Leseprobe

POLIZEI
DEIN PARTNER
Gewerkschaft der Polizei



Sicher im Netz: Schütze Dich!

www.vdp-polizei.de



Sicher im Netz: Schütze Dich!

POLIZEI DEIN PARTNER
Gewerkschaft der Polizei

Impressum

Verantwortlich für den redaktionellen Teil:
pressto GmbH – agentur für medienkommunikation, Köln

Foto Titel/Innentitel: Drobot Dean/stock.adobe.com

Nachdruck des redaktionellen Teils nur nach ausdrücklicher Genehmigung des Herausgebers.

Sämtliche hier veröffentlichte Anzeigen, die im Kundenauftrag für die Drucklegung vom Verlag gestaltet wurden, sind urheberrechtlich geschützt. Nachdruck, Vervielfältigung und elektronische Speicherung ist nur mit Zustimmung des Anzeigenkunden und des Verlages erlaubt. Verstöße hiergegen werden vom Verlag, auch im Auftrag des Anzeigenkunden, unnachsichtig verfolgt.

Der Verlag behält sich die Verwertung der urheberrechtlich geschützten Inhalte dieses Werkes für Zwecke des Text- und Data-Minings nach § 44b UrhG ausdrücklich vor. Jegliche unbefugte Nutzung ist hiermit ausgeschlossen.

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Anzeigenverwaltung
Ein Unternehmen der Gewerkschaft der Polizei

Forststraße 3 a • 40721 Hilden
Telefon 0211 7104-0 • Telefax 0211 7104-174
av@vdp-polizei.de

Geschäftsführer: Dominik Lehmanns
Anzeigenleiterin: Antje Kleuker

Gestaltung und Layout: Sandra Storchmann

Anzeigensatz und Druck:

© 2026

012-2026-000

www.vdp-polizei.de

Rundum sicher im Netz x
Surfen und mailen – aber sicher! x
Wie schütze ich meine Daten? x
Die richtige Absicherung x
Smart Home – sicher vernetzt x
Prävention kompakt – Cybercrime spezial x
Digital im Netz einkaufen und bezahlen x
Einflussnahme und Desinformation x
Sicherheit im Umgang mit Künstlicher Intelligenz x
Urheberrechte gelten für jeden x
Social Selling und Fake-Produkte auf Social Media-Kanälen x
Soziale Netzwerke: 10 Tipps für den Schutz Ihrer Daten x
Phishing erkennen und richtig reagieren x

Special für Kids:
10 Dinge, die du wissen musst x

Tipps für Eltern und Lehrer x

Rundum sicher im Netz

Die Nutzung digitaler Medien hat unser Leben in den letzten Jahrzehnten radikal verändert. Heute nutzen 95 Prozent der Deutschen ab 14 Jahren zumindest ab und zu das Internet. Täglich sind 69 Prozent der Bevölkerung online unterwegs, und zwar im Durchschnitt fünf Stunden und 22 Minuten. Wie das Statistische Bundesamt mitteilt, gaben im Jahr 2024 gut 83 Prozent der Bevölkerung im Alter von 16 bis 74 Jahren an, schon einmal etwas im Internet gekauft oder bestellt zu haben. Dieser Trend soll sich fortsetzen. Im Jahr 2029 soll die Zahl der Menschen, die regelmäßig online einkaufen, schätzungsweise 51,77 Millionen Nutzer betragen und damit einen neuen Höchststand erreichen. Die vielen digitalen Möglichkeiten sorgen aber auch dafür, dass Cyberkriminelle versuchen, an Daten oder Geld zu gelangen: Durch Cybercrime entstehen Schäden in Milliardenhöhe. Insgesamt erfasste die Polizei im vergangenen Jahr 131.391 Fälle von Cybercrime – ein leichter Rückgang von 2,2 Prozent im Vergleich zu 2023.

Damit Sie sicher im Netz unterwegs sind, liefert Ihnen dieses Heft nützliche Anregungen und hilfreiche Tipps: Worauf muss ich achten, wenn ich online unterwegs bin? Was sind aktuelle Betrugsmaschen und wie kann man sich davor schützen? Ein Experte vom Landeskriminalamt Niedersachsen erklärt uns, wie man WLAN, Rechner und Smartphone richtig absichert. Auch das Thema „Smart Home“ boomt. Was man beachten sollten, wenn man Smart-Home-Technologie einsetzt, das erläutert Martin Meingast von der Initiative „Deutschland sicher im Netz (DsiN)“. Mit den sozialen Medien sind außerdem Fake-Profile ein Teil unseres digitalen Alltags geworden. Sie werden von Betrügern erstellt, um Daten zu stehlen, Aktivitäten menschlicher Nutzer vorzutäuschen oder Menschen politisch zu beeinflussen. Sie erfahren in diesem Heft, wie Sie gefälschte Accounts besser erkennen und was Sie dagegen unternehmen können. Durch den Einsatz künstlicher Intelligenz (KI) ist es für Angreifer einfacher geworden, uns zu manipulieren und zu betrügen. Welche potenziellen Gefahren gibt es und wie kann man sicher mit KI umgehen? Wir geben Ihnen Antworten. Eine weitere Gefahr in den sozialen Medien sind Werbeanzeigen für gefälschte Produkte, die auf den Social Media-Kanälen von Influencerinnen und Influencern gezielt beworben werden. Eine Expertin des Verbraucherzentrale Bundesverbands verrät, wie Sie Fakeshops von seriösen Angeboten unterscheiden können. Außerdem geben wir Ihnen nützliche Tipps, was Sie tun können, wenn Sie trotz aller Vorsicht Opfer von Cybercrime geworden sind.

Nur die Wenigsten können oder wollen heute noch auf die digitale Kommunikation verzichten. Damit man sicher in der digitalen Welt unterwegs ist, muss man aber auch selbst Verantwortung übernehmen und die richtigen Entscheidungen treffen. Dabei möchten wir Sie unterstützen!

Eine anregende Lektüre wünscht Ihnen
Ihre Redaktion



tadamichi/stock.adobe.com

Soziale Netzwerke:

10 Tipps für den Schutz Ihrer Daten

Über Dienste wie Facebook oder Telegram kann man sich mit Freunden austauschen, Urlaubsfotos hochladen oder eine Veranstaltungsgruppe für die nächste Geburtstagsparty erstellen. Auch wenn diese Funktionen praktisch sind, sollte man gut überlegen, mit wem man sich vernetzt und was man veröffentlicht. Denn im Zweifel können die Infos von Kriminellen ausgenutzt werden, beispielsweise von Einbrechern, die dann ganz genau wissen, dass man gerade nicht zuhause ist. Auch Cyberkriminelle greifen immer wieder auf diese Kanäle zurück, um Schadsoftware zu verbreiten oder Nutzerdaten abzuschöpfen. Damit Sie die Kontrolle über Ihre Daten behalten, sollten Sie einige Hinweise beachten:

1 Lesen Sie die Allgemeinen Geschäftsbedingungen (AGB) und Datenschutzbestimmungen aufmerksam durch, bevor Sie sich ein Profil anlegen. Dadurch wissen Sie, was hier mit Ihren Daten passiert.

2 Verwenden Sie unterschiedliche Passwörter für jeden Dienst. Hinweise, wie ein sicheres Passwort aussieht, finden Sie in diesem Heft.

3 Aktivieren Sie alle Einstellungen, die Ihre Privatsphäre schützen. Dazu gehört, dass Personen, mit denen Sie nicht vernetzt sind, Inhalte nicht sehen können. Zudem ist es bei manchen Diensten möglich, dass das Profil von Dritten nicht über die Plattform selbst oder über Suchmaschinen gefunden werden kann.

4 Überlegen Sie genau, mit wem Sie sich „anfreunden“. Jeder Kontakt kann Ihre Inhalte sehen, sofern Sie dies nicht einschränken. Im besten Fall vernetzten Sie sich nur mit Personen, die Sie aus der „Offline-Welt“ kennen.

5 Das Netz vergisst nichts! Prüfen Sie kritisch, welche Informationen Sie veröffentlichen wollen und schränken Sie den Empfängerkreis ein. Je weniger personenbezogene Daten Sie veröffentlichen, desto besser.

6 Bei einigen Diensten übertragen Sie die Nutzungsrechte an Ihren Fotos und Videos an den Betreiber. Das gilt auch meist dann noch, wenn Sie das Netzwerk verlassen und Ihr Profil deaktivieren. Überlegen Sie also vor jeder Veröffentlichung, ob Sie die Rechte an diesem Inhalt teilen möchten.

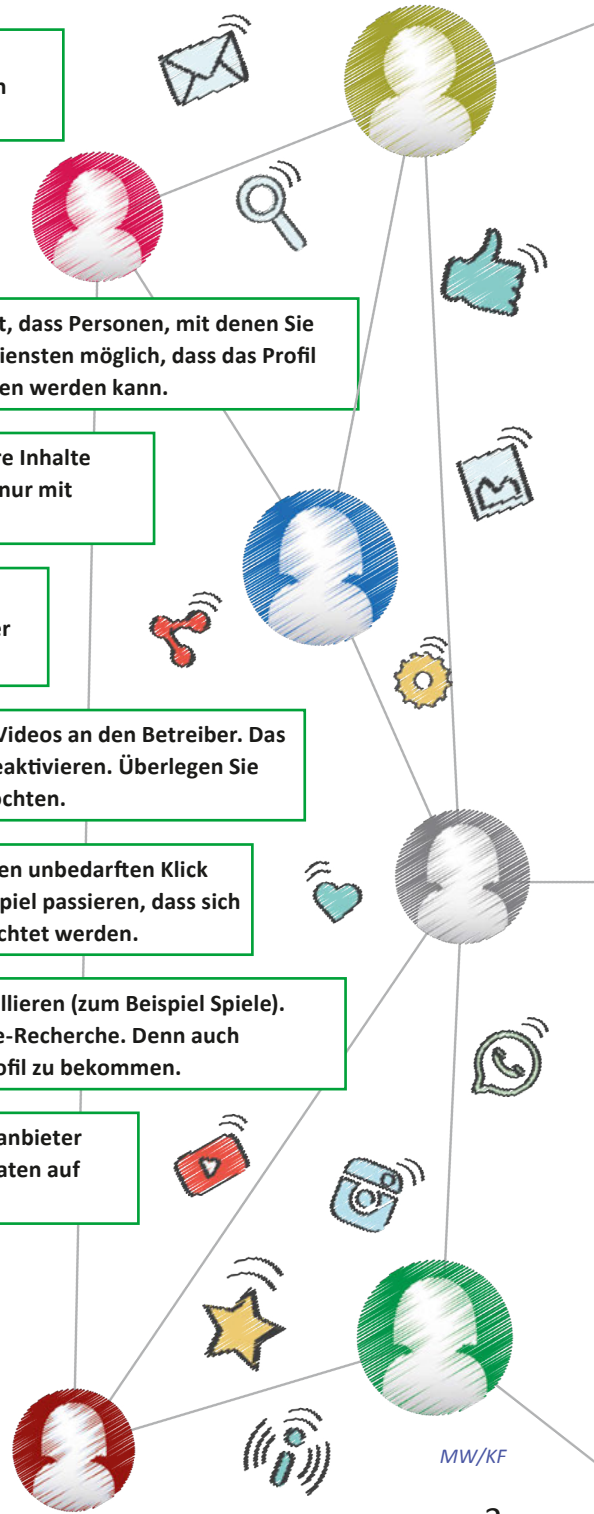
7 Achten Sie genau darauf, welche Links oder Buttons Sie anklicken. Durch einen unbedarften Klick kann man sich schnell Schadsoftware herunterladen. Dann kann es zum Beispiel passieren, dass sich die Kamera an Ihrem Computer oder Smartphone einschaltet und Sie beobachtet werden.

8 Viele soziale Netzwerke erlauben, Anwendungen von Drittanbietern zu installieren (zum Beispiel Spiele). Prüfen Sie diese auf Vertrauenswürdigkeit, beispielsweise durch eine Google-Recherche. Denn auch Kriminelle erstellen oder hacken solche Anwendungen, um Zugriff auf Ihr Profil zu bekommen.

9 Für die Nutzung per Smartphone oder Tablet stellen die Betreiber oder Drittanbieter Apps zur Verfügung. Kontrollieren Sie, welchen Zugriff diese Apps auf Ihre Daten auf dem mobilen Endgerät haben (zum Beispiel Kontakte).

10 Wenn Sie belästigt oder beleidigt werden, sollten Sie dies dem Betreiber melden. Unseriöse Profile werden gelöscht. Bei offensichtlichen oder vermuteten Straftaten sollten Sie sich auch an die Polizei wenden.

! Weiterführende Hinweise finden Sie auf der Unterseite „Verbraucherinnen und Verbraucher“ auf der Website des Bundesamts für Sicherheit in der Informationstechnik https://www.bsi.bund.de



MW/KF