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: rimmdream/stock.adobe.com

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: Bodo Andrae, Joachim Kranz
Anzeigenleiterin: Antje Kleuker

Gestaltung und Layout: Jana Kolfhaus

Anzeigensatz und Druck:
Wölfer Druck + Media, Haan

12/2018/xx

www.vdp-polizei.de

Das Vertrauen in die IT-Sicherheit ist elementar x
Surfen und kommunizieren – aber sicher! x
Wie schütze ich meine Daten? x
Die richtige Absicherung
Sicherheit auf dem Prüfstand x
Prävention kompakt – Cybercrime spezial x
Sicher im Netz einkaufen und bezahlen x
Urheberrechte gelten für jeden x
Soziale Netzwerke: 10 Tipps für den Schutz Ihrer Daten x
Phishing, Trojaner, Identitätsdiebstahl? x
Die Arbeit der Cybercrime-Experten des BKA

Special für Kids:
Klartext zu Surfen, Chatten, Social Media x
10 Dinge, die du wissen musst x
Teste dein Wissen – mach den Internet-Führerschein x

Tipps für Eltern und Lehrer x

Das Vertrauen in die IT-Sicherheit ist elementar

Die Nutzung digitaler Medien hat unser Leben in den letzten Jahrzehnten radikal revolutioniert. Heute nutzen 81 Prozent der Deutschen das Internet, und zwar 149 Minuten im Schnitt an jedem Tag des Jahres (Quelle: statista)! 53,59 Millionen Menschen in Deutschland kaufen online ein. 81 Prozent der Befragten gaben an, in den vergangenen 30 Tagen einen Online-Händler besucht zu haben. Während 72 Prozent sagten, ein Produkt oder eine Dienstleistung online erworben zu haben, waren es immerhin 26 Prozent, die dies über ein mobiles Endgerät getan haben (Quelle: Digital Report 2017). Ganz offensichtlich ist dieser Wandel auch im öffentlichen Raum: Die meisten Menschen sind in Bussen und Bahnen mit ihrem Smartphone beschäftigt und es gibt täglich und überall Beinahe-Zusammenstöße mit „Smombies“, also mit Menschen, die während des Gehens auf ihr mobiles Gerät starren.

Zwei Ereignisse haben zuletzt erneut klar gemacht, dass mit der Nutzung digitaler Medien nicht nur Chancen, sondern auch Risiken einhergehen:

Die im Mai 2018 in Kraft getretene europäische Datenschutzgrundverordnung (DSGVO) hat viele Unternehmen und Vereine nachdrücklich auf das Thema IT-Sicherheit aufmerksam gemacht: Im Zentrum der Verordnung steht der Schutz personenbezogener Daten. Dabei wurde das Recht der Bürger erweitert, zu erfahren, was mit ihren Daten passiert. Der Umgang mit personenbezogenen Daten wird sich durch die DSGVO verbessern – doch dies ist nur ein Aspekt des Themas „Sicher im Netz“. Das Thema ist für Privatpersonen ebenso wichtig wie für Unternehmen. Das wurde auch bei diversen Datenlecks und den zwielichtigen Geschäftspraktiken großer Social-Media-Plattformen wie etwa Facebook deutlich. Das führte dazu, dass sich einige Menschen sogar ganz aus den Sozialen Medien zurückziehen. Damit stehen nicht nur Geschäftsmodelle von weltweit agierenden Internetunternehmen auf dem Spiel, sondern auch unsere alltägliche digitale Kommunikation: unsere Chats und unsere Einkäufe im Internet. Vertrauen ist eine harte Währung – und davon wurde in letzter Zeit viel verspielt. Das birgt auch Risiken für die Einführung neuer digitaler Technologien, etwa beim bargeldlosen Bezahlen.

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. Nicht alles, was bequem und funktional ist, ist auch sicher. Um gegen die IT-Sicherheitsrisiken von heute gewappnet zu sein, helfen Ihnen die Tipps in diesem Heft. In einem Glossar erklären wir die wichtigsten Fachbegriffe. Wir klären über Gefahren im Netz auf – und wie man mit ihnen umgeht. Wir zeigen Ihnen, wie Sie Ihre Daten richtig schützen. Wir sagen Ihnen, was Sie tun können, wenn Sie trotz aller Vorsicht Opfer von Cybercrime geworden sind. Abgerundet wird das Heft durch Tipps für Kinder und Jugendliche, Lehrer und Eltern.

Eine anregende Lektüre wünscht Ihnen

Ihre Redaktion

Soziale Netzwerke: 10 Tipps für den Schutz Ihrer Daten

Über Dienste wie Facebook oder Twitter 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.

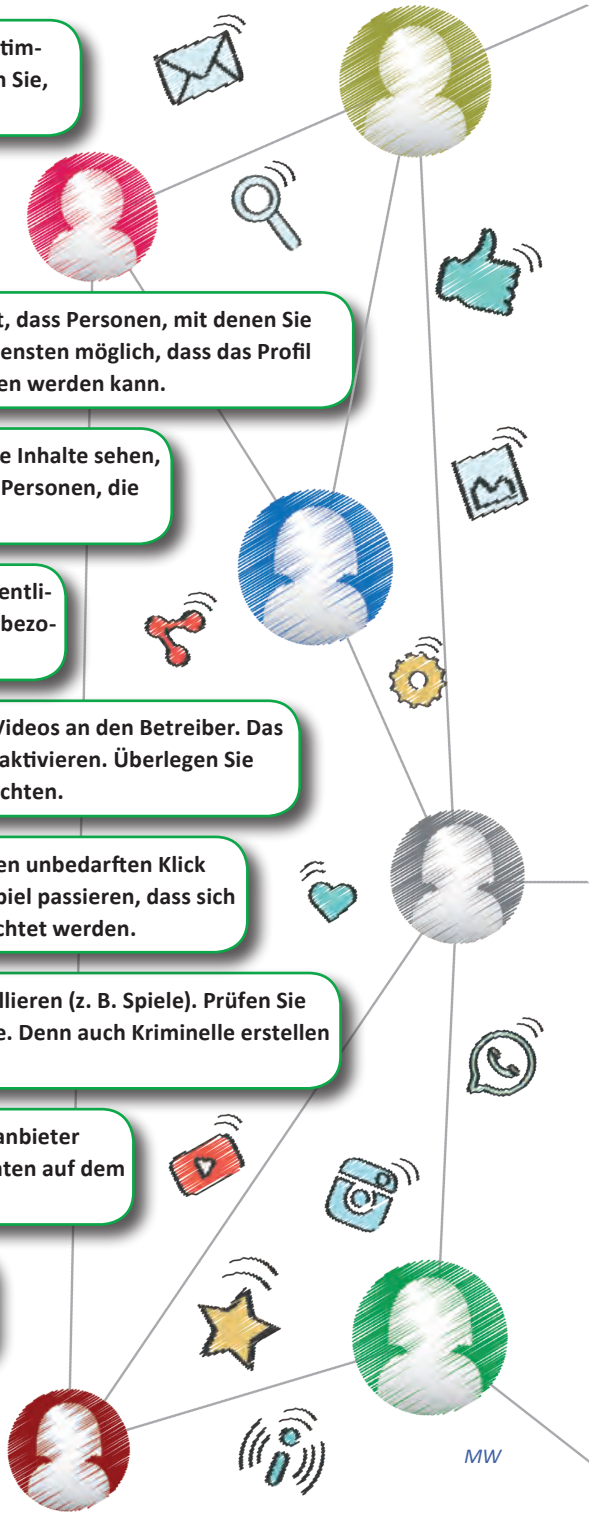
7. Achten Sie genau darauf, welche Links oder Buttons Sie anklicken. Durch einen unbedarften Klick kann man sich schnell Schadsoftware herunterladen. Dann kann es zum Beispiel passieren, dass sich die Kamera an Ihrem Computer oder Smartphone einschaltet und Sie beobachtet werden.

8. Viele soziale Netzwerke erlauben, Anwendungen von Drittanbietern zu installieren (z. B. 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 (z. B. 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 dem Portal „BSI für Bürger“ (www.bsi-fuer-buerger.de), einem Angebot des Bundesamts für Sicherheit in der Informationstechnik.



MW