nutzer sehr sicher und bequem. Ein Hardwarekey ist für besonders wichtige Konten noch stärker, weil der Schlüssel physisch getrennt ist. Beispiele: Yubico YubiKey, Swissbit iShield Key. Immer mindestens zwei Schlüssel registrieren.

! Was Passkeys leisten — und was nicht

Der Schutz steckt nicht im Schlüssel: Ein Hardwarekey weiß nicht, auf welcher Seite Sie gerade sind. Die Bindung an die echte Adresse macht der **Browser**. Er lässt die Anmeldung unter einer anderen Domain gar nicht erst zu — auch dann nicht, wenn die nachgebaute Seite alles an den echten Dienst weiterreicht.

Zwei Wege bleiben trotzdem. **Erstens der Umweg:** Die gefälschte Seite fragt statt des Passkeys etwas anderes ab — „Passkey gerade nicht verfügbar, bitte SMS-Code eingeben“. Dieser Weg funktioniert, weil Sie den Code selbst eintippen. Werden Sie misstrauisch, wenn ein Dienst plötzlich eine andere Anmeldeart will als sonst. **Zweitens die bestehende Sitzung:** Der Schlüssel schützt die Anmeldung, nicht das, was danach im Browser gilt — dazu das nächste Kapitel.

! Der wichtigste Fehler

Geben Sie einen Sicherheitscode, Push-Code oder Recovery-Code niemals an andere weiter — auch nicht an angeblichen Support. Wer den Code bekommt, kann sich oft als Sie anmelden.

Abmelden nicht vergessen — auch mit 2FA

Zwei-Faktor-Schutz sichert die Anmeldung. Was danach passiert, schützt er nicht mehr.

DER UNSICHTBARE AUSWEIS

Nach dem Anmelden merkt sich der Dienst Sie über einen unsichtbaren Ausweis im Browser: „Diese Person hat Passwort und zweiten Faktor bereits gezeigt.“ Solange er gilt, fragt niemand mehr nach — auch nicht nach dem 2FA-Code. Genau diesen Ausweis wollen Angreifer haben, nicht Ihr Passwort.

Wie der Diebstahl abläuft

- 1 Sie klicken auf einen Link und landen auf einer Seite, die aussieht wie Ihre Bank oder Ihr E-Mail-Anbieter.
- 2 Diese Seite reicht alles, was Sie eingeben, unbemerkt an die **echte** Seite weiter — auch den 2FA-Code. Die echte Seite meldet Sie an, für Sie sieht alles völlig normal aus.
- 3 Im selben Moment fängt der Angreifer den Ausweis ab. Er ist damit angemeldet — **ohne Passwort, ohne zweiten Faktor** — und bleibt es oft tage- oder wochenlang.

Was hilft

- ✓ Bei wichtigen Konten am Ende bewusst auf **Abmelden** klicken. Nur das Fenster zu schließen genügt nicht — der Ausweis bleibt gültig.
- ✓ „Angemeldet bleiben“ bei Bank, E-Mail und Behördenportalen nicht aktivieren, auf fremden Geräten grundsätzlich nicht.
- ✓ Viele Dienste führen unter „Sicherheit“ eine Liste aktiver Sitzungen. Dort nachsehen, wann immer Sie auf einen verdächtigen Link geklickt haben, und „**Auf allen Geräten abmelden**“ wählen — das macht auch gestohlene Ausweise ungültig.
- ✓ Ein Passwortwechsel beendet bei vielen Diensten zugleich alle Sitzungen — aber nicht bei allen. Die Geräteliste danach zusätzlich prüfen.
- ✓ **Passkeys und Hardwarekeys** schützen sehr wirksam vor klassischen Phishing-Seiten: Der Browser lässt die Anmeldung nur für die echte Internetadresse des Dienstes zu — auch dann, wenn die gefälschte Seite alles an den echten Dienst weiterreicht. Bereits bestehende Sitzungen können jedoch — etwa durch Schadsoftware oder den Diebstahl von Sitzungstokens — unter Umständen trotzdem übernommen werden. Deshalb bleiben ein aktueller Browser, ein sauberes Gerät und bewusstes Abmelden auf fremden Geräten wichtig.

DNS verstehen: das Telefonbuch des Internets

DNS übersetzt Namen wie `beispiel.de` in technische IP-Adressen. Ein anderer DNS-Anbieter kann mehr Privatsphäre, Geschwindigkeit oder Schutzfilter bieten — sieht aber auch, welche Domains angefragt werden.

`beispiel.de` → Welche IP? → **203.0.113.42**

Sie tippen DNS fragt Antwort — Browser lädt die Webseite

Ein Schutz-DNS kann bekannte Schadseiten blockieren — ersetzt aber keinen gesunden Klick-Verstand.

Vorteile anderer DNS-Server

Kann bekannte Schadseiten, Phishing- oder Malware-Domains blockieren; manchmal schneller; oft mit DNS-over-HTTPS oder DNS-over-TLS nutzbar.

Nachteile und Grenzen

Der DNS-Anbieter sieht Ihre Domain-Anfragen. Manche Filter blockieren legitime Seiten oder sind leicht umgehbar. DNS ersetzt keinen Virenschutz und keine Updates.

WARUM DNS EINE DATENSCHUTZFRAGE IST

Jede aufgerufene Domain läuft über den DNS-Server — auch bei HTTPS-Seiten. Wer den DNS betreibt, kann daraus ablesen, welche Dienste, Banken, Ärzte oder Zeitungen Sie nutzen. Ohne eigene Einstellung ist das der Server des Internetanbieters, meist unverschlüsselt im Klartext. **DNS-over-HTTPS (DoH)** oder **DNS-over-TLS (DoT)** verschlüsseln diese Anfragen — sichtbar bleiben sie weiterhin für den gewählten Anbieter. Die eigentliche Entscheidung lautet also nicht „DNS ja oder nein“, sondern: **Wem vertraue ich diese Liste an?**

Wichtig für Familien

Schutz-DNS kann ein gutes zusätzliches Netz sein, besonders für Kinder oder weniger erfahrene Nutzer. Erklären Sie, warum Warnseiten erscheinen und wie man bei Fehlblockaden reagiert.

DNS-Anbieter im Vergleich

Diese Beispiele sind keine Werbung, sondern Orientierung. Adressen vor der Einrichtung immer auf der offiziellen Anbieter-Webseite prüfen.

Cloudflare DNS

1.1.1.1

Standard primär	1.1.1.1 / 2606:4700:4700::1111
Standard sekundär	1.0.0.1 / 2606:4700:4700::1001
Malware-Filter	1.1.1.2 / 1.0.0.2 · ::1112 / ::1002
Malware + Erwachsene	1.1.1.3 / 1.0.0.3 · ::1113 / ::1003

Sehr verbreitet, meist schnell, einfache Adressen. Für Schutzfilter müssen die Families-Adressen genutzt werden. Großer zentraler Anbieter.

Google Public DNS

8.8.8.8

Primär	8.8.8.8 / 2001:4860:4860::8888
Sekundär	8.8.4.4 / 2001:4860:4860::8844

Sehr hohe Verfügbarkeit und globale Infrastruktur. Kein Malware- oder Familienfilter im Standarddienst. Wer Google aus Datenschutzgründen meiden möchte, sollte einen anderen Anbieter wählen.

Schutz-DNS: Quad9 und DNS4EU

Schutz-DNS blockiert bekannte gefährliche Domains. Hilfreich gegen manche Malware- und Phishing-Seiten — ersetzt aber keine Updates, keinen Virenschutz und kein vorsichtiges Verhalten.

Quad9 DNS

Sicherheitsfokus

Primär (empfohlen)	9.9.9.9 / 2620:fe::fe
Sekundär	149.112.112.112 / 2620:fe::9
DoH	https://dns.quad9.net/dns-query

Blockiert bekannte bösartige Domains, validiert DNSSEC, starker Sicherheits- und Datenschutzfokus. Primär Sicherheitsfilter ohne umfangreiche Familien- oder Werbefilter.

DNS4EU

EU · mehrere Profile

Protective	86.54.11.1 / 2a13:1001::86:54:11:1
Protective + Child	86.54.11.12 / 2a13:1001::86:54:11:12
Protective + Ads	86.54.11.13 / 2a13:1001::86:54:11:13
Protective + Child + Ads	86.54.11.11 / 2a13:1001::86:54:11:11
Unfiltered	86.54.11.100 / 2a13:1001::86:54:11:100

EU-orientierter Dienst mit mehreren Profilen. Vor Einrichtung aktuelle Dokumentation und gewünschtes Profil prüfen.

DNS einrichten: einfache Wege

Am Router

DNS-Adressen im Router eintragen. Vorteil: alle Geräte im WLAN profitieren. Nachteil: Menü je Hersteller unterschiedlich.

Auf Einzelgeräten

DNS pro Gerät setzen. Vorteil: gut zum Testen. Nachteil: jedes Gerät separat pflegen.

Im Browser

DNS-over-HTTPS in den Browser-Einstellungen wählen. Vorteil: einfach. Nachteil: gilt meist nur für diesen Browser.

Per Anbieter-App

Manche Anbieter bieten Apps. Vorteil: bequem. Nachteil: zusätzliche Software und Berechtigungen prüfen.

Sichere Test-Reihenfolge

- 1 Gewünschten Anbieter und Profil auswählen. Adressen von der offiziellen Anbieter-Webseite kopieren.
- 2 Erst ein Gerät testen. Webseiten öffnen, Videokonferenzen, Banking und Streaming prüfen.
- 3 Wenn alles funktioniert, DNS am Router setzen oder auf weitere Geräte übertragen.
- 4 Nach der Umstellung prüfen, ob Schutzseiten blockiert werden und ob Fehlblockaden auftreten.
- 5 Alte Werte notieren, damit Sie bei Problemen zurückstellen können.

! Nicht blind kopieren

DNS-Adressen aus Foren, Kommentaren oder Screenshots können falsch sein. Nutzen Sie immer die offiziellen Webseiten der Anbieter.

Geräte, Updates, WLAN und Backups

Updates

Automatische Updates für Betriebssystem, Browser, Apps und Router aktivieren.

Bildschirmsperre

PIN, Passwort, Fingerabdruck oder Gesichtserkennung nutzen.

Backups

Wichtige Daten regelmäßig sichern: Cloud plus externe Festplatte ist ideal.

WLAN

Starkes WLAN-Passwort, aktueller Router, WPA2/WPA3 und Gastnetz für Besuch oder Smart-Home-Geräte.

DIE 3-2-1-REGEL FÜR BACKUPS

3 Kopien der Daten, auf 2 verschiedenen Medien, davon 1 außer Haus oder offline. Wer das einhält, übersteht Ransomware, Diebstahl und Festplattenschäden gleichermaßen.

Für das Handy eigens

Sperre, Berechtigungen, Verlust und der heikle Gerätewechsel mit zweitem Faktor stehen in „Smartphone absichern“. Router, WLAN, Gastnetz und vernetzte Kleingeräte behandelt „Heimnetz und Smart Home“.

Ransomware-Schutz im Alltag

- ✓ Mindestens eine Sicherung sollte nicht dauerhaft mit dem Computer verbunden sein.
- ✓ Cloud-Sync ist praktisch, aber kein vollständiger Ersatz für Backups.
- ✓ Gelegentlich testen, ob sich Dateien aus dem Backup wiederherstellen lassen.
- ✓ Keine unbekannten Programme installieren, besonders nicht aus Links in Nachrichten.

Öffentliche WLANs und unterwegs

Hotel, Café, Bahn, Flughafen: Offene Netze sind bequem und meist unproblematisch, solange man weiß, was sie nicht leisten. Moderne Webseiten sind per HTTPS verschlüsselt – der Inhalt ist also geschützt. Sichtbar bleibt trotzdem, mit welchen Diensten Ihr Gerät spricht.

Gefälschte Hotspots

Ein Netz namens „Hotel-Gast-WLAN“ kann von jedem aufgespannt werden. Im Zweifel den Namen beim Personal erfragen, nicht raten.

Automatisch verbinden

Geräte verbinden sich mit einmal gespeicherten Netznamen später wieder von allein. Alte Hotspots regelmäßig aus der Liste löschen.

Sichtbar im Netz

Datei- und Druckerfreigabe im öffentlichen Netz abschalten. Windows, macOS und Linux fragen beim ersten Verbinden nach dem Netzwerktyp – „öffentlich“ wählen.

Fremde Ladebuchsen

An öffentlichen USB-Buchsen nur laden, nicht Daten übertragen. Sicherer ist das eigene Netzteil oder eine Powerbank.

Was ein VPN leistet – und was nicht

EIN VPN...	BEWERTUNG	ERLÄUTERUNG
verbirgt Ihre Aktivität vor dem Netzbetreiber	✓ ja	Wer das Netz betreibt – das Café oder Hotel hier, zu Hause Ihr Internetanbieter – sieht nur noch eine verschlüsselte Verbindung zum VPN-Anbieter.
verlagert das Vertrauen	~ beachten	Statt des Netzbetreibers sieht nun der VPN-Anbieter Ihren Datenverkehr. Anbieterwahl ist deshalb eine Vertrauensfrage.
schützt vor Phishing und Schadsoftware	✗ nein	Ein VPN prüft keine Inhalte. Gefälschte Login-Seiten funktionieren durch das VPN hindurch genauso.
macht Sie anonym	✗ nein	Anmeldungen, Cookies und Konten identifizieren Sie weiterhin.



Kostenlose VPN-Apps

Wer nichts zahlt, finanziert den Dienst anders. Bei kostenlosen VPN-Anbietern ist der Weiterverkauf von Verbindungsdaten ein bekanntes Geschäftsmodell – das ist das Gegenteil dessen, wofür man ein VPN nutzt. Für unterwegs reicht oft der eigene Handy-Hotspot.



Zusammenhang mit DNS

Auch mit VPN bleibt die Frage, wer Ihre Namensauflösung sieht. Ein VPN bringt meist einen eigenen DNS mit – welchen, steht in den Einstellungen des Anbieters. Mehr dazu im Kapitel „DNS verstehen: das Telefonbuch des Internets“ und den drei folgenden.

Erpressung, Schockanrufe und falscher Support

Diese Maschen zielen nicht auf Technik, sondern auf Gefühle: Angst, Scham, Respekt vor Autorität und Zeitdruck. Wer das Muster kennt, erkennt sie meist im ersten Satz.

ERPRESSUNGSMAIL (SEXTORTION)

„Ich habe Sie über Ihre Webcam gefilmt. Zahlen Sie in Bitcoin, sonst ...“

Fast immer ein Bluff per Massenversand. Das mitgeschickte „Beweis“-Passwort stammt meist aus einem alten Datenleck. Nicht zahlen, nicht antworten, löschen — und das genannte Passwort überall ändern, wo es noch im Einsatz ist.

FALSCHER SUPPORT-ANRUF

„Hier ist Microsoft. Ihr Rechner sendet Fehlermeldungen.“

Kein Hersteller ruft unaufgefordert wegen eines Virus an. Ziel ist Fernzugriff oder eine Zahlung. Auflegen — nicht diskutieren, nicht zurückrufen unter der genannten Nummer.

FERNWARTUNG

„Installieren Sie kurz dieses Hilfsprogramm, dann sehe ich das Problem.“

Wer Fernzugriff bekommt, sieht Konten, Online-Banking und gespeicherte Passwörter. Fernwartung nur, wenn Sie den Support selbst über eine offizielle Nummer angerufen haben.

SCHOCKANRUF / NEUE NUMMER

„Mama, mein Handy ist kaputt — das ist meine neue Nummer. Kannst du kurz überweisen?“

Erst Beziehung aufbauen, dann Zahlung. Immer über die alte, bekannte Nummer zurückrufen. Eine Rückfrage, deren Antwort nur die echte Person kennt, entlarvt die Masche zuverlässig.

GEMEINSAMER NENNER

Alle vier Maschen brauchen eine sofortige Reaktion. **Genau die dürfen Sie sich nehmen: Zeit.** Auflegen, kurz durchatmen und über einen selbst gewählten Kanal zurückfragen kostet nichts — und beendet jeden dieser Angriffe.

Wenn schon etwas passiert ist

- ✓ Fernwartung lief bereits: Gerät sofort vom Netz trennen, Passwörter von einem **anderen** Gerät ändern, Bank informieren, Gerät prüfen lassen.
- ✓ Geld überwiesen: sofort die Bank anrufen und nach einer Rückholung fragen — bei schneller Meldung ist sie manchmal möglich.
- ✓ Erpressungsmail erhalten: nicht zahlen. Zahlungen bestätigen dem Absender nur eine aktive Adresse.
- ✓ Beweise sichern und Anzeige erstatten — auch bei geringen Beträgen, weil erst die Summe der Anzeigen Ermittlungen ermöglicht.

Wenn doch etwas passiert



Wichtig

Ruhig bleiben, aber schnell handeln. Die Reihenfolge hängt vom Vorfall ab.

#	SCHRITT	WAS TUN?
1	Verbindung trennen	Bei Malware-Verdacht WLAN/LAN trennen. Nicht sofort ausschalten, wenn Beweise wichtig sein könnten.
2	Passwort ändern	Von einem sauberen Gerät aus wichtige Passwörter ändern, besonders E-Mail, Bank und Passwortmanager.
3	Sitzungen abmelden	In Konten „alle Geräte abmelden“ oder „Sitzungen beenden“ wählen.
4	Anbieter informieren	Bank, Kreditkarte, E-Mail-Anbieter oder Plattform kontaktieren, wenn Geld oder Identität betroffen sind.
5	Beweise sichern	Screenshots, E-Mails, Telefonnummern, Zeitpunkte und Abbuchungen dokumentieren.



Auskunft und Löschung verlangen

Nach einem Vorfall ist oft unklar, wer welche Daten hat. Welche Rechte Sie dabei haben und wie ein Antrag aussieht, steht in „**Deine Rechte an deinen Daten**“, Kapitel „So stellen Sie einen Antrag“.



Bei Geldverlust oder Identitätsdiebstahl

Kontaktieren Sie Bank oder Kreditkartenanbieter, ändern Sie Passwörter, sichern Sie Beweise und wenden Sie sich bei Bedarf an Polizei oder Verbraucherberatung.

Karten und Zugänge sperren

Nach Verlust, Diebstahl oder Kartenbetrug zählt jede Minute. Wo Sie anrufen müssen, hängt vom Land ab — eine europaweit einheitliche Nummer gibt es entgegen der ursprünglichen Absicht nicht.

LAND	ZENTRALER SPERRDIENST	HINWEIS
Deutschland	116 116 Ausland: +49 116 116	girocard immer; Kreditkarten nur, wenn der Herausgeber Kooperationspartner ist (über 90 Prozent der Karten, nicht alle).
Österreich	0800 204 88 00 Ausland: +43 1 204 88 00	Zentraler Bankomatkarten-Sperrnotruf. Innerhalb der Banköffnungszeiten führt der Weg über die eigene Bank.
Andere Länder	kein vergleichbarer Dienst	Direkt beim Herausgeber sperren: Nummer auf der Kartenrückseite, in der Banking-App oder auf der Website der Bank.

Warum es keine EU-weite Nummer gibt

Die 116 116 gehört zum EU-weit reservierten Nummernbereich 116xxx für Dienste von sozialem Wert und war ausdrücklich für das Sperren verlorener Zahlungskarten vorgesehen. Freigeschaltet hat sie in der Praxis vor allem Deutschland — in den meisten Mitgliedstaaten führt kein zentraler Dienst zusammen, was dort die einzelnen Banken tun.

Immer gültig: Die Sperrnummer des Herausgebers steht auf der Kartenrückseite und in der Banking-App. Im Ausland helfen zusätzlich die weltweiten Notdienste der Kartensysteme — Visa Global Customer Assistance und Mastercard Global Service — rund um die Uhr, mit eigenen Rufnummern je Land. Notieren Sie sich Ihre Nummern vorab; im Ernstfall ist die Karte weg, auf der sie stehen.

Spickzettel zum Ausdrucken

Diese Seite lässt sich einzeln ausdrucken und neben den Rechner legen. Sie enthält deshalb bewusst nur Häkchen und Telefonnummern — keine Zugangsdaten.

VOR DEM KLIICK

- ☐ Domain stimmt exakt
- ☐ Kein Link aus einer Mail blind geklickt
- ☐ Druck und Drohung ignoriert
- ☐ Dateianhang war erwartet

KONTOSCHUTZ

- ☐ Passwortmanager aktiv
- ☐ 2FA/Passkey aktiv
- ☐ Recovery-Codes sicher abgelegt
- ☐ SMS ist nicht der einzige Faktor

GERÄTE

- ☐ Updates automatisch
- ☐ Backups vorhanden und getestet
- ☐ Kein Admin-Konto im Alltag
- ☐ Router-Passwort geändert

NOTFALLKONTAKTE

Bank / Kreditkarte (Sperrnummer):

E-Mail-Anbieter:

Mobilfunkanbieter:

Sperrdienst im eigenen Land:

! Was hier nicht hingehört

Keine Passwörter, PINs, TANs, Recovery-Codes und keine Antworten auf Sicherheitsfragen. Ein Zettel neben dem Rechner ist für jeden lesbar, der im Raum steht — für Besuch, Handwerker, Reinigungskraft oder bei einem Einbruch. **Recovery-Codes gehören verschlossen:** versiegelter Umschlag, abschließbare Schublade, Tresor oder Bankschließfach. Wer sie digital ablegt, nutzt dafür einen zweiten, getrennt gesicherten Speicher — nicht denselben Passwortmanager, für den sie die Notfalloflösung sind.

WENN SIE NUR EINE REGEL BEHALTEN

Niemals über einen Link aus einer Nachricht einloggen. App öffnen oder Adresse selbst eintippen.

Erste Hilfe bei verdächtigen Nachrichten

Komische Nachricht bekommen? Nicht sicher, ob echt? Ruhig bleiben und der Reihe nach vorgehen.

GRUNDREGEL

Nicht antworten, keine Codes weitergeben, keine Fernwartung starten. Im Zweifel über die offizielle App, eine bekannte Telefonnummer oder die selbst eingetippte Adresse prüfen — nie über einen Link aus der Nachricht.

Typische Situationen

- ? „Ihr Konto wird gesperrt“ — Link in E-Mail oder SMS. Link nicht klicken. App öffnen oder Adresse von Hand eintippen und dort prüfen.
- ? Jemand fragt nach einem Code, den Sie gerade bekommen haben. Niemals weitergeben — egal ob Telefon, Chat oder angeblicher Support. Wer den Code hat, ist eingeloggt.
- ? Unbekannter Anhang oder unerwartete Datei. Nicht öffnen. Absender über einen bekannten Kanal fragen (nicht per Antwort), ob er sie wirklich geschickt hat.
- ? Sie haben bereits geklickt oder Daten eingegeben. Passwort sofort von einem anderen Gerät ändern, alle Sitzungen abmelden, Bank informieren. Beweise (Screenshot, URL) sichern.
- ? Fernwartungssoftware wurde installiert oder geöffnet. Sofort Internetverbindung trennen (WLAN aus oder Kabel ziehen). Gerät von einer Fachperson prüfen lassen.

i Geld oder Identität betroffen?

Bank und Kreditkartenanbieter sofort anrufen. Bei Identitätsdiebstahl Anzeige bei der Polizei erstatten und gegebenenfalls die Verbraucherberatung kontaktieren.

Quellen und weiterführende Hinweise

BSI: Zwei-Faktor-Authentisierung

[bsi.bund.de](#) → Accountschutz → Zwei-Faktor-Authentisierung

BSI: Passkeys

[bsi.bund.de](#) → Accountschutz → Passkeys

BSI: Passwortmanager

[bsi.bund.de](#) → Accountschutz → Passwort-Manager

CISA: Recognize and Report Phishing

[cisa.gov/secure-our-world/recognize-and-report-phishing](#)

NCSC UK: Password managers

[ncsc.gov.uk](#) → top-tips-for-staying-secure-online

Quad9: Service Addresses & Features

[quad9.net/service/service-addresses-and-features/](#)

DNS4EU: Public Service

[joindns4.eu/for-public](#)

Cloudflare: 1.1.1.1 Setup and Families

[developers.cloudflare.com/1.1.1.1/setup/](#)

Google Public DNS

[developers.google.com/speed/public-dns/docs/using](#)

Yubico: FIDO2 / YubiKey

[yubico.com/authentication-standards/fido2/](#)

Swissbit: iShield Key 2

[swissbit.com](#) → Produkte → iShield Key 2

Have I Been Pwned: Datenleck-Prüfung

[haveibeenpwned.com](#)

BSI: Sicher im öffentlichen WLAN

[bsi.bund.de](#) → Verbraucher → Netzwerk-Sicherheit → WLAN

BSI: Virtuelle Private Netzwerke (VPN)

[bsi.bund.de](#) → Verbraucher → Netzwerk-Sicherheit → VPN

Verbraucherzentrale: Erpressungsmails und Sextortion

[verbraucherzentrale.de](#) → Digitale Welt → Phishing-Radar

Polizeiliche Kriminalprävention: Falsche Support-Anrufe und Schockanrufe

[polizei-beratung.de](#) → Themen → Betrug

Sperr-Notruf 116 116: Umfang, Kooperationspartner und Ablauf

[sperr-notruf.de](#) (Partnerliste unter „Anbieter“)

Payment Services Austria: Bankomatkarten-Sperrnotruf

[oesterreich.gv.at](#) → Steuern und Finanzen → Bankgeschäfte

Kartensysteme: weltweite Notdienste je Land

[visa.com](#) → Lost/Stolen • [mastercard.com](#) → Emergency Services

Weitere Broschüren dieser Reihe

Cybersecurity im Alltag — diese Broschüre

Social Media Sicherheit — Konten, Privatsphäre-Einstellungen, Fake-Profile, Datenweitergabe.

Smartphone absichern — Sperre, Berechtigungen, App-Quellen, Verlust, Gerätewechsel, Backups.

Heimnetz und Smart Home — Router, WLAN, Gastnetz, vernetzte Geräte, Kameras, Portfreigaben.

Kinder online begleiten — Für Eltern: Altersgrenzen, Regeln, Mobbing, Grooming, Anlaufstellen.

Deine Rechte an deinen Daten — DSGVO praktisch: Auskunft, Löschung, Übertragbarkeit, Musterschreiben.

Gruppen sicher organisieren — Rollen, Regeln, Störer, Treffen, Voice, Minderjährige in der Gruppe.

Allergene und Kennzeichnung — Die 14 Pflichtangaben, Zutatenlisten lesen, „kann Spuren enthalten“.

Erste Schritte — Zweiseitiges Merkblatt zum Einstieg — kein Heft.

Weitergabe und Lizenz

Herausgeber

Plotspace.eu · info@plotspace.eu

Anschrift und Verantwortlicher im Impressum:

plotspace.eu/impressum

Lizenz

CC BY 4.0 — Kopieren, Weitergeben und Bearbeiten ausdrücklich erlaubt. Bitte „Plotspace.eu“ als Quelle nennen und Änderungen kenntlich machen; bearbeitete Fassungen dürfen nicht so wirken, als kämen sie von Plotspace.eu. creativecommons.org/licenses/by/4.0/deed.de

Schriften: Public Sans und IBM Plex Mono, SIL Open Font License 1.1.

Diese Broschüre darf einzeln weitergegeben werden. Sie ist so aufgebaut, dass sie für sich allein verständlich bleibt; Querverweise auf die Schwesterbroschüre sind Ergänzung, keine Voraussetzung.



Hinweis

Diese Broschüre ersetzt keine individuelle IT-Beratung. Dienste und Anbieter ändern Funktionen, Adressen und Datenschutzbedingungen. Prüfen Sie vor der Einrichtung stets die aktuelle offizielle Dokumentation.