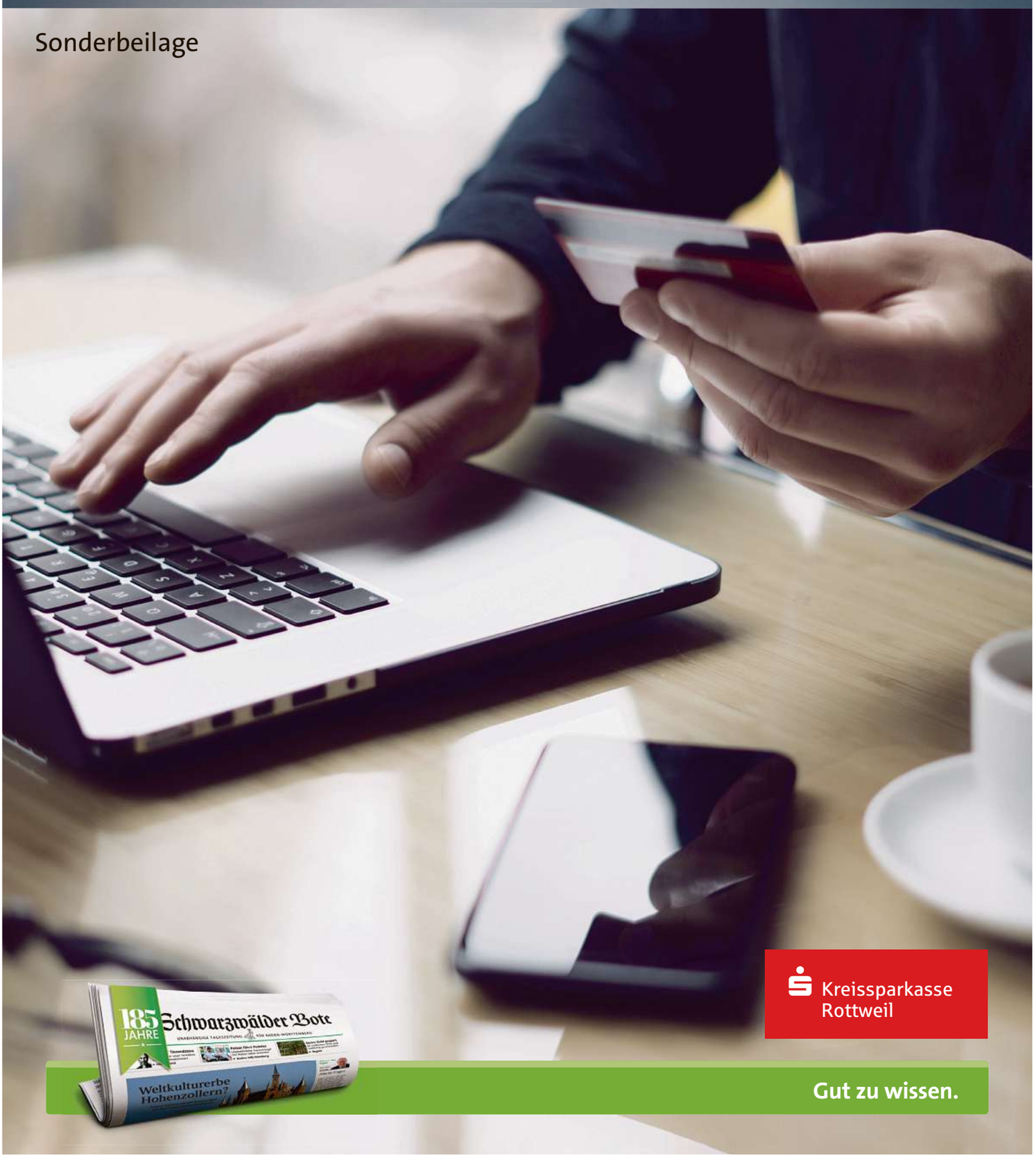
Sparkassen-Info-Serie

Online? Aber sicher!

Sonderbeilage



Kreissparkasse Rottweil

Gut zu wissen.

Vorwort

Online? Aber sicher!

Das Internet hat unsere Welt und auch die Kommunikationswege grundlegend verändert. Gerade in Zeiten des Corona-Virus lassen sich dadurch Sozialkontakte reduzieren. Die vielfältigen Möglichkeiten des Internets helfen uns dabei, die Ausbreitung des Virus zu verlangsamen um unser Gesundheitssystem nicht zu überlasten. Doch auch in „normalen“ Zeiten ist das World Wide Web wegen den unglaublich vielen Vorteilen aus unserem Leben nicht mehr wergzudenken. Dank Smartphones ist es nun jederzeit und überall verfügbar. Ob Videokonferenzen, Musikstreaming, E-Learning, Serien, Online-Tutorials, oder Online-Shopping – all das kann sowohl bequem von zu Hause oder auch unterwegs erfolgen, wenn sich spontan ein Zeitfenster auftut. Auch das Erledigen der Bankgeschäfte kann so einfach online erfolgen.

Ob Handel, Gewerbetreibende oder auch Sparkassen – alle wollen die Chancen des Internets nutzen und ihren Kunden einen digitalen Mehrwert bieten. Das wird von den Konsumenten inzwischen erwartet. Wir meinen, dass es dabei gilt, die Vorzüge persönlicher Kontakte und Kundennähe mit den Möglichkeiten der digitalen Welt zu verbinden. Die Kreissparkasse Rottweil investiert daher laufend in den Ausbau von modernen digitalen Angeboten. Gerade bei einfachen Dienstleistungen greifen Kunden sehr gerne auf unsere digitalen Angebote zurück, während bei umfangreichen Themenstellungen die Präferenz der Kunden klar auf der persönlichen Beratung liegt. Informieren im Netz –ja–, Abschluss –nein–. Den meisten Menschen ist eine persönliche Beratung weiterhin wichtig. Daher investieren wir nicht nur in digitale Angebote, sondern stärken gleichzeitig auch die persönliche Beratungskompetenz unserer Mitarbeiter durch individuelle Weiterbildungsmaßnahmen.

Bei aller Digitalisierungs-Euphorie muss uns auch bewusst sein, dass sich im Web leider auch „schwarze Schafte“ tummeln. Wir haben daher mit dem Schwarzwälder Boten die Infoserie „Online? Aber sicher!“ initiiert. Wir wollen unsere Kunden und die Leser für das Thema Sicherheit im Netz sensibilisieren. Durch einen vernünftigen Umgang mit Daten, mit cleveren Schutzmaßnahmen und einigen Verhaltensregeln, kann man die vielen positiven Mehrwerte im Netz mit ruhigem Gewissen nutzen. Diese wertvollen Hinweise haben wir nun nach Abschluss der Serie in diesem Kompendium für Sie zusammengefasst. Hier lesen Sie nochmals alle interessanten Infos und Tipps zum Schutz vor „Neppern, Schleppern und Bauernfängern“ im Netz. Mit Wachsamkeit und intelligenten Sicherheitstricks können wir es den dreisten Betrügern im Netz erschweren, Schindluder zu treiben und uns selbst schützen. Gleichzeitig investiert die Kreissparkasse Rottweil in immer neue und bessere Sicherheitsmaßnahmen für ihr Online-Banking-Angebot. So werden wir Sie auch in Zukunft mit „Sicherheit“ rundum beraten – ob im Netz oder nach überstandener Corona-Krise gerne wieder persönlich in unseren Geschäftsstellen.

Kreissparkasse Rottweil

Matthäus Reiser Roland Eckhardt Christian Kinzel

Inhalt

7 Tipps zur Passwortsicherheit

Was Sie tun können, dass Ihre Passwörter nicht geknackt werden!

Egal, ob für den Kauf neuer Schuhe im Onlineshop oder für den Online-Banking Zugang – die Anzahl der im Alltag benötigten Passwörter steigt stetig. Passwörter sind sozusagen der digitale Schlüssel zu unseren Daten und sollten daher mit Bedacht gewählt werden! Die Sicherheitsexperten des Potsdamer Hasso-Plattner-Institut weisen seit etlichen Jahren auf die Notwendigkeit sicherer Passwörter hin, um sich vor dem Zugriff Krimineller zu schützen. Erschreckende Realität: Viele Internetnutzer verlassen sich immer noch auf zu simple Kennwörter wie „123456“, „Passwort“ oder „qwertz. Für die Opfer können die Folgen zu persönlichen und finanziellen Fiasko werden. Darum ist es ratsam, sich mit sicheren Passwörtern zu schützen.

1. Passwörter nicht mehrfach verwenden: Nutzen Sie für jeden Online-Dienst (z.B. Online-Shops oder soziale Netzwerke) jeweils ein eigenes Passwort. Wird nämlich ein Zugang geknackt, sind auch die übrigen in Gefahr.

2. Je länger desto sicherer: Die Passwortsicherheit steigt mit jedem Zeichen. Experten empfehlen daher Passwörter mit mindestens acht Zeichen, besser sind 16.

3. Verwenden Sie Passwörter „ohne Sinn“: Hacker testen mit ihrer Software meist zuerst eine lange Liste gängiger Phrasen, etwa „Schatz“ oder Tastaturmuster wie „asdfgh“. Dann folgen Begriffe aus Wörterbüchern und anschließend probieren die Algorithmen auch Sonderzeichen aus. Verwenden Sie daher unsinnige Zahlen- und Buchstabenkombinationen.

4. Keine Wörter mit persönlichem Bezug: Verwenden Sie keine Namen von Familienmitgliedern, von Freunden, Haustieren, oder deren Geburtsdaten als Passwort. Angreifer könnten die Namen oder Daten aus öffentlichen Informationen zusammensuchen, etwa aus Profilen in sozialen Netzwerken.

5. Alle Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen): Kombinieren Sie die verschiedenen Zeichenklassen um Ihre Passwörter zu bilden. Bauen Sie sich dazu Eselsbrücken, um sich auch komplizierte Passwörter merken zu können. Überlegen Sie sich einen Satz und verwenden Sie davon nur dessen Wortanfänge um Ihr Passwort zu bilden. So wird aus „Im Winter 2019 habe ich mir mein rechtes Bein gebrochen!“ das Passwort „IW2019himmrBg!“

© iStock

6. Nutzen Sie Passwort-Manager: Viele Nutzer sind überfordert damit, sich für jeden Dienst ein anderes Passwort zu merken und verwenden daher ein Passwort mehrfach – gefährlich. Mit einem Passwort-Manager werden Ihre Daten mit sicheren kryptografischen Verfahren verschlüsselt und Sie müssen nur ein Masterkennwort im Gedächtnis behalten, um Zugriff auf all Ihre Logins zu erhalten. Wählen Sie aber unbedingt einen guten Passwort-Manager, lassen Sie sich gegebenenfalls im Fachgeschäft beraten.

7. Zwei-Faktor-Authentifizierung: Für Konten mit wichtigen und sensiblen Daten, wie z.B. Ihren E-Mail-Account, sind einzigartige Passwörter unablässig. Sie können den Schutz aber noch deutlich verbessern, wenn Sie auf die sogenannte Zwei Faktor-Authentifizierung (2-F-A) setzen. Mit der 2-F-A ist für die Anmeldung zusätzlich zum Passwort eine weitere Eingabe nötig. Dies kann je nach Dienst und technischer Voraussetzung ein Finger-Abdruck-Scan oder ein Code, den Sie auf Ihr Smartphone geschickt bekommen, sein. Hacker benötigen dann also nicht nur Ihr Passwort, sondern auch physischen Zugriff auf Ihr Handy, wenn Sie Ihr Konto übernehmen wollen.

Sicher einkaufen im Internet

Online-Shopping liegt voll im Trend – quer durch alle Altersklassen und Gesellschaftsschichten. Vor allem die große Auswahl und die Möglichkeit jederzeit bequem von zu Hause aus auf Einkaufstour zu gehen ist verlockend.

Vor jedem Kauf sollten Sie aber den jeweiligen Händler genau überprüfen, um Problemen oder gar Betrügereien aus dem Weg zu gehen. Mit unseren Sicherheitstipps sind unseriöse Anbieter und nicht ausreichend gesicherte Online-Shops jedoch keine Gefahr mehr für Sie!

Überprüfung der Geschäftsbedingungen des Händlers

Alle wichtigen Informationen zum Händler stehen in der Regel im Impressum auf dessen Website. Sie finden dort den Namen des Unternehmens, die Anschrift, die Telefonnummer, sowie die E-Mail-Adresse. Auch die Steuer- bzw. Registernummer des Händlers ist dort normalerweise zu finden. Ist dies nicht der Fall oder sind die Möglichkeiten zur schnellen Kontaktaufnahme sehr begrenzt, oder fehlt das Impressum gar gänzlich, ist Vorsicht geboten. Sind die Informationen zum Datenschutz nicht zur Einsicht oder die AGB lückenhaft, könnte es sein, dass Ihre Daten verkauft oder zu Werbezwecken verwendet werden.

Erfahrungswerte von anderen Nutzern des Online-Shops

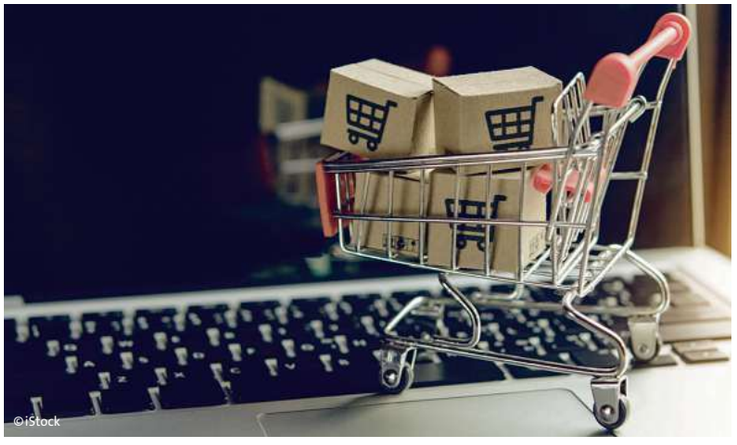
Mithilfe von Beurteilungen von anderen Nutzern des Online-Shops in Foren und dergleichen können Sie sich meist auch ein gutes Bild von einem Anbieter machen. Geben Sie dazu einfach den Namen des Shops und das Wort „Bewertung“, „Problem“ oder „Betrug“ in einer Suchmaschine ein. Aus den Ergebnissen können Sie oft gute Schlüsse hinsichtlich der Seriosität des Unternehmens ziehen.

Eindeutige Hinweise vor Bestellabschluss

Verbraucher sollen vor unerwünscht abgeschlossenen Online-Geschäften durch die so genannte Button-Lösung geschützt werden, die in Deutschland seit 2012 in Kraft ist. Eine eindeutige Formulierung wie „jetzt zahlungspflichtig bestellen“ soll laut Gesetz auf das Ende eines Bestellprozesses hinweisen. Ist dies nicht der Fall, kommt daher auch kein bindender Vertrag zustande. Der Gesetzgeber verlangt außerdem, dass unmittelbar vor Abschluss der Bestellung bestimmte Informationen wie Gesamtpreis inklusive Mehrwertsteuer und Versandkosten und Produktmerkmale klar verständlich und gut sichtbar angezeigt werden.

Gütesiegel überprüfen

Oftmals verfügen sogenannte Fake-Shops, die nur dem Zweck dienen, arglose Käufer zu betrügen, über gefälschte Gütesiegel bekannter Prüfstellen. Deshalb: Prüfen Sie vor dem Kauf, ob der Online-Shop auch tatsächlich auf der Website des Siegels gelistet wird.


©iStock

Auf verschlüsselte Datenübertragung achten

Beim Bezahlen sollten Sie unabhängig vom Online-Shop und der gewünschten Zahlungsmethode immer darauf achten, dass alle Daten verschlüsselt übermittelt werden. Die SSL/TLS- Technik identifiziert die Internetseite und stellt sicher, dass Daten während der Übertragung weder gelesen noch manipuliert werden können. Eine verschlüsselte Datenverbindung erkennen Sie daran, dass ein „s“ (für: „secure“, dt. „sicher“) hinter den Buchstaben „http“ in der Adresszeile des Browsers steht. Beim Aufruf einer https-Adresse prüft der Browser, ob der Anbieter ein gültiges Sicherheitszertifikat vorweisen kann. Kann er das nicht, erhalten Sie eine Warnung, dann sollten Sie die Website besser verlassen. Erscheint die Adresszeile nach dem Aufruf der Seite aber in grün, weist dies auf die höchste Zertifikatsstufe hin – diese Verbindung ist sicher. Wenn Sie diese Sicherheitstipps beachten, sind Sie beim Online-Shopping um einiges sicherer unterwegs!

Was ist Phishing?

Phishing ist ein zusammengesetztes Kunstwort aus „password“ und „fishing“. Es steht für das Stehlen von Passwörtern. Der beste Schutz? Aufmerksamkeit!

Phishing ist ein zusammengesetztes Kunstwort aus „password“ und „fishing“. Es steht für das Stehlen von Passwörtern. Der beste Schutz? Aufmerksamkeit!

„Phishing“ bezeichnet das Bestreben, über gefälschte E-Mails oder Webseiten nach Passwörtern, PINs oder TANs zu angeln, und diese kriminell gegen Sie zu verwenden. Als seriöse Bank, Internetanbieter o.ä. getarnt, werden Sie durch betrügerische E-Mails dazu verleitet, eine Phishing-Seite aufzurufen, vermeintlich um z.B. Ihr Konto wieder frei zu schalten, wo Sie dann aufgefordert werden, Ihr Passwort, Ihre Online-Banking-Zugangsdaten, oder gar TANs einzugeben. Tun Sie dies, erbeuten die Datendiebe, auf diesem Wege hochsensible Informationen. Diese Daten könnten die Kriminellen dann z.B. zur Durchführung von betrügerischen Online-Überweisungen in Ihrem Namen nutzen.

Sowohl die Phishing-Mail selbst, als auch die gefälschte Website, auf die ein Link im Text verweist, sind dabei zumeist fast perfekt nachgeahmt. Allzu oft gelingt es Cyber-Kriminellen, durch professionelle Imitation des Corporate Designs (Logo, Farbgebung, Schriftarten der jeweiligen Organisation) überzeugend Echtheit vorzutäuschen. So werden Sie, als ahnungsloser Empfänger solcher Mails, leichter dazu verleitet, auf einen Link in der Mail zu klicken, wodurch Ihre Daten großer

©shutterstock

Gefahr ausgesetzt sind, gestohlen zu werden. Dies geschieht durch Abgreifen der eingegebenen Daten auf der gefälschten Website einer Organisation, die als vertrauenswürdig anerkannt ist. Oder aber Sie installieren durch den Aufruf des Links unwissentlich Schadsoftware auf Ihrem Gerät, welche dann ebenfalls Daten abfängt.

Öffnen Sie deshalb am besten niemals einen E-Mail-Anhang eines unbekannten Absenders! Der wirksamste Schutz gegen Passwort-Diebstahl: Reagieren Sie nicht auf Nachrichten unbekannter Herkunft und ignorieren Sie die Aufforderung, Daten einzugeben.

Wichtig: Ihre Sparkasse wird Sie niemals darum bitten, aus einer E-Mail heraus Internetseiten zu öffnen, um dort Daten wie Ihre IBAN, PIN, TAN oder Ihre Kreditkartendaten einzugeben!

Bei genauem Hinsehen weisen Phishing-Attacken oftmals typische Merkmale auf:

- Mails sind in fehlerhaftem Deutsch verfasst, fehlende Umlaute weisen auch darauf hin, dass etwas nicht stimmt. Die Qualität der Nachahmungen wird aber immer besser, sodass Sie diese nicht immer sofort als solche entlarven können.
- In vielen Fällen ist die Anrede unpersönlich: „Sehr geehrter Kunde“. Aber Achtung, mittlerweile kann auch die Anrede persönlich gestaltet sein und Ihren Namen enthalten, um der Nachricht eine höhere Glaubwürdigkeit zu verleihen.
- Meistens geht es in Phishing-Mails um Kontosperren, Datenabgleich oder Ähnliches. Mit den Mails wird gezielt Druck oder Panik aufgebaut, um eine schnelle, unüberlegte Handlung zu erzwingen. Oder sie versprechen Gewinne oder Sonderangebote.
- Imitate von Internetseiten mit sensiblen Daten haben kein gültiges Sicherheitszertifikat. Die Adresse in der Adresszeile des Browsers beginnt wahrscheinlich nicht mit https („s“ für: „sicher“), sondern nur mit „http“.

Im Zweifel gilt: Wenn Ihre Bank Ihnen nie E-Mails schickt, Ihre E-Mailadresse eigentlich gar nicht kennen kann, oder ein anderer Dienstleister sie kontaktiert, mit dem Sie keine Geschäftsbeziehung haben – löschen Sie die E-Mail.

Sicher bezahlen im Internet

Sie können im Internet auf viele unterschiedliche Arten bezahlen – wir stellen Ihnen diese vor und sagen, was zu beachten ist.

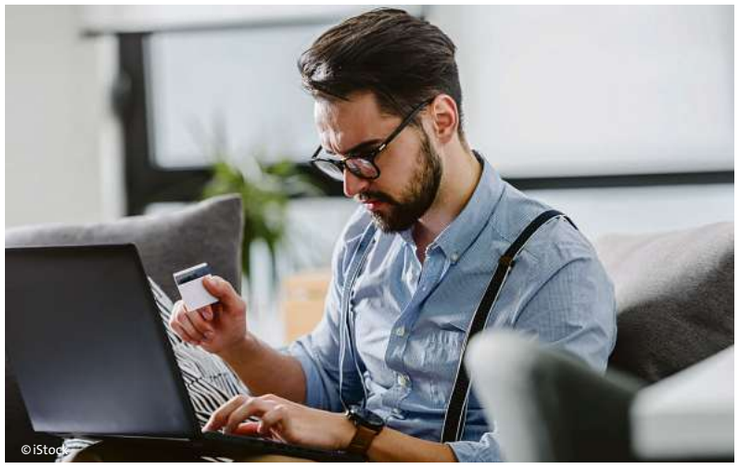
Alle Bezahlverfahren haben ihre Vor- und Nachteile. Wägen Sie bei jedem Online-Kauf zwischen Komfort und Sicherheit ab, ehe Sie sich für eine Zahlungsmethode entscheiden. Für welches Verfahren Sie sich auch entscheiden: Wir raten Ihnen generell darauf zu achten, dass alle Daten über eine sichere SSL-Verbindung verschlüsselt übertragen werden – sowohl Ihre persönlichen Angaben als auch alle Informationen zu Bankverbindungen oder Kreditkarteninformationen. Dies erkennen Sie daran, dass in der URL-Zeile Ihres Browsers statt http nun https am Anfang der Webadresse angezeigt wird. Diese Möglichkeiten gibt es:

Zahlen per Rechnung

Über eine Rechnung zu bezahlen ist für Sie als Kunde definitiv die sicherste Variante. Sie bekommen die Ware zuerst zugeschickt, können sie prüfen und erst dann begleichen Sie die Rechnung. Allerdings müssen Sie sich selbst um die Überweisung kümmern. Es geht komfortabler.

Lastschrift vom Girokonto

Bei dieser Zahlungsweise wird der Rechnungsbetrag mit Ihrem Einverständnis in Form einer Einzugsermächtigung von Ihrem Girokonto abgebucht, was in der Regel beim Versand der Ware geschieht. Nachteil: Sie müssen dazu Ihre Kontodaten an den Händler übermitteln. Dafür haben Sie ein achtwöchiges Widerspruchsrecht und können sich so Ihr Geld einfach wieder zurückholen, sollte etwas nicht passen.



Zahlen per Kreditkarte

In den meisten Online-Shops können Sie mit Kreditkarte bezahlen. Das ist ziemlich unkompliziert – Sie müssen lediglich ein paar Kartendaten eingeben und sich anschließend legitimieren, um nachzuweisen, dass auch tatsächlich der Karteninhaber mit den Kartendaten zahlt. So wird das Bezahlen mit Kreditkarte im Internet zusätzlich durch das 3D-Secure-Verfahren (Mastercard® Identity Check™/ Visa Secure) abgesichert. Auch hier können unrechtmäßige Abbuchungen erstattet werden, der Aufwand ist allerdings größer als bei der Lastschrift.

Zahlen per Nachnahme

Bei der Nachnahme zahlen Sie den Rechnungsbetrag bei Lieferung der Ware direkt und bar an den Postzusteller. Sie müssen die Ware zwar erst bezahlen, wenn sie tatsächlich bei Ihnen angekommen ist, aber Sie können die Ware nicht vor dem Bezahlen kontrollieren. Dadurch kann es zu Problemen bei der Reklamation kommen. Außerdem müssen Sie bei der Anlieferung zu Hause sein und es werden häufig Nachnahmegebühren fällig.

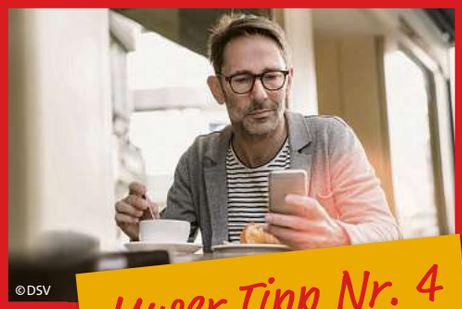
Zahlen per Vorkasse

Von einer Vorkasse-Zahlung ist generell abzuraten. Ein seriöser Online-Händler wird immer mindestens eine alternative Zahlungsmethode anbieten. Bei der Zahlung per Vorkasse überweisen Sie dem Verkäufer das Geld und erst danach verschickt dieser die Ware. Kommt die Ware nicht an, haben Sie gegen den Verkäufer wenig in der Hand. Immer wieder probieren Betrüger und unseriöse Händler, Kunden durch Zahlung per Vorkasse Geld abzuknöpfen.

Zahlen über Bezahlsystem-Anbieter

Der Vorteil dieser Zahlungsmethode ist, dass Sie sensible Daten wie Bankverbindung oder Kreditkartennummer nicht bei jeder einzelnen Transaktion eingeben müssen. Diese werden bei der Registrierung beim jeweiligen Dienst, ebenso wie ein festzulegender Benutzername und ein Passwort hinterlegt. Wenn ein Online-Shop nun diesen Bezahlsystemanbieter unterstützt, werden Sie direkt auf dessen Website geleitet. Dort melden Sie sich an und bestätigen die Transaktion, woraufhin der Anbieter die Zahlung an den Shop weitergibt und anschließend den Betrag von Ihrem Bankkonto oder Ihrer Kreditkarte einzieht.

Sicher zahlen mit paydirekt!



paydirekt ist das kostenlose Online-Bezahlverfahren der deutschen Sparkassen und Banken. Es bietet Ihnen bei jedem Online-Einkauf maximale Sicherheit und optimalen Komfort. paydirekt ist eine Zusatzfunktion Ihres Online-Bankings und bucht das Geld direkt von Ihrem Girokonto ab, egal ob Sie mobil oder am Computer bezahlen. Es ist kein fremder Zahlungsdienstleister zwischengeschaltet, Ihre Daten bleiben verschlüsselt und nach deutschen Datenschutzbestimmungen auf inländischen Bankservern. Da der Händler sofort eine Zahlungsbestätigung bekommt, kann er die Ware sofort losschicken. Für den Fall, dass Sie keine Ware geliefert bekommen, bietet paydirekt außerdem Käuferschutz: Sie bekommen Ihr Geld bis zu 30 Tage nach der Bezahlung zurück. Obendrein gibt es wechselnde attraktive Rabatt-Aktionen und Angebote der Partner-Händler – paydirekt lohnt sich also in mehrfacher Hinsicht!

So nutzen Sie paydirekt:

Wenn Sie also künftig Online mit paydirekt bezahlen wollen, müssen Sie sich als Sparkassenkunde nur einmalig im Online-Banking für paydirekt registrieren. Dann können Sie einfach mit Ihrem Benutzernamen und Passwort bezahlen.

Interessiert? Weitere Infos zu paydirekt finden Sie auf **www.ksk-rw.de/paydirekt**

Kreissparkasse Rottweil

Kontaktlos schneller bezahlen.

ksk-rw.de

Mit Sparkassen-Card[1], Mastercard[2], per Android- oder Apple-Smartphone.

Mehr Infos unter www.ksk-rw.de

[1] Bei diesem Produkt handelt es sich um eine Debitkarte.

[2] Bei diesem Produkt handelt es sich um eine Kreditkarte.

Wenn's um Geld geht

Kreissparkasse Rottweil

Schutz vor Identitätsdiebstahl

Das Thema Identitätsdiebstahl gewinnt im Zeitalter des Internets mehr und mehr an Bedeutung – Kriminelle spähen personenbezogene Daten Dritter aus, um damit Straftaten zu begehen. Beherzigen Sie darum ein paar Schutzmaßnahmen, mithilfe derer Sie das Vorhaben der Kriminellen um einiges erschweren können.

Beim Identitätsdiebstahl beschaffen sich die Täter zunächst ausschließlich die Identität eines Menschen, indem Sie den Namen und das Geburtsdatum stehlen. Meistens bemerkt die betroffene Person den Datenklau erst, wenn es dann zu einem Missbrauch kommt, d.h. wenn die Täter diese Daten benutzen, indem sie sich als Sie ausgeben. Die Betrüger bestellen dann z.B. Ware im Internet und leiten diese an eine gewünschte Adresse weiter – die Rechnung, wie auch die Mahnung bekommen Sie. Identitätsdiebstahl kann aber auch genutzt werden, um falsche Accounts in sozialen Netzwerken anzulegen, mit dem Ziel, den Ruf der Opfer zu beschädigen. Halten Sie alle Softwarekomponenten Ihres Gerätes aktuell. Verwenden Sie eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme, insbesondere des Webbrowers. Nutzen Sie wenn möglich die automatische Update- Funktion, die oft voreingestellt ist. Somit können Angreifer keine alten, bereits bekannten Schwachstellen ausnutzen.

1. Nutzen Sie Virenschutz und Firewall. In den gängigen Betriebssystemen sind diese bereits integriert und erschweren schon in der Standardkonfiguration Angriffe aus dem Internet. Aktivieren Sie diese oder besser verwenden Sie ein Virenschutzprogramm eines anderen Anbieters. Lassen Sie sich nicht durch einen aktivierten Virenschutz oder die Firewall zu Unvorsicht verleiten, sie garantieren keine vollständige Sicherheit.

2. Schützen Sie Ihre digitalen Identitäten, indem Sie nicht überall dieselbe E-Mailadresse nutzen, um sich anzumelden. Damit können Sie einem aufschlussreichen Gesamtprofil entgegenwirken. Außerdem sollten Sie das gleiche Passwort nicht mehrfach verwenden, sondern jeweils ein anderes, möglichst komplexes Passwort wählen. So vermeiden Sie eine Kettenreaktion, für den Fall, dass Ihr E-Mail-Konto geknackt werden sollte.

3. Geben Sie bei der Anmeldung bei einem Dienst, wie auch generell im Internet, möglichst wenige Informationen preis. Ihr Geburtsdatum sollten Sie lieber verschweigen. Wenn Ihnen eine Webseite Sicherheitsfragen anbietet, wählen Sie eine Frage, deren Antwort sich nicht im Internet recherchieren lässt. Wägen Sie außerdem sorgfältig ab, wo Sie Ihren richtigen Namen benutzen und wo ein Alias als Nutzername ausreichend ist.

4. Melden Sie sich immer von allen Internetseiten ab, wenn Sie einen öffentlichen Internetzugang benutzen und nutzen Sie Ihren E-Mail-Account am besten nicht auf öffentlich zugänglichen Rechnern. Ihr Passwort könnte dort ausgespäht werden.

5. Öffnen Sie keine Links oder Anhänge in E-Mails von unbekannten Absendern. Dahinter könnte sich ein Trojaner verbergen, eine Software, die Ihre Daten abfangen und weiterleiten kann. Aus dem selben Grund sollten Sie Daten aus dem Internet nur aus vertrauenswürdigen Quellen herunterladen. Überprüfen Sie bei Links in der Browser-Adresszeile außerdem genau, ob dort wirklich die richtige Internetadresse steht.

Mobiles Bezahlen? Aber sicher!

Das Bezahlen im Handel mit dem Smartphone wird noch von vielen Skeptikern als unsicher eingeschätzt. Zurecht? Wir gehen Mythen rund um das mobile Bezahlen auf den Grund.

Mythos 1: Aus Versehen bezahlen

Kann nicht passieren! Beim mobilen Bezahlen wird, ebenso wie beim kontaktlosen Bezahlen mit der Sparkassen-Card (Debitkarte) oder der Kreditkarte, die sogenannte NFC-Technik (Near Field Communication) angewandt. Das bedeutet, dass Sie mit Ihrem Smartphone bis auf wenige Zentimeter an das Kassenterminal herankommen müssen, welches in diesem Moment aktiviert sein muss. Außerdem müssen Sie Ihr Smartphone durch Fingerabdruck, Gesichtserkennung oder Geräte-Code entsperrt haben. Ziemlich unwahrscheinlich also, dass das alles gleichzeitig passiert, ohne, dass Sie es merken.

Mythos 2: Handy weg – Geld weg

Keine Sorge, das Geld verbleibt sicher auf Ihrem Konto. Auf dem Smartphone ist nämlich kein Geld „gespeichert". Lassen Sie dennoch – wie bei beim Verlust einer Sparkassen-Card oder Kreditkarte auch – die „digitale Karte" bei Ihrer Sparkasse sperren, um einen Missbrauch auszuschließen. Sie können dies alternativ auch unter dem Sperrnotruf

116 116 tun. Ihre physischen Karten können Sie dennoch weiterhin nutzen, diese sind von der Sperrung ihrer „digitalen Karte" nicht betroffen.

Mythos 3: Kein Internet – kein Shopping

Falsch. Der Bezahlvorgang beim mobilen Bezahlen ist nicht von einer Internetverbindung abhängig, sondern erfolgt wie bereits erwähnt über NFC-Technik. Sie können auch offline mobil bezahlen. Bis zu zehn Mal hintereinander ist dies möglich. Erst dann braucht die App eine erneute Verbindung zum Internet, um den Transaktionszähler zurückzusetzen. Sind nur noch wenige Zahlungen möglich, erhalten Sie eine entsprechende Nachricht.

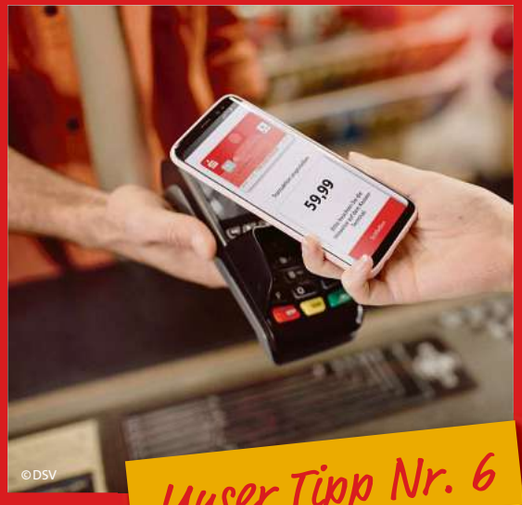
Mythos 4: Prepaid-Guthaben oder Smartphonerechnung werden belastet

Das ist nicht der Fall. Mobiles Bezahlen ist eine gewöhnliche Kartenzahlung – Sie zahlen immer mit Ihrer Sparkassen-Card (Debitkarte) oder Ihrer Kreditkarte. Die Abbuchung erfolgt wie gewohnt per Lastschrift von Ihrem Konto.

Mythos 5: Daten werden abgegriffen

Auch das ist nicht richtig. Das mobile Bezahlen ist sehr datensparsam. Transaktionen erhalten keine persönlichen Daten wie z.B. Ihren Namen oder Ihre Adresse. Es werden lediglich die Informationen über die kontaktlose Schnittstelle verschlüsselt übermittelt, die zur Abwicklung der Zahlung tatsächlich notwendig sind.

Mobiles Bezahlen ist smart!



Unser Tipp Nr. 6

Kreissparkasse Rottweil

Ein Großteil der Händler in unserem Geschäftsgebiet bietet Ihnen bereits die Möglichkeit, mobil zu bezahlen - nutzen Sie dieses Angebot, zahlen Sie künftig mobil mit Ihrem Android-Smartphone.

- Praktisch: Das Smartphone ist als täglicher Begleiter immer dabei – Sie sind auch ohne Bargeld stets zahlungsfähig.
- Schnell: NFC-Technologie ermöglicht die kontaktlose Datenübertragung beim Bezahlvorgang in Sekundenschnelle.
- Sicher: Die Zahlungsfreigabe erfolgt mithilfe Ihres Fingerabdrucks, Gerätecodes oder Gesichtserkennung. Es gelten die gleichen hohen Sicherheitsstandards wie bei der Sparkassen-Card (Debitkarte) oder Mastercard (Kreditkarte).
- Modern: Mit dieser intuitiven und innovativen Bezahlweise liegen Sie voll im Trend.
- Hygienisch: Sie müssen Ihr Smartphone beim Bezahlen nicht aus der Hand geben und kommen auch nicht mit verschmutztem Bargeld in Kontakt.
- Transparent: Alle Abbuchungen sehen Sie wie gewohnt auf Ihrem Kontoauszug.

An allen Kartenterminals, an denen kontaktlose Zahlungen mit der Sparkassen-Card (Debitkarte) oder der Mastercard (Kreditkarte) akzeptiert werden, können Sie auch mobil bezahlen. Achten Sie auf das Kontaktlos-Wellensymbol.

Grundvoraussetzung für das mobile Bezahlen ist, dass Ihr Smartphone mindestens das Android-Betriebssystem 6.0 installiert hat und eine NFC-Funktion besitzt. Sie benötigen einen Online-Banking Zugang bei Ihrer Sparkasse und die App „Mobiles Bezahlen" muss installiert und eingerichtet sein.

Weitere Informationen zum mobilen Bezahlen finden Sie auf **www.ksk-rw.de/mobilesbezahlen**

Gute Gründe fürs Online-Banking

In Deutschland erledigen immer mehr Menschen ihre Bankgeschäfte mit Online-Banking. Und gerade jetzt in Zeiten des Coronavirus lassen sich dadurch Sozialkontakte vermeiden und die Gefahr der Übertragung einschränken. Aber nicht nur aus gesundheitlichen Gründen spricht einiges dafür, Überweisungen von zu Hause aus zu tätigen. Wir haben gute Gründe für Sie zusammengetragen, jetzt umzustellen.

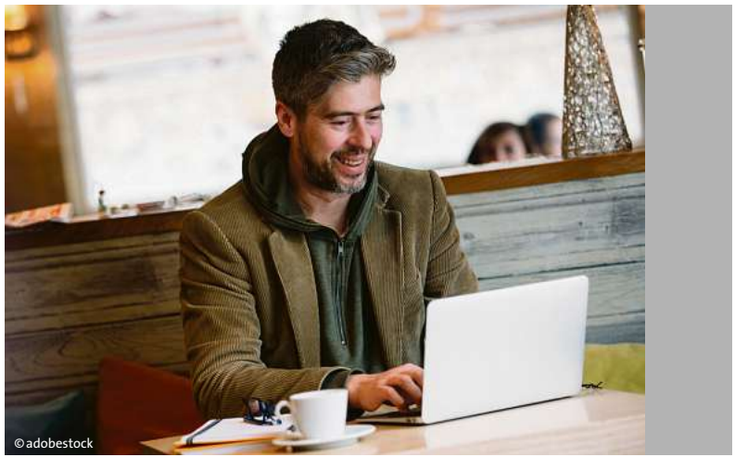
Möglicherweise haben auch Sie sich schon überlegt, ob Sie Online-Banking nicht gerne einmal ausprobieren würden. Vielleicht stehen Sie diesem Thema aber auch etwas skeptisch gegenüber oder haben schlicht noch ungeklärte Fragen. Wir zeigen Ihnen eine Auswahl der Möglichkeiten, die sich Ihnen bieten, falls Sie sich dafür entscheiden sollten.

Zeit und Wege sparen

Haben Sie eine dringende Überweisung zu tätigen, oder wollen Sie einen Dauerauftrag einrichten? Jedes Mal, wenn Sie Ihre Bankgeschäfte online erledigen, sparen Sie sich den Weg zur Bankfiliale und damit auch Zeit. Außerdem sind Sie viel flexibler, weil Sie sich nicht an Öffnungszeiten halten müssen und Ihre Bankgeschäfte sogar im Urlaub oder einfach bequem von zu Hause aus erledigen können. Alles was Sie dazu benötigen, ist ein Online-Banking-Teilnehmervertrag, den Sie mit Ihrer Bank schließen müssen, sowie ein Gerät (PC/Laptop/Smartphone/Tablet) mit Internetzugang.

Jederzeit Zugriff auf wichtige Dokumente

Falls gewünscht, stellen wir Ihnen Ihre Auszüge für Girokonten, Kreditkarten, Darlehen, aber auch Wertpapierabrechnungen oder



Steuerbescheinigungen im Elektronischen Postfach in Ihrem Online-Banking-Zugang (anstatt papierhaft) zur Verfügung. Dadurch sind Ihre Dokumente ständig und ohne großes Suchen griffbereit und abrufbar. Kostenpflichtige Zwangsausdrucke oder lästiges Abheften und sich türmende Kontoauszugshefter gehören damit der Vergangenheit an. Außerdem haben Sie die Möglichkeit den Elektronischen Safe zu aktivieren, den wir Ihnen kostenlos anbieten. Dabei handelt es sich um eine Art digitales Schließfach, welches nur durch Anmeldung über den Online-Banking-Zugang sowie die Eingabe einer gültigen TAN zu öffnen ist. Dokumente aus dem Elektronischen Postfach lassen sich problemlos in den Elektronischen Safe übertragen und Sie können sogar eigene Dokumente, z.B. eine Kopie Ihres Personalausweises, einfach vom Smartphone oder PC hochladen. Ihre Dokumente werden hier nach deutschem Datenschutzstandard aufbewahrt und stehen Ihnen zeitlich unbegrenzt zur Verfügung. Benötigen Sie die Dokumente, können Sie diese jederzeit und überall herunterladen.

Stets alle Konten im Blick

Mit der Multibanking-Funktion bündeln Sie Ihre Konten und Depots vieler Banken, Sparkassen und Zahlungsdienstleister (z.B. paydirekt oder PayPal) – so haben Sie immer alle im Blick. Zudem können Sie mittlerweile bestandsverändernde Transaktionen (z.B. Überweisungen oder Daueraufträge) von Fremdbankkonten im Online-Banking der Sparkassen durchführen. Die Zugangsdaten all Ihrer Bankkonten werden hierzu direkt im Online-Banking mehrfach gesichert und nur verschlüsselt hinterlegt.

Sicher im Internet bezahlen

Haben Sie einen Online-Banking-Zugang, können Sie auch paydirekt nutzen, das kostenlose Online-Bezahlverfahren der deutschen Banken und Sparkassen. Es ist direkt an Ihr Girokonto gebunden und bietet Ihnen beim Online-Shopping optimalen Komfort und maximale Sicherheit. Dabei erhält der Händler eine umgehende Zahlungsbestätigung und Sie genießen Käuferschutz bei ausbleibender Lieferung. paydirekt unterliegt den deutschen Datenschutzbestimmungen.

Noch mehr Infos zum Online-Banking und zur Registrierung erhalten Sie auf **www.ksk-rw.de/online-banking-beantragen.**

Foto machen, statt IBAN abtippen

Mit der Fotoüberweisung in der „Sparkasse“-App können Sie Rechnungen bequem mit dem Smartphone abfotografieren. Die relevanten Daten werden automatisch erkannt und direkt ins Überweisungsformular übertragen. Lästiges Abtippen der IBAN oder der Rechnungsnummer bleibt Ihnen erspart. Nachdem Sie die Überweisungsdaten überprüft haben, benötigen Sie nun nur noch eine TAN, um die Überweisung auszulösen.

Das pushTAN-Verfahren

Um an die benötigte TAN zu gelangen, bietet sich das pushTAN-Verfahren als bequemste Lösung an: Sie erhalten die TAN über die „S-pushTAN-App“ direkt auf Ihr Smartphone oder Tablet. Somit können Sie mit nur einem Gerät flexibel und sicher auf Ihr Online-Banking zugreifen und auch die TAN anfordern. Passwort-Schutz bzw. biometrische Sicherheitsverfahren und kryptografische Schlüssel machen das Verfahren sicher. Der TÜV Saarland hat die App in Sachen Sicherheit geprüft. Um pushTAN nutzen zu können, benötigen Sie ein Sparkassen-Konto mit Online-Banking-Zugang sowie die kostenfreie S-pushTAN-App. Jetzt müssen Sie sich noch für das pushTAN-Verfahren freischalten (lassen). Gehen Sie dazu einfach auf unsere Homepage oder fragen Sie auf einer unserer Filialen nach.

Interessiert? Weitere Details finden Sie auf **www.ksk-rw.de/pushtan**

Kreissparkasse Rottweil

Sicherheit – auch für Ihr Smartphone und Tablet!

Die Sicherheitsanforderungen an mobile Geräte haben sich verändert. Zum Schutz Ihrer Daten geben wir Ihnen einige hilfreiche Tipps.

Um Ihr Smartphone oder Tablet vor Angriffen von Cyber-Kriminellen und Schadsoftware zu schützen, genügen normalerweise wenige Maßnahmen:

• Gerät sperren:
Es mag umständlich und nervig sein, aber aktivieren Sie stets die Tastatur-, Geräte- oder Displaysperre, wenn Sie Ihr Gerät gerade nicht benutzen.

• Schnittstellen deaktivieren:
Aktivieren Sie Verbindungen wie Bluetooth oder WLAN nur dann, wenn Sie diese tatsächlich benötigen, um erst gar keine Angriffsstellen von außen für Kriminelle oder schädliche Software zu bieten.

• Im Blick behalten:
Um Ihr Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie ihr Smartphone niemals unbeobachtet liegen lassen oder verleihen.

• Vertrauenswürdige Apps:
Installieren Sie ausschließlich Apps aus vertrauenswürdigen Quellen und überprüfen Sie vor der Installation das Einräumen von Zugriffsrechten auf Ihre Daten.


© adobestock

• Vorsicht in öffentlichen WLANs:
Dieselbe Eigenschaft, die kostenlose WLAN-Hotspots für die breite Öffentlichkeit so interessant macht, macht sie gleichzeitig auch so attraktiv für Hacker: Es ist keine Authentifizierung erforderlich, um eine Verbindung zum Netzwerk herzustellen. Dadurch erhalten Hacker nahezu uneingeschränkten Zugriff auf ungesicherte Geräte im selben Netzwerk. Nutzen Sie daher möglichst eine App, die eine virtuelle private Netzwerkverbindung (VPN) aufbauen kann. Hier werden Ihre Daten sicher verschlüsselt. Ist dies nicht möglich, nutzen Sie SSL-Verbindungen (https) auf Webseiten, bei denen Sie Zugangsdaten eingeben müssen, sodass diese trotzdem verschlüsselt übermittelt werden.

• Sichern Sie Ihre Daten:
Machen Sie regelmäßig Backups, um Datenverlust (in Form von Dokumenten, Fotos, Videos, Nummern) zu vermeiden. Für den Fall, dass das Gerät verloren geht oder beschädigt wird sind diese sonst womöglich unwiederbringlich verloren.

• Löschen Sie Daten:
Wenn Sie Ihr altes Smartphone verkaufen oder entsorgen wollen, sollten Sie alle sensiblen Daten davor löschen. Das Zurücksetzen auf Werkseinstellungen reicht dabei nicht unbedingt aus, um die Daten zu löschen, sodass diese nicht wiederherstellbar sind. Informieren Sie sich am besten beim Gerätehersteller, wie da das geht.

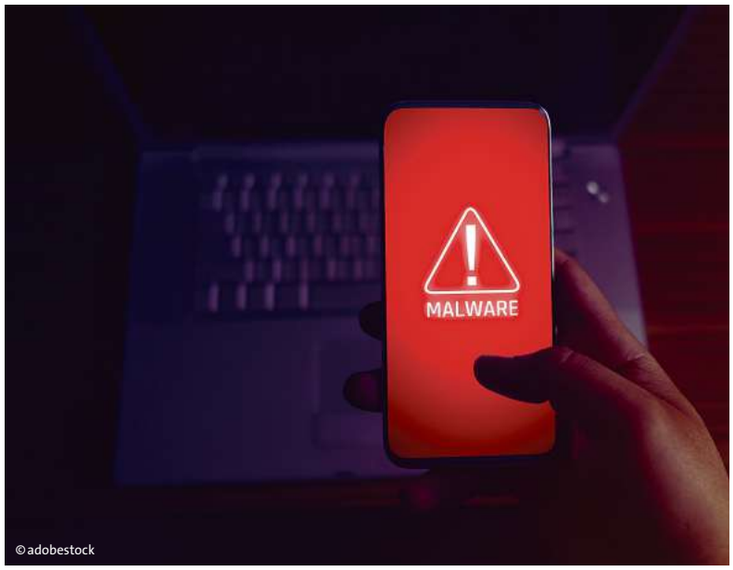
Diese und noch mehr Infos finden Sie auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de).

So schützen Sie sich gegen Malware

Malware ist ein Sammelbegriff für Schadsoftware, die Daten ausspähen oder den Computer unbrauchbar machen kann. Es gibt etliche Arten von Malware, z.B. Viren, Trojaner oder Spyware. Wie Sie sich schützen können, erfahren Sie hier.

Malware hat das Ziel, auf fremden Geräten unerwünschte Aktionen durchzuführen, um dort Schaden anzurichten. Man kann über sehr viele Wege mit Malware in Kontakt kommen – ob beim Surfen im Internet, beim Öffnen eines Downloadlinks oder eines E-Mail-Anhangs, aber auch durch das Anschließen eines USB-Sticks. Wie immer gilt: Mit Vorsicht und ein paar Schutzmaßnahmen können Sie die Gefahren reduzieren. Unsere Tipps um sich gegen Schadsoftware zu schützen:

Virenschutz-Software:
Das A und O beim Schutz gegen Schadsoftware ist ein Virenscanner. Dieser prüft alle neu heruntergeladenen Programme, um sicherzugehen, dass sie keine Malware enthalten. Er scannt den Computer regelmäßig, um Schadsoftware, die trotzdem Eingang gefunden hat, aufzuspüren und zu entfernen. Er sollte regelmäßig aktualisiert werden, um alle aktuellen Bedrohungen zu erkennen. Ein guter Virenschutz kann auch zuvor unbekannte Malware-Bedrohungen anhand von gemeinsamen Merkmalen erkennen.



Firewall:
Eine Firewall ist sozusagen ein digitaler Türsteher für ein Netzwerk oder einen Rechner. Sie stellt sicher, dass kein Netzwerkverkehr unerlaubt an ihr vorbeirauscht, sodass Schädlinge wie Trojaner oder Internet-Würmer gar nicht erst ins System gelassen werden. Damit die Sicherheit gewährleistet ist, sollten Sie die Firewall in aller Regel nicht abschalten.

Kein Administratorkonto:
Verwenden Sie nach Möglichkeit kein Administratorkonto, welches zum Installieren neuer Software berechtigt. Legen Sie stattdessen für die Internetnutzung ein Benutzerkonto mit eingeschränkten Rechten an, um zu verhindern, dass Malware auf Ihrem Computer installiert wird.

Dateianhänge:
Öffnen Sie keine ungeprüften Dateianhänge. Löschen Sie verdächtige E-Mails mit Anhang von fremden Personen. Manchmal handelt es sich hierbei nur um Spam, oftmals enthalten Sie aber auch Malware. Seien Sie kritisch bei ausführenden Programmdateien (erkennbar an der Endung .exe) oder Zip-Dateien.

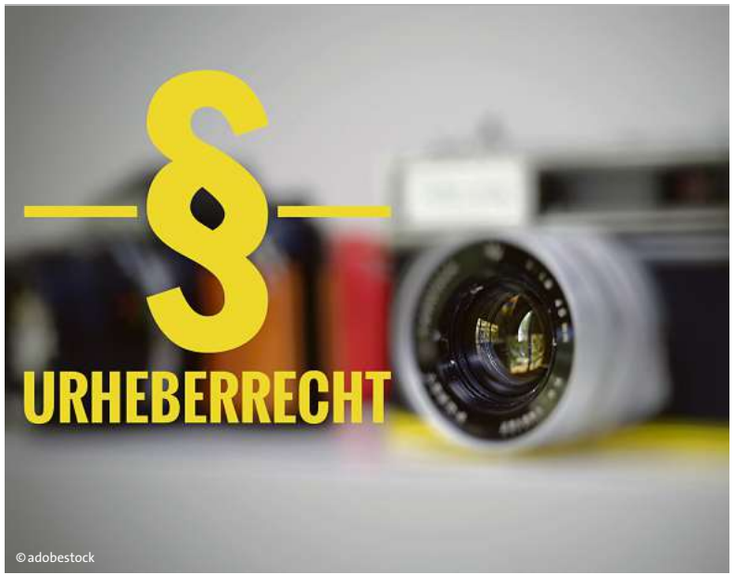
Computer und Software immer aktuell halten:
Installieren Sie stets die neuesten Updates für Ihr Betriebssystem und andere Software.

Urheberrecht und das Recht am eigenen Bild im Internet

Bilder, Videos und Musik sind im Internet leicht zu bekommen. Schnell ist das passende Foto gefunden – und auf der eigenen Website oder dem Facebook-Kanal geteilt. Doch beachten Sie: Nicht alle Daten dürfen von jedem einfach so verwendet werden.

Die virtuelle Welt ist kein rechtsfreier Raum, auch im Internet müssen alle Teilnehmer Regeln befolgen. Zwei wesentliche Bereiche sind das Urheberrecht sowie das Recht am eigenen Bild.

Urheberrecht: Im Internet Inhalte zu finden und diese dann mit anderen zu teilen ist kinderleicht. Die Verwendung von fremden Inhalten ohne die Erlaubnis des Rechteinhabers ist aber grundsätzlich illegal, denn nur der Urheber eines Werkes (z.B. eines Bildes, Videos oder Songs) entscheidet, wofür es verwendet werden darf – frei zugänglich heißt nicht frei verwendbar. Um das Werk eines anderen nutzen zu dürfen, benötigt man also dessen Erlaubnis. Es sei denn, das Urheberrechtsgesetz gestattet die Nutzung in speziell geregelten Fällen (z.B. das Zitat oder die Privatkopie) auch ohne eine solche. Es wird geraten, genau darauf zu achten, für welchen Nutzen der Inhalt freigegeben wurde und ihn dann auch nur dafür zu verwenden. Am besten, man holt sich immer die Genehmigung des Urhebers. Manchmal ist für die Nutzung eines Werkes auch eine Vergütung zu entrichten.

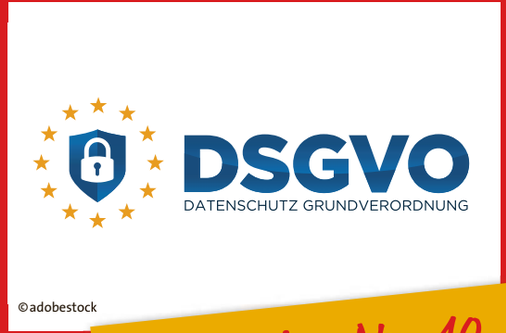


Im Internet gibt es diverse Datenbanken, bei denen Lizenzen an Bildern, Musik, Videos, Spielen usw. erworben und diese Inhalte damit rechtlich einwandfrei genutzt werden können. Man sollte aber beispielsweise kein geschütztes Musikstück in eine Tauschbörse stellen, da dann zivilrechtliche Konsequenzen drohen würden.

Das Recht am eigenen Bild: Das Recht am eigenen Bild stellt ein im Grundgesetz definiertes Element der Persönlichkeitsrechte dar. Verschiedenste Vorschriften sollen die Entfaltung der Persönlichkeit sicherstellen und den Schutz vor Eingriffen in die Lebens- und Freiheitsbereiche gewährleisten. Nur die abgebildete Person darf entscheiden, welches Bild von ihr veröffentlicht werden darf und welches nicht. Das gilt sogar auf Fotos, auf denen die Person nur aufgrund von auffälligen Merkmalen (z.B. eine Tätowierung) eindeutig zu erkennen ist. Denken Sie daran, dass das Recht am eigenen Bild auch für Freunde, Arbeitskollegen oder Familienmitglieder gilt. Auch hier dürfen Sie das Bild ohne Erlaubnis des Gezeigten nicht einfach im Internet verbreiten.

Es gibt einige rechtliche Stolperfallen im Internet, deshalb empfiehlt die Kreissparkasse Rottweil, sich im Zweifel juristische Hilfe zu holen. Der Text stellt keine Rechtsberatung dar, sondern ist lediglich eine kurze Zusammenfassung des Themas um zu sensibilisieren.

DSGVO: Die Datenschutz-Grundverordnung



User Tipp Nr. 10

Hinter der DSGVO verbirgt sich die Verordnung, die in der Europäischen Union den Umgang mit Daten regelt. Sie trat am 25. Mai 2018 in Kraft. Ziel der Verordnung ist es, ein einheitliches Datenschutz-Niveau in der gesamten EU zu schaffen. Sie als Verbraucher profitieren durch die DSGVO von einem größeren Schutz Ihrer Daten. So gibt es z.B. ein „Recht auf Vergessenwerden“, was vor allem für die Nutzung von Internet-Diensten wie Google oder Facebook große Bedeutung hat.

Was hat das mit Ihrer Sparkasse zu tun?

Wir haben unsere Datenschutzstandards an die DSGVO angepasst und unsere Kundinnen und Kunden darüber informiert. Schon davor haben wir aber den sehr hohen Datenschutz-Ansprüchen genügt und werden das auch weiterhin tun. Von einem Großteil unserer Kundinnen und Kunden liegt uns die DSGVO-Einwilligung mittlerweile vor. Mit Ihrer Einwilligung stimmen Sie zu, dass Ihre Sparkasse personenbezogene Daten nutzt, um Sie weiterhin im gewohnten Maße entsprechend Ihren Bedürfnissen und Ihren Wünschen individuell zu beraten. Ihre Daten machen es möglich, für Sie relevante Produkte und Services zu erkennen und Ihnen maßgeschneiderte Angebote zu unterbreiten. Das spart Zeit, reduziert die Werbeflut und bringt Ihnen Informationsvorteile. Für eine bestmögliche Beratung arbeitet Ihre Sparkasse mit spezialisierten Unternehmen der Sparkassen-Finanzgruppe zusammen: zum Beispiel mit der Landesbausparkasse, der Deka und regionalen Versicherungspartnern. Auch hier gewährleistet Ihre Sparkasse, dass mit Ihren Daten sicher und sorgsam umgegangen wird.

Kreissparkasse Rottweil

Tipps für barrierefreie Internetseiten

Hinter Barrierefreiheit steckt weit mehr als rollstuhlgerechte Einrichtungen. Auch das Internet sollte barrierefrei sein – für Menschen mit und ohne Behinderung, Senioren, Kinder und Eltern. Tipps für barrierefreie Internetseiten.

Wer gute Augen hat, nicht unter Farbenblindheit leidet oder die Computer-Maus problemlos mit seinen Fingern bewegen kann, hat sich vermutlich noch keine Gedanken darüber gemacht, ob Webseiten im Internet gut nutzbar sind. Sobald aber das Sehvermögen nachlässt und man seine Brille gerade nicht zur Hand hat, kann es zu ersten Beeinträchtigungen kommen. Eine zu kleine Schrift ist mühsam zu entziffern. Dieses ärgerliche Problem einer leichten Sehschwäche kann man mit einem Trick lösen: Drücken Sie in Ihrem Internet-Browser einfach die Tastenkombination „strg“ und „+“ um den Schriftgrad zu vergrößern. Wem die Tastatur aber Schwierigkeiten bereitet, erhält in Online-Shops Angebote für Tastaturen mit extra großen Tasten oder kontrastreichen Beschriftungen. Hilfreich wäre es jedoch, wenn Websites von vornherein ein paar Grundsätze erfüllen würden, um bedienerfreundlich und dann auch barrierefrei zu sein:

Große Bedienflächen: Manche User tun sich schwer damit, kleine Schaltflächen und Links anzuklicken, besonders mit dem Finger auf dem Smartphone.

Bildbeschreibungen: Für Blinde sind Bilder mit sogenannten Alternativtexten sehr wichtig, da Vorlese-Anwendungen Bildbeschreibungen für die Sprachausgabe des Inhalts nutzen.

©adobestock

Verständliche Sprache: Jedem Nutzer hilft es, wenn auf Fremdwörter weitgehend verzichtet wird und die Sätze kurz und klar strukturiert sind.

Logische Struktur: Eine logische Struktur im Aufbau einer Internetseite, eine Einteilung in einen Navigationsbereich und einen Bereich mit Seiteninhalt, trägt zur leichteren Orientierung bei. Innerhalb dieser Bereiche gibt es Überschriften, Fließtexte oder Listen. Gerade Überschriften innerhalb eines Internetauftritts sind für Menschen, die auf Sprachausgabe angewiesen sind, eines der wichtigsten Mittel, um sich zurechtzufinden.

Ausreichend große Schrift: Ist z.B. die Produktbeschreibung eines Angebots bei einem Online-Shop zu klein oder nur schwer lesbar, bereitet das allen Kunden Schwierigkeiten, sich richtig zu informieren und die wenigsten werden dort etwas kaufen.

Farbkontraste: Schwache Farbkontraste erschweren es Besuchern der Internetseite, den Inhalt schnell zu konsumieren, da Text und Hintergrund zu einer Fläche verschwimmen.

Mit wenigen und sehr einfachen Maßnahmen also ermöglicht man allen – nicht nur Menschen mit Handicap – eine bequemere Nutzung des Internets, wenn einige grundlegende Dinge beachtet werden.

Kids, Eltern und das Internet

Wie können Eltern ihre Kinder begleiten, für eine verantwortungsvolle Nutzung des Internets? Wir haben Tipps für Sie zusammengetragen.

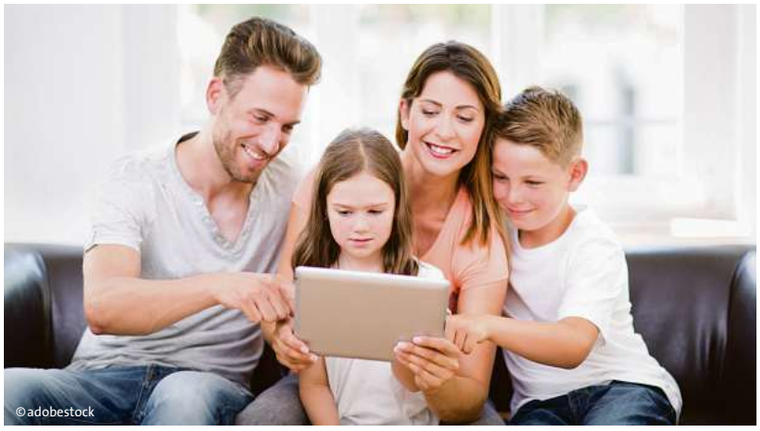
Kids und Jugendliche wachsen mit den neuen Medien inzwischen wie selbstverständlich auf. Sie surfen im Internet, verwenden Smartphones und sind in sozialen Netzwerken zu Hause.

Wir haben auf www.klicksafe.de – der EU-Initiative für mehr Sicherheit im Netz – für Sie recherchiert. Ein paar der Tipps haben wir hier für Sie zusammengestellt:

Nutzungszeiten vereinbaren: Vereinbaren Sie gemeinsam mit Ihren Kids Internetnutzungszeiten. Für Kinder von 10 bis 13 Jahren werden ca. 60 Minuten täglich empfohlen. Aber auch mit älteren Kindern sollten Nutzungszeiten besprochen werden, um exzessivem Online-Konsum vorzubeugen. Mit zunehmendem Alter sollten die Eltern sich mehr und mehr zurücknehmen und dem Jugendlichen mehr Freiraum geben, ein zeitlicher Richtwert ist hier aber aufgrund verschiedener persönlicher und familiärer Situationen schwierig zu definieren. Achten Sie darauf, dass noch genügend Zeit für Schule, Ausbildung und andere Hobbies bleibt.

Vorbild sein: Eltern haben auch hier eine Vorbildfunktion. Nutzen Sie selbst das Internet mehrere Stunden am Tag? Wie oft schauen Sie auf Ihr Smartphone? Seien Sie sich bewusst, dass sich Kinder sehr viel von ihren Eltern abschauen – auch im Umgang mit den Medien.

Kommunikation: Möglicherweise findet Ihr Kind Kontakte und Freunde im Internet und sozialen Netzwerken. Sprechen Sie miteinander: Mit wem steht Ihr Kind in Kontakt? Welche Erlebnisse macht es im Internet? Welche Inhalte findet es interessant oder seltsam?


©adobestock

Gemeinsam surfen: Lassen Sie sich von Ihren Kindern zeigen, wo diese gerne surfen. So erhalten Sie einen guten Einblick in das Surfverhalten und die Interessen Ihrer Kinder. Sollten Sie bestimmte Inhalte und Seiten untersagen wollen, begründen Sie dies immer. In der Regel verstehen Kinder dann Ihre Sorge.

Über Rechte im Netz aufklären: Sprechen Sie mit Ihrem Kind über Rechte, die im Internet beachten werden müssen. Insbesondere das „Recht am eigenen Bild“ sowie das „Urheberrecht“ sind wichtige Regelungen.

Technischer Schutz: Vor allem für jüngere Kinder ist es sinnvoll als ergänzende Maßnahme Filterprogramme, die problematische Inhalte blockieren, beim Surfen einzusetzen. Viel wichtiger ist aber, dass Sie ihren Kindern vertrauen und ihnen beim Einstieg ins Internet zur Seite zu stehen.

Für den Datenschutz sensibilisieren: Sprechen Sie mit Ihren Kindern über Datenschutz. Ein Grundsatz lautet: Das Netz vergisst nichts! Sie schützen ihre Kinder am besten vor Online-Risiken, wenn sie ihnen einen vorsichtigen, kritischen und selbstbestimmten Umgang mit privaten Daten im Internet vorleben und nahebringen.

Über Gefahren im Internet aufklären: Thematisieren Sie auch die Themen Virenschutz, sichere Passwörter und generell Sicherheit im Internet. Was für Sie selbst gilt, gilt natürlich auch für Ihren Nachwuchs: verdächtige E-Mails löschen, Betriebssysteme, Software und Anti-Viren-Programme stets auf dem aktuellen Stand halten, u.v.m.

Weitere Infos zum Thema finden Sie auf **www.klicksafe.de**

Online bequem den Kontostand abfragen.

Im Online-Banking oder in der App „Sparkasse“.

Mehr Infos unter www.ksk-rw.de

ksk-rw.de

Wenn’s um Geld geht

Kreissparkasse Rottweil