Merkliste: Schritt für Schritt sicher im Netz unterwegs – damit du nicht zum Opfer wirst!

Denke nach, bevor du etwas teilst:

Starte mit einem einfachen, aber wichtigen Schritt: Überlege, bevor du etwas ins Internet stellst.

Frage dich: Würde ich das auch einer fremden Person zeigen? Ist das für immer okay, wenn es online bleibt?

Social Media klug nutzen: überprüfe regelmäßig deine Privatsphäre-Einstellungen.

Gib keine persönlichen Daten preis:

Teile keine Passwörter, Adressen oder andere private Informationen in Chats oder E-Mails – auch nicht mit Freunden.

Achte auf Warnsignale in Chats:

Wenn jemand dich unter Druck setzt oder ungewöhnliche Dinge von dir verlangt, sei skeptisch und rede mit einem Erwachsenen. Bist du bereits Erwachsen? Dann rede mit einem Profi oder wende dich an die Polizei-/Behördenstelle.

Bleib aufmerksam und lern dazu:

Cybersicherheit ist ein Lernprozess: Informiere dich über neue Bedrohungen und Technologien.

Nutze dein Wissen: Hilf Familie und Freunden, sicher im Netz unterwegs zu sein!

Sei vorsichtig mit Links und Anhängen:

Klicke nicht auf verdächtige Links oder Anhänge, vor allem in E-Mails oder Nachrichten von unbekannten Personen.

Erstelle sichere Passwörter:

Wähle Passwörter, die mindestens 12 Zeichen lang sind und eine Mischung aus Buchstaben, Zahlen und Sonderzeichen enthalten. Beim Passwort gilt: Je länger desto besser!

Du hast keine Lust auf Passwörter?

Nutze Passkeys: Sie ersetzen Passwörter und machen Phishing nahezu unmöglich (unterstützt von Google, Apple, etc.). Passkeys empfehle ich aber nur geübten Anwendern und Anwenderinnen.

Nutze eine Zwei-Faktor-Authentifizierung:

Füge eine zweite Sicherheitsebene hinzu, indem du z. B. einen Code über eine Authenticator-App erhältst. Dadurch wird dein Konto viel schwerer zu hacken. SMS-Codes sind so 2010! Wie Postkarten: Jeder kann sie lesen, wenn er will.

Prüfe Webseiten, bevor du etwas kaufst:

Kaufe nur auf sicheren Webseiten ein, die mit „https://“ beginnen und ein Schloss-Symbol in der Adressleiste zeigen.

Wenn dir ein Onlineshop die neueste PlayStation für 50 Euro anbietet, sei skeptisch – außer, du glaubst auch an Einhörner, die Pizza liefern! Fake-Shops erkennen meist nur die, die zweimal hinschauen.

Halte deine Geräte und Apps aktuell:

Installiere Updates zeitnah, wenn sie verfügbar sind.
Sie enthalten oft wichtige Sicherheitsverbesserungen.

Nutze Antivirus-Programme:

Installiere ein gutes Antivirus-Programm und lasse es regelmäßig nach Schadsoftware suchen. Es erkennt und blockiert viele Gefahren automatisch.

Installiere Browser-Plugins: Tools wie „uBlock Origin“ oder „Emsisoft Browser Security“ erkennen gefährliche Seiten.

Melde Probleme sofort:

Wenn etwas Verdächtiges passiert, sprich mit jemandem, dem du vertraust (z. B. Eltern oder Lehrern). Lieber einmal zu viel fragen, als ein großes Problem zu riskieren.

Sei vorsichtig mit kostenlosen Downloads:

Lade Apps, Spiele oder Programme nur aus offiziellen Quellen wie dem Google Play Store oder Apple App Store herunter.

Gerätesicherheit:

Verhindere Kameramissbrauch und verwende physische Abdeckungen für Webcam und Mikrofon oder deaktiviere sie in den Geräteeinstellungen.

Du fühlst dich noch nicht sicher genug?

Verwende einen Passwort-Manager:

Mit einem Passwort-Manager musst du dir nur ein starkes Hauptpasswort merken. Alle anderen Passwörter oder Passkeys werden sicher für dich gespeichert.

Schütze dein WLAN:

Ändere das Standardpasswort deines WLAN-Routers zu einem starken Passwort. So schützt du dein Zuhause vor ungebetenen Gästen im Netzwerk.

Für Fortgeschrittene: Nutze starke WPA3-Verschlüsselung und trenne IoT-Geräte in ein eigenes Netzwerk.

Verwende unterschiedliche E-Mail-Adressen:

Nutze eine separate E-Mail-Adresse für Games oder soziale Medien, um deine wichtigsten Konten zu schützen.

Daten prüfen und löschen: Nutze Dienste wie „Have I Been Pwned?“ und lösche unnötige alte Accounts.

Zusatz-Tipp für Eltern und Jugendliche

Schaut euch die Liste gemeinsam an und setzt die Maßnahmen Schritt für Schritt um. So bleibt niemand allein und die Sicherheit wächst Stück für Stück.

Du willst voll der Pro sein und angeben?

DNS-Filter nicht nur am Handy nutzen: Dienste wie Quad9 oder OpenDNS blockieren bekannte gefährliche Webseiten automatisch.

Firmware-Updates beachten: Aktualisiere nicht nur dein Smartphone oder PC, sondern auch Geräte wie Router, Smart-TVs und IoT-Geräte.

Browser-Isolation für sensible Aufgaben: Nutze separate Browser oder „Sandbox"-Funktionen, um Online-Banking oder Einkäufe sicherer zu gestalten.

Externe Medien sichern: Verschlüssele USB-Sticks oder externe Festplatten mit Tools wie BitLocker oder VeraCrypt.

Cloud-Dienste richtig nutzen: Bevorzuge „Zero-Knowledge"-Anbieter, die deine Daten verschlüsseln.

Auf KI-Plattformen achtsam sein: Gib keine vertraulichen Daten in ChatGPT oder andere KI-Tools ein.

Standard-Passwörter ändern: Ändere die Werkseinstellungen bei Smart-Geräten sofort. Insbesondere bei allem, was dir als Smart-Home verkauft wird.

Sicherheits-Score-Tools verwenden: Lass deinen Sicherheitsstatus von Diensten wie Microsoft oder Dashlane analysieren.

Hinweis:

Die genannten Beispiele dienen lediglich der Veranschaulichung und stellen keine Produktempfehlungen dar. Es gibt viele Alternativen auf dem Markt – wähle die, die am besten zu deinen Bedürfnissen passt!

Verlag:
eTransfusion
Michael Bätscher
Buchenweg 10
79664 Wehr
eTransfusion.de