WEISSER RING

Wir helfen Kriminalitätsopfern.

–HACKED–

Mit Highspeed kriminell

Alles über die Gefahren aus dem Web und wie Sie sich davor schützen

Inhaltsverzeichnis

Schöne smarte Welt und ihre Schattenseiten 3
Phishing: Gemeiner Datenklau 4
Identitätsdiebstahl: Das bin ich nicht 6
Datendiebstahl durch Social Engineering: Einfach menschlich 8
CEO Fraud: Der falsche Chef 9
Cybermobbing: Endlose Schikanen im Netz 10
Cyberstalker: Nachgestellt im Netz 12
Cybergrooming: Perverse Masche 13
Die vier besten Sicherheits-Tipps für soziale Medien 14
Fake-Shops: Typisch mit Vorkasse 16
Schadprogramme / Malware: Rundum kriminell 17
Sicher auf der Datenautobahn unterwegs: Tipps fürs Web 18
Smart Home: Für ein smartes, aber sicheres Zuhause 20
Glossar: Die wichtigsten Begriffe kurz erklärt 22
Ob online oder offline: Jede Spende zählt 23

Schöne smarte Welt und ihre Schattenseiten

Ob Onlineshopping, Bankgeschäfte erledigen, Urlaub buchen oder mit Freunden die neuesten Schnappschüsse teilen — das Internet macht alles möglich. Schnell und bequem per Smartphone, Tablet oder Computer. In Deutschland nutzen rund 62 Millionen Menschen* die smarten Vorteile des World Wide Webs.

Doch im digitalen Raum lauern zahlreiche Gefahren und trickreiche Cyberkriminelle, die jede mögliche Schwachstelle ausnutzen. Die Zahlen bestätigen es: Jeder zweite Internetnutzer** wurde bereits Opfer von Cyberkriminalität. In 50% der Fälle entstand finanzieller Schaden. Angezeigt werden dabei die wenigsten Verbrechen. 2017 zählte die Polizei nur ca. 194.000 Fälle von Computerkriminalität und -betrug***.

* ARD/ZDF-Onlinestudie 2017 ** Bitkom-Studie Okt. 2016 *** BKA Polizeiliche Kriminalstatistik 2017

Wissen ist die beste Prävention

Wir vom WEISSEN RING erleben es täglich selbst. Immer mehr Opfer von Internetkriminalität wenden sich an uns. Dazu gehören z. B. Fälle von Cybermobbing, unter dem besonders Jugendliche leiden. Den Cyberkriminellen ins Netz zu gehen, kann leider jeden treffen.

Nachfolgend haben wir für Sie die häufigsten Internetdelikte zusammengetragen, mit authentischen Fallbeispielen und praktischen Sicherheitstipps. Denn Wissen ist der beste Schutz, um nicht selbst zum Opfer zu werden.

Phishing: Gemeiner Datenklau

Täuschend echt wird echt zum Problem

Motorräder sind seine Welt. Christian S. bekam von seinem Lieblingsmotorradshop eine E-Mail und wurde aufgefordert, seine Kundendaten zu aktualisieren. Nichts Böses ahnend, klickte er auf den Link, füllte das Formular auf der scheinbar echten Website aus und gab natürlich seine Bankverbindung an. Ein fataler Fehler, es war eine Phishing-Mail. Von seinem Konto wurden kurz danach mehrere Beträge abgebucht. Der finanzielle Schaden: fast fünfstellig.

Was macht Phishing so gefährlich?

Durch das „Abfischen“ von sensiblen Daten wie Passwörtern, Adress- und Bankdaten, TANs, PINs, Kreditkartennummern können die Betrüger finanziellen Schaden verursachen oder sogar Identitätsdiebstahl begehen. Um die Opfer zu ködern, verschicken die Täter gefälschte, täuschend echt aussehende E-Mails bzw. Links zu Websites im Namen von seriösen Banken, Versandhändlern und Unternehmen. Oft wird den E-Mail-Empfängern auch vorgegaukelt, ihr Konto werde bei Nichtbefolgung gesperrt. Beim Onlinebanking ist Phishing besonders häufig.

Wie können Sie sich schützen?

- Lassen Sie sich nicht täuschen, achten Sie auf die E-Mail-Adresse des Absenders und die korrekte Schreibweise. Oft werden Phantasieadressen verwendet mit kryptischen Buchstaben oder falschen Umlauten.
- Auch der Link der gefälschten Websites verrät die Betrüger. Sichere Websites erkennen Sie am „s“ bei https://...
- Generell gilt: Vertrauenswürdige Informationen, wie z. B. Kontodaten oder TANs, werden von Banken und Unternehmen nicht per Mail abgefragt.

© iStockphoto

Identitätsdiebstahl: Das bin ich nicht

Ein anderer benutzt Ihr Profil

Wie jeden Tag checkte Rhena H. kurz ihr Facebookprofil und erschrak. Unter ihrem Namen hatte ein Unbekannter zahlreiche, gehässige Kommentare hinterlassen, auch bei Arbeitskollegen, und zudem brutale Videos gelikt. Außerdem verschickte der Täter persönliche Nachrichten an ihre Freunde, die Links mit Schadsoftware enthielten. Zum Glück bemerkte eine Freundin diesen Betrug rechtzeitig und konnte die anderen warnen.

Was macht Identitätsdiebstahl so gefährlich?

Name, Adresse und Geburtstag: Persönliche Daten sind für Betrüger eine lohnenswerte Beute.
Dazu gehören auch die private E-Mail-Adresse, die Handynummer, Login-Daten, Profildaten für soziale Medien etc. Mit diesen sensiblen Daten kann man nicht nur die betreffende Person schädigen und Rufmord begehen, sondern mit der geklauten Identität Onlinekäufe tätigen und sich bereichern.

Wie können Sie sich schützen?

- Gehen Sie in den sozialen Medien sparsam mit persönlichen Daten um und achten Sie auf Phishing-Mails.
- Verwenden Sie bei verschiedenen Plattformen unterschiedliche Nutzernamen und wechseln Sie regelmäßig Ihre Passwörter.
- Weitere Tipps finden Sie auf den Seiten 14 / 15.

© iStockphoto

Datendiebstahl durch Social Engineering: Einfach menschlich

Wenn Leichtgläubigkeit raffiniert ausgenutzt wird

Aus der IT-Abteilung kommt ein Anruf. Der Rechner von Bianca T. braucht dringend ein Update, dafür benötigt der IT-Verantwortliche jedoch ihr Passwort. Da Bianca T. gleich zum Meeting muss, sagt sie ohne nachzudenken ihr zehnstelliges Passwort durch. Was sie nicht weiß: Der Anrufer ist ein Betrüger und will sich Zugang ins Unternehmensnetzwerk verschaffen, um Schadsoftware einzuschleusen.

© iStockphoto

Was macht Social Engineering so gefährlich?

Hier nutzt der Angreifer die Schwachstelle Mensch aus. Die Täter treten mit ihren Opfern in direkten Kontakt, sei es per Mail, per Telefon oder auf persönlichem Wege. Hemmungslos gaukeln sie ihrem ahnungslosen Gegenüber etwas vor, geben sich z. B. als Vorstand oder Chef aus, als Netzwerk-Administrator oder Techniker einer Firma. Ihr Ziel: an vertrauliche Informationen zu kommen, Sicherheitsfunktionen zu übergehen und Passwörter zu erbeuten.

Wie können Sie sich schützen?

- Teilen Sie niemals Passwörter oder sensible Daten per Telefon oder E-Mail mit.
- Gehen Sie in den sozialen Medien sparsam mit persönlichen Daten um, auch, was Ihre Arbeitsstelle betrifft.
- Weitere Tipps finden Sie auf den Seiten 14 / 15.

CEO Fraud: Der falsche Chef

Geschäftsmasche: Überweisungen anweisen

Mittwochnachmittag, per Mail wurde die Buchhalterin Anne S. vom Vorstandsvorsitzenden des Transportunternehmens beauftragt, eine größere Summe ins Ausland zu überweisen. Das war nicht unüblich. Zwar war Anne S. etwas irritiert über die Höhe der sechsstelligen Summe, aber sie leitete die Zahlung sofort in die Wege. Schließlich ging es um eine wichtige Investition. Problem: Der Auftrag kam nicht von ihrem echten Chef.

Was macht CEO Fraud so gefährlich?

Es ist der große finanzielle Verlust, den Unternehmen erleiden. Mithilfe von Identitätsdiebstahl geben sich die Betrüger als Vorstand, Geschäftsführer oder Führungskraft aus und veranlassen Mitarbeiter, hohe Überweisungen auf ausländische Konten zu tätigen, meist nach China. Die Täter haben vorher aufwändig Adressen und Mitarbeiter im Netz ausgespäht und wissen um firmeninterne Abläufe.

Wie können Sie sich und das Unternehmen schützen?

- Nur wenig allgemeine Kontaktdaten und Interna des Unternehmens veröffentlichen, besonders in den sozialen Medien, auf der Homepage und in Wirtschaftsberichten.
- Mitarbeiter über die Betrugsform CEO Fraud aufklären und Schutzmechanismen bei höheren Summen einrichten.
- Die entsprechende E-Mail-Adresse stets auf die korrekte Schreibweise überprüfen und größere Aufträge entsprechend verifizieren.

Cybermobbing: Endlose Schikanen im Netz

Vom Schulhof in die digitale Welt und zurück

Seit Wochen leidet die 16-jährige Schülerin Jana P. unter gemeinen Cybermobbing-Attacken, ausgelöst durch ein harmloses Partyfoto auf Instagram. In WhatsApp-Gruppenchats und in den sozialen Medien wird sie von Mitschülern und fremden Personen fies attackiert, beleidigt und bloßgestellt. Die Schülerin weiß nicht mehr weiter. Ob zu Hause oder in der Schule, Hunderte von Nachrichten kommen bei ihr rund um die Uhr auf dem Smartphone an. Die Scham ist zu groß, um sich jemandem anzuvertrauen.

Was macht Cybermobbing so gefährlich?

Cybermobbing läuft wie klassisches Mobbing über einen langen Zeitraum und setzt den Betroffenen massiv zu. Seelisch wie körperlich. Es dringt zudem in die Privatsphäre ein und lässt den Opfern keine Pause, auch nicht zu Hause im Kinderzimmer. Größtenteils sind Kinder und Jugendliche zwischen 12 und 19 Jahren betroffen, aber auch Lehrer und Erwachsene werden im Privatleben oder in der Arbeitswelt zur Zielscheibe gemeiner Lästereien. Cybermobbing ist eine Straftat, gegen die man sich juristisch wehren kann. Beleidigendes Material zu sichern, z. B. mit der NO STALK App vom WEISSEN RING (voraussichtlich erhältlich ab Anfang 2019), ist unerlässlich.

Wie kann man sich davor schützen?

- Wenig Angriffsfläche bieten und in den sozialen Medien sparsam mit persönlichen Inhalten umgehen.
- Weitere Tipps finden Sie auf den Seiten 14 / 15.

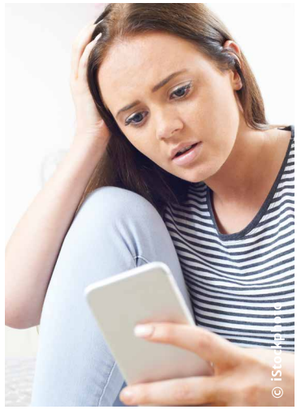
Cyberstalker: Nachgestellt im Netz

Im digitalen Raum nirgendwo sicher vor ihm

Céline S. weiß bis heute nicht, wer es ist, der sie im und über das Internet terrorisiert. Angefangen hat ihre Leidensgeschichte in Facebook, als ein Unbekannter kompromittierende Nachrichten über ihr Privatleben postete. Erst in großen Abständen, dann nahezu täglich. Kurze Zeit später begann auch das mit den Paketen, die der anonyme Täter online auf ihren Namen bestellte und sowohl an ihre private Adresse als auch ins Büro liefern ließ. Woher hatte er all die Informationen?

Was macht einen Cyberstalker so gefährlich?

Verfolgt und belästigt: Für die Betroffenen ist ein Cyberstalker eine große psychische Belastung. Rund um die Uhr können sie online attackiert bzw. geschädigt werden. Der Täter agiert anonym, versteckt sich hinter falschen Profilen oder Konten, so dass sein Opfer nicht weiß, wer er ist. Auch Spionageprogramme kommen zum Einsatz, um dem Opfer das Leben schwer zu machen. Beweise zu sichern, z. B. mit der NO STALK App vom WEISSEN RING (voraussichtlich erhältlich ab Anfang 2019), ist wichtig, um sich juristisch zur Wehr zu setzen.



Wie können Sie sich davor schützen?

- Wenig Angriffsfläche bieten und in den sozialen Medien sparsam mit persönlichen Inhalten umgehen.
- Weitere Tipps finden Sie auf den Seiten 14 / 15.

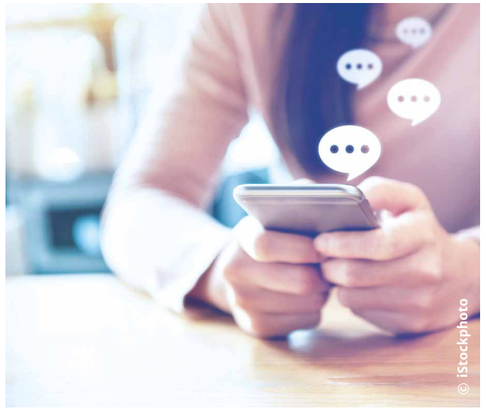
Cybergrooming: Perverse Masche

Kinder online anbaggern und bedrängen

Die 11-jährige Hanna O. spielte auf dem Smartphone ihr Lieblingsonlinespiel, als sie von einer Marie13 angeschrieben wurde. Im Chat tauschten sich die Mädchen etwas aus, plauderten über Jungs und Schule, bis Marie13 fragte, ob sie ihr ein Nacktfoto von sich schicken könnte. Hanna O. war entsetzt. Das ging zu weit.

Was macht Cybergrooming so gefährlich?

Meist in Chats kontaktieren ältere Männer Kinder und Jugendliche und geben vor, gleichaltrig zu sein. Ihr Ziel: Vertrauen aufbauen, um ihre minderjährigen Opfer später zu sexuellen Handlungen zu bringen und in der realen Welt zu missbrauchen. Oft werden die Kinder auch aufgefordert, Fotos zu schicken, sexuelle Handlungen an sich vorzunehmen oder sie bekommen pornografisches Material zugesendet. Wichtig zu wissen: Schon die onlinebasierte Anbahnung zum sexuellen Missbrauch ist strafbar.



Wie kann man sich davor schützen?

- In Chats am besten einen Nickname verwenden, der wenig über das Alter, das Geschlecht und den echten Namen verrät.
- Keine intimen bzw. privaten Fotos oder anderes Material an angeblich gute Freunde im Netz verschicken.

Die vier besten Sicherheits-Tipps für soziale Medien

Sich austauschen, im Gespräch bleiben oder das Netzwerk vergrößern: Jeder Zweite in Deutschland nutzt regelmäßig soziale Netzwerke wie Facebook, Twitter, Instagram oder die beruflichen Plattformen wie Xing bzw. Linkedin. Die folgenden vier Tipps sorgen für mehr Sicherheit in den sozialen Medien.

1 ***Seien Sie sparsam mit persönlichen Daten***
Das Internet vergisst nichts. Weder Textbeiträge noch Fotos, Videos oder andere Inhalte. Überlegen Sie sich genau, welche Daten Sie in den sozialen Netzwerken oder im Netz teilen. Auch hier gilt: Weniger ist mehr und Privates sollte privat bleiben. Vertrauliche Infos über Ihre Arbeit gehören hier ebenfalls nicht hin.

2 ***Schützen Sie Ihre Privatsphäre***
In den Privatsphäre-Einstellungen der entsprechenden Plattform können Sie selbst festlegen, wer Ihr Profil sehen darf und wer nicht. Definieren Sie einen eher kleinen Personenkreis, um die Kontrolle über Ihre Daten zu behalten.

3 ***Clever und sicher: Unterschiedliche Passwörter***
Verwenden Sie unterschiedliche und sichere Passwörter für Ihre Profile in den sozialen Netzwerken. Und ändern Sie diese regelmäßig. Ein sicheres Passwort besteht aus mindestens acht Zeichen und enthält eine Kombination aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Bitte keine Namen oder Geburtsdaten verwenden. Passwörter sollten auf keinen Fall an Dritte weitergegeben werden.

4 ***Mehr Misstrauen bitte!***
Seien Sie misstrauisch bei Anfragen von Unbekannten und prüfen Sie kritisch den Absender. Denn hinter falschen bzw. unseriösen Profilen können sich Cyberkriminelle verstecken. Vermeiden Sie es, Links oder Downloads anzuklicken oder sensible Daten von sich preiszugeben. Melden Sie Auffälligkeiten umgehend bei den Seitenbetreibern.

© iStockphoto

Fake-Shops: Typisch mit Vorkasse

Bestellt, bezahlt und leer ausgegangen

Alice C. wollte nur schnell das Lieblingsparfüm ihrer Freundin bestellen, der Geburtstag war schon am Wochenende. Sie googelte kurz und fand einen seriös wirkenden Onlineshop, der durch sein gutes Preis-Leistungs-Verhältnis überzeugte. Alice C. bestellte, bezahlte mit Kreditkarte und wartet leider bis heute auf das Produkt. Denn der Shop war ein Fake-Shop.

Was ist an einem Fake-Shop gefährlich?

In Anlehnung an bekannte Marken- und Onlineshops richten Betrüger unter ähnlichen Web-Adressen sogenannte Fake-Shops ein. Hier bieten sie hochwertige Markenprodukte zu einem günstigen Preis an, natürlich nur gegen Vorkasse. Geliefert wird das bestellte Produkt in den meisten Fällen nicht oder es wird minderwertige Ware verschickt. Problematisch: Neben dem erlittenen finanziellen Verlust werden in diesen Fake-Shops auch Kontodaten erbeutet.

Wie können Sie sich schützen?

- Vermeiden Sie Spontankäufe und achten Sie auf die genaue Web-Adresse. Sichere Online-Verbindungen erkennen Sie am „s“ in https://... Außerdem haben geprüfte Onlineshops eins der folgenden Gütesiegel.
- Seien Sie misstrauisch, wenn die Preise zu günstig sind und Vorkasse der einzige Zahlungsweg ist.
- Überprüfen Sie die Seriosität des Onlineshops.

Schadprogramme/Malware: Rundum kriminell

Programmiert, um Schaden anzurichten

Die E-Mail kam von einer alten Schulfreundin, die Peter Z. zum 20-jährigen Klassentreffen einlud. Peter Z. öffnete den Anhang und kurz danach ging auf dem Rechner des freien Journalisten nichts mehr. Weder Zugangsdaten noch Passwörter funktionierten. Alle Daten waren plötzlich verschlüsselt. Kein Zugriff, außer er bezahlte ein vierstelliges Lösegeld an einen anonymen Täter im Ausland.

Was macht Schadsoftware so gefährlich?

Ob beim Öffnen eines Downloads oder eines E-Mail-Anhangs, Schadsoftware kann sich unbemerkt in ein System einschleusen und schädliche Aktionen auslösen, wie z. B. Passwörter, sensible Daten oder Bankverbindungen ausspionieren und Fehlfunktionen verursachen. Schadsoftware ist auch unter dem Begriff Malware bekannt, ein Sammelbegriff für viele verschiedene Unterarten wie Trojaner, Bot-Netze, Würmer oder Viren. Letztere sind sich selbst reproduzierende Schadprogramme, die sich eigenständig weiterverbreiten, z. B. über einen USB-Stick, oder sie versenden sich selbst per Mail an das gesamte Mailadressbuch. Schadprogramme existieren nicht nur für Smartphones, Tablets und Co, sondern für viele internetfähige Geräte wie Smart-Home-Anwendungen.

Wie können Sie sich schützen?

- Keine E-Mail-Anhänge öffnen, die nicht angekündigt wurden.
- Aktuelle Anti-Viren-Software bzw. Virenscanner verwenden und eine Firewall einrichten.
- Einfach sicherer: Regelmäßig die neuesten Updates für Smartphone, Tablet und Rechner runterladen.

Sicher auf der Datenautobahn unterwegs: Tipps fürs Web

Das Wichtigste zuerst: Sie müssen selbst aktiv werden, um sich im digitalen Raum vor potenziellen Gefahren zu schützen. Die gute Nachricht: Die Technik hilft Ihnen dabei.

Nutzen Sie Updates und Software-Aktualisierungen

Jeder kennt das. Von Smartphone bis Rechner: Regelmäßige Updates der Hersteller sorgen dafür, dass Ihre Systeme nicht nur auf dem neuesten technischen Stand, sondern auch sicherer sind. Nicht zu vergessen: immer einen aktuellen Internetbrowser benutzen.

Stoppen ungebetene Gäste: Virenscanner & Co

Verwenden Sie Virenscanner oder eine Anti-Viren-Software, um Ihre Geräte vor Angriffen oder Eindringlingen zu schützen. Zusätzliche Sicherheitssoftware wie Firewalls sind ebenfalls sehr empfehlenswert.

Wichtig: Gute Passwörter

Auch wenn es schwerfällt: Benutzen Sie unterschiedliche Passwörter für unterschiedliche Anwendungen, z. B. für Ihr E-Mail-Programm, für soziale Netzwerke oder zum Onlineshoppen. Sichere Passwörter sind achtstellig und enthalten eine Kombination aus Groß- und Kleinbuchstaben sowie Zahlen bzw. Sonderzeichen. Und: sie sollten regelmäßig verändert werden.

Öffentliche WLAN-Netzwerke vermeiden

Ob am Bahnhof, Flughafen oder im Café: Vorsicht bei frei zugänglichen WLAN-Netzwerken bzw. Hotspots. Die Gefahr: Ihre Daten werden hier unverschlüsselt übertragen und können leicht abgefangen werden.

Auf der sicheren Seite

Gerade beim Onlineshoppen oder Onlinebanking sollten Sie darauf achten, dass Sie eine sichere Verbindung nutzen. Sie erkennen diese am „s“ in https://... und an dem kleinen Schloss-Symbol in der Adressleiste. Für Bankgeschäfte geben Sie am besten die Webadresse selbst in die Adresszeile ein.

Couragiert: Auffälligkeiten und Straftaten melden

Kriminelle Vorfälle oder den Verdacht darauf sollten Sie bei den Seitenbetreibern umgehend melden. Natürlich können Sie sich bei Cyberdelikten auch direkt an die Polizei wenden.

Ihr regelmäßiges Wissens-Update: Nützliche Webadressen

Aktuelle Informationen und neueste Entwicklungen zum Thema Cyberkriminalität finden Sie unter den folgenden Links: **www.bsi-fuer-buerger.de**
www.polizei-beratung.de
www.bka.de

© IStockphoto

Smart Home: Für ein smartes, aber sicheres Zuhause

Intelligent vernetzt, aber angreifbar

Von Rollläden, die sich früh Punkt 7 hochfahren, über intelligente Lautsprecher, die den Wetterbericht wiedergeben, bis hin zur Kaffeemaschine, die Ihren Lieblingskaffee aufsetzt: In immer mehr Haushalte sind smarte Produkte eingezogen, die den Alltag leichter und komfortabler machen.

Ein vernetztes Zuhause ist praktisch, birgt aber auch Risiken. Denn viele dieser Smart-Home-Anwendungen sind mit dem Internet verbunden — daher auch der Name Internet of Things (kurz: IoT) — und bieten ein Einfallstor für Cyberkriminelle und Hacker-Angriffe. Mit den folgenden Tipps können Sie Ihr Smart Home sicherer machen.

Sicherheit geht vor: Mit regelmäßigen Updates

Was fürs Smartphone und den PC gilt, hat auch für IoT-Produkte seine Gültigkeit. Achten Sie schon beim Kauf darauf, dass regelmäßige Sicherheitsupdates möglich sind und potenzielle Sicherheitslücken geschlossen werden. Auch sollte die Kommunikation der Geräte verschlüsselt sein.

So individuell wie Sie: Persönliche Passwörter

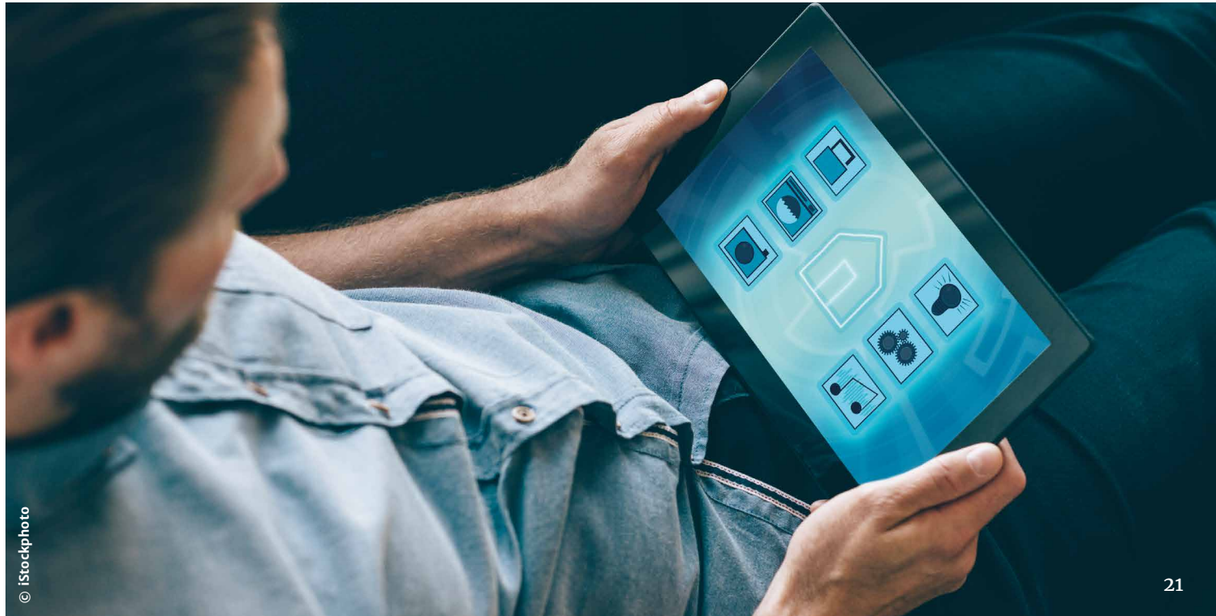
Viele IoT-Geräte haben voreingestellte Passwörter, wie z. B. „admin“ oder „root“. Ändern Sie das Standardpasswort durch ein individuelles, sicheres Passwort. Und verwenden Sie unterschiedliche Passwörter für verschiedene Geräte. Das macht Angreifern das Leben schwer.

Vernetzt, oft auch ohne Internet

Muss die Kaffeemaschine immer online sein? Nein, viele Geräte sind auch ohne ständige Internetverbindung funktionsfähig. Sollten Anwendungen von unterwegs angesteuert werden, empfiehlt sich die Einrichtung eines sicheren VPN-Netzwerkes.

Smart überwacht?

Die Sicherheitskamera hat Datenberge von Filmmaterial aufgenommen. Der Lautsprecher speichert alles, was man angefragt und bestellt hat. Datenschutz ist auch bei IoT-Anwendungen ein zentrales Thema. Brisant ist außerdem: Die gesammelten Daten können auch zur Überwachung missbraucht werden, z. B. Sicherheitskameras, die ungefragt den Babysitter filmen.



© iStockphoto

Glossar: Die wichtigsten Begriffe kurz erklärt

CEO Fraud Eine Betrugsmasche, bei der sich ein Täter als vermeintlicher Vorgesetzter oder Chef ausgibt, um z. B. Überweisungen zu veranlassen.

Cybergrooming Das ist die Anbahnung sexuellen Missbrauchs von Kindern und Minderjährigen im Internet, meist in Chats und Foren durch ältere Männer.

Cybermobbing Permanentes Belästigen, Bedrängen und Schikanieren eines anderen über das Internet, es findet größtenteils in den sozialen Medien und WhatsApp statt.

Cyberstalker Ein Unbekannter buhlt online um die Aufmerksamkeit eines anderen, terrorisiert ihn und stellt dem Betroffenen meist in den sozialen Medien nach.

Identitätsdiebstahl Wenn persönliche Daten wie z. B. Namen, Passwörter oder das Geburtsdatum gestohlen und die geklaute Identität für kriminelle Zwecke missbraucht wird.

Internet of Things Kurz IoT — das Internet der Dinge. Das sind intelligente, smarte Anwendungen, die mit dem Internet verbunden und vernetzt sind. Für zu Hause, für Unternehmen und die Industrie.

Instant Messenger Steht für „sofortige Nachrichtenübermittlung“ zwischen Internetnutzern. Beliebte Messenger-Dienste sind WhatsApp und Threema.

Malware Ein Sammelbegriff für unterschiedliche Schadprogramme, die sich ins System einschleusen und Schaden unterschiedlichster Art verursachen.

Nickname Eine Art Spitzname bzw. Pseudonym, mit dem man im Internet bzw. in Chats unterwegs ist.

Phishing Ein Kunstwort aus „Password“ und „Fishing“, übersetzt bedeutet es „nach Passwörtern angeln“. Und das mithilfe gefälschter E-Mails und Websites.

Social Engineering Eine Betrugsmasche, bei der jemand gezielt manipuliert und belogen wird, um sensible Informationen preiszugeben. Hier wird die Schwachstelle Mensch ausgenutzt.

VPN Steht für Virtuelles Privates Netzwerk, hier werden dank bestimmter Verfahren Daten besonders verschlüsselt und geschützt.

Ob online oder offline: Jede Spende zählt

Auch beim Helfen braucht man alle Hilfe: Unterstützen Sie die Arbeit des WEISSEN RINGS mit Ihrer Spende. Mehr als 3.000 ehrenamtliche Helferinnen und Helfer sind deutschlandweit für uns im Einsatz. Professionell kümmern sie sich z. B. um Cybermobbing-Opfer und in Not geratene Menschen, leisten menschlichen Beistand und beraten.

Neben der Opferhilfe engagieren wir uns außerdem im Bereich Präventions- und Aufklärungsarbeit, damit Gefahren auch im Internet frühzeitig erkannt und abgewehrt werden können. Da sich unsere Arbeit komplett aus Spenden finanziert, freuen wir uns über jeden Beitrag.

Jeder Betrag bewegt etwas

Mit *35 Euro* unterstützen Sie uns, einen Vortrag zum Thema Internetkriminalität durchzuführen.

Mit *50 Euro* setzen Sie sich dafür ein, dass wir ein Präventionsprojekt vor Ort starten.
Auch in Zusammenarbeit mit der Polizei.

Mit *75 Euro* helfen Sie uns, einen Infostand zu finanzieren, um z. B. auf das Thema Gefahren im Internet aufmerksam zu machen.

Spendenkonto WEISSER RING
IBAN: DE68 5505 0120 0000 3434 34
BIC: MALADE51MNZ
Sparkasse Mainz

Oder ganz bequem per Paypal. Mehr dazu unter: **www.weisser-ring.de/unterstuetzung/spende**

Opfer-Telefon:

116 006

(bundesweit kostenfrei)

400 Außenstellen bundesweit

Onlineberatung:
weisser-ring.de/hilfe/onlineberatung

WEISSER RING e. V.
Bundesgeschäftsstelle • Weberstraße 16 • 55130 Mainz • Germany
info@weisser-ring.de • www.weisser-ring.de
www.facebook.com/weisserring
www.youtube.com/weisserringev

Oktober 2018
Artikelnummer: 1115