Rat und Hilfe für Verbraucher in Europa

ECC-Net

Europäisches Verbraucherzentrum Österreich

Sicher zahlen im Web

Die gängigsten Zahlungsformen im Vergleich

Mag. Georg Mentschl
Leiter des Europäischen
Verbraucherzentrums
Österreich

Liebe Leserin, lieber Leser,

die Informations- und Netzwerktechnologien haben sich in den letzten Jahren rasant weiterentwickelt. Einkaufen im Internet liegt voll im Trend. Unternehmen aus der ganzen Welt wittern ihre Chance, durch günstige Preise neue Kunden in Österreich zu werben.
Was man schon vor dem Einkauf im Internet wissen und während des Zahlungsvorganges beachten sollte, haben wir auf den folgenden Seiten für Sie übersichtlich zusammengefasst. Wir möchten Ihnen damit ermöglichen, angebotene Zahlungsmethoden hinsichtlich Kundenfreundlichkeit und Risiko zu bewerten und die Ihren Bedürfnissen entsprechende Form zu wählen.

Denn wer gute Informationen hat, der ist bekanntlich im Vorteil. Das sieht auch die Generaldirektion für Justiz der Europäischen Kommission so, die diese Broschüre finanziell unterstützt. Sollte es dennoch zu Problemen mit einem Unternehmen im europäischen Ausland kommen, dann gibt es beim Europäischen Verbraucherzentrum kompetente Hilfe. Weitere nützliche Informationen zu Konsumententhemen finden Sie auf ***www.europakonsument.at****, der Website des Europäischen Verbraucherzentrums Österreich, sowie auf unserer Facebookseite* ***https://www.facebook.com/europakonsument.at.***

Sicher ist sicher

Bezahlen auf Rechnung
Am sichersten ist es, bestellte Ware erst zu bezahlen, wenn man sie erhalten hat. Wird Ihnen diese Möglichkeit angeboten, dann sollten Sie nicht zögern, diese Variante zu wählen. Nur so haben Sie die Möglichkeit, zunächst einmal abzuwarten, ob die Ware überhaupt kommt, und dann zu überprüfen, ob sie in Ordnung ist und mit der Bestellung übereinstimmt. Das Risiko dieser Variante ist null.

Zahlen per Nachnahme
Unter Nachnahme versteht man eine Versand- und Zahlungsart, bei der die Bezahlung einer Ware beim Empfang derselben durch den Empfänger an das ausführende Post- bzw. Logistikunternehmen erfolgt. Auch dieses Verfahren ist risikolos, da Sie hier jedenfalls die Sicherheit haben, erst zu bezahlen, wenn die Ware eingetroffen ist. Zu empfehlen ist allerdings, sich vom Boten nicht stressen zu lassen, sondern in aller Ruhe zu untersuchen, ob das, was da geliefert wurde, auch dem Bestellten entspricht und in Ordnung ist, insbesondere keine Transportschäden aufweist. Im gegenteiligen Fall sollten Sie die Annahme verweigern und auch nichts bezahlen. Selbstverständlich sollten Sie sich die Zahlung bestätigen lassen! Wenn Sie all das beachten, ist das Risiko ebenfalls null, Sie müssen allerdings eine Nachnahmegebühr in Kauf nehmen.

Zahlung per Online-Überweisung
Diese Zahlungsmethode zählt zu den beliebtesten bei Online-Einkäufen. Der Verkäufer schickt die Ware erst ab, wenn der Kaufpreis auf seinem Konto eingelangt ist. Die Möglichkeit, die Ware vorher zu prüfen, besteht nicht. Der Käufer ist also auf Rückforderungsansprüche beschränkt, falls die Lieferung nicht der Bestellung entspricht. Die Möglichkeit, eine Überweisung „zurückzuholen", nachdem sie auf dem Konto des Empfängers angekommen ist, hat die Bank nämlich nicht. Sie sollten daher genau überprüfen, wem Sie da gerade Geld überweisen, sonst kann es schlimmstenfalls passieren, dass sich der Verkäufer als Betrüger herausstellt und mitsamt dem Geld untertaucht.
Alle größeren Banken bieten mittlerweile die Option an, Überweisungen online durchzuführen. Als Kunde melden Sie sich auf dem Rechner der Bank mit Kundendaten beziehungsweise Kontonummer und PIN an. Das Überweisungsformular füllen Sie direkt digital aus und schicken es ab. Als zusätzliche Sicherheit und Ersatz der Unterschrift dient die TAN (Transaction Number), eine Sicherheitsnummer, die Sie nur für eine einzige Überweisung verwenden können und die danach verfällt. Früher übermittelten Banken dem Kunden Listen mit mehreren TANs, die allesamt bis zu ihrer Verwendung gültig waren. Um das Risiko durch Diebstahl

von TANs zu minimieren, haben die meisten Banken jedoch mittlerweile auf mobile TANs umgestellt, die dem Kunden nach Ausfüllen des Überweisungsformulars auf sein Mobiltelefon übermittelt werden und nur kurze Zeit gültig sind. Dieses Verfahren nimmt einem Betrüger die Möglichkeit, eine Liste mit mehreren TANs an sich zu bringen, die längere Zeit verwendbar sind. Das System bietet jedoch nur dann einen Gewinn an Sicherheit, wenn das Onlinebanking selbst auf einem anderen Gerät durchgeführt wird als der Empfang der TAN-SMS. Andernfalls kann ein auf diesem Gerät installierter Trojaner sämtliche für eine Überweisung nötigen Daten abfangen und unbemerkt weiterleiten.

Die Gefahr, dass Bankdaten Internetbetrügern in die Hände fallen, droht praktisch nur auf dem eigenen Rechner, falls dort unbemerkt Schadsoftware installiert wurde und Daten aufzeichnet. Solange die Überweisung auf der tatsächlichen Website der Bank durchgeführt wird, besteht kaum ein Risiko, dass die Daten auf dem Weg zwischen Kunden und Bank abgefangen werden. Die Verbindung ist verschlüsselt und die Rechner von Banken sind ausreichend gesichert. Wer also über ausreichenden Virenschutz verfügt, sich vor Trojanern und ähnlicher Spyware schützt und regelmäßig Sicherheitsupdates durchführt, hat keinen Datendiebstahl bei der Onlineüberweisung zu befürchten.

Fotos: Bacho, Rocketclips / Shutterstock.com

Tipp: Empfang von TAN-SMS und Onlinebanking sollten auf unterschiedlichen Geräten erfolgen. Das neue secTAN-Verfahren ist mit einer Handy-App verknüpft und entspricht einer TAN-SMS.

Lastschriftverfahren

Einzugsermächtigung. Das Einzugsermächtigungsverfahren besteht darin, dass Sie Ihren Gläubiger (also etwa einen Zeitungsverlag) ermächtigen, von Ihrem Konto Geld abzubuchen. Eine solche Ermächtigung kann mittels eines schriftlichen Formulars, aber auch online erfolgen. Natürlich müssen Sie dafür sorgen, dass Ihr Konto ausreichende Deckung aufweist. Was aber, wenn Sie Grund dazu haben, Ihre Zahlungsverpflichtung im Nachhinein anzuzweifeln (der Betrag erschien Ihnen merkwürdig hoch), oder wenn der Gläubiger (die Zeitung) versuchen sollte, das Konto „abzuräumen"? Das Gesetz ermöglicht es Ihnen, überhöhte Abbuchungen binnen 56 Tagen ab dem Tag der Abbuchung rückgängig zu machen. Sie bekommen Ihr Geld dann auch tatsächlich wieder auf Ihrem Konto gutgeschrieben, allerdings nur, wenn der Betrag wirklich überhöht war. Das Zurückholen geht also nicht, wenn Sie die genaue Höhe des Betrags bereits im Vorhinein ausdrücklich mit dem Gläubiger vereinbart hatten oder Sie mit der Höhe des Betrags ohnehin rechnen mussten. Haben Sie also beispielsweise im letzten Monat einige längere Telefonate ins Ausland geführt und war Ihre Telefonrechnung dann höher als sonst (damit mussten Sie rechnen), können Sie die Überweisung nicht rückgängig machen. Sehr wohl aber können Sie eine Überweisung rückgängig machen, wenn Ihr Gläubiger (die Zeitung) plötzlich mehr abbucht als sonst.

Die meisten größeren Banken ermöglichen es Ihnen, dass Sie die Abbuchung (binnen 56 Tagen) auch dann rückgängig machen können, wenn der abgebuchte Betrag gar nicht überhöht war, also auch dann, wenn Sie genau wussten, dass dieser Betrag abgebucht werden wird.

Somit können Sie das Geld bei diesen Banken auch dann binnen 56 Tagen zurückverlangen, wenn die Höhe des Betrags ausdrücklich im Vorhinein mit dem Gläubiger (beispielsweise einer Zeitung) vereinbart war und Sie aber im Anschluss mit der Leistung unzufrieden waren – einfach, indem Sie die Rückerstattung verlangen, ohne Wenn und Aber. Ob auch Ihre Bank das so macht, kann nur ein Blick in die aktuellen Geschäftsbedingungen klären bzw. sollten Sie sich telefonisch mit Ihrem Berater in Verbindung setzen.

Fotos: Bjoern Wylezich / Shutterstock.com BilderBox.com

SEPA-Lastschriftverfahren. Seit Oktober 2014 gibt es das europaweit gleiche SEPA-Lastschriftverfahren:

Dieses entspricht dem inländischen Einzugsermächtigungsverfahren, und die Banken dürfen (auch wenn der Empfänger im Ausland ist) erfreulicherweise auch keinen Cent mehr dafür verlangen. Einziger Unterschied zu dem davor im Inland verwendbaren Einziehungsauftrag ist der Name des Verfahrens – und dass Sie anstatt der gewöhnlichen Kontonummer die europäischen IBAN- und BIC-Codes angegeben müssen. Auch beim SEPA-Lastschriftverfahren können Sie innerhalb von 56 Tagen die Erstattung des bereits abgebuchten Betrags verlangen – und zwar ohne jede Begründung. Zusätzlich kann die Zahlung im Falle einer „unautorisierten Lastschrift", also, wenn kein gültiger Auftrag für die Abbuchung vorliegt, sogar 13 Monate lang zurückgerufen werden.

Fazit: Solange man durch regelmäßige Kontrolle der Kontoauszüge den Überblick über den eigenen Zahlungsverkehr behält, sind Lastschriftverfahren mehr oder weniger risikolos, da Sie ungerechtfertigte Abbuchungen (mitunter mit gewissem Aufwand) rückgängig machen können.

Bezahlen mit Kreditkarte

Das Bezahlen mit Kreditkarte gehört zu den häufigsten Zahlungsformen im Internet. Wenn die Bezahlung über einen sogenannten „Secure Socket Layer", abgekürzt SSL, abgewickelt wird (was im Moment des Bezahlvorgangs aufscheint), dann können Außenstehende nicht auf den Datenfluss zugreifen. Diese Form der Online-Nutzung einer Kreditkarte ist in Wahrheit sicherer, als die Kreditkarte dem Kellner in einem dubiosen Lokal in die Hand zu drücken, der sie im Hinterzimmer schnell missbräuchlich verwendet. Aber was, wenn das Geld zwar abgebucht wurde, Sie die Ware aber nicht erhalten? Ist das Geld dann weg? Nein, nicht unbedingt. Denn Kreditkartenzahlungen können unter Umständen noch lange nach der Transaktion rückgebucht werden („chargeback"), wenn der Käufer dies von seinem Kreditkartenunternehmen verlangt. Die Frage ist allerdings, ob der Karteninhaber dem Kartenunternehmer nachweisen kann, dass die Zahlung ungerechtfertigt ist.

Beachten Sie aber, dass die Zahlung mit Kreditkarte dem Charakter als Anweisung nach (Sie weisen das Kreditkartenunternehmen an, an Ihren Gläubiger zu zahlen) grundsätzlich unwiderruflich ist – „was liegt, das pickt". Jede Art der Rückgängigmachung der Zahlung ist eine Serviceleistung des Kartenunternehmens. Wie und unter welchen Bedingungen diese Serviceleistung erfolgt, ist in den (meist nur internen) „quality regulations" oder „rule books" festgeschrieben. Bei einem Fall glatter Nichtlieferung führen Kreditkartenunternehmen in aller Regel eine Rückbuchung durch. Heikler wird es, wenn die Lieferung zwar erfolgt ist, die Ware aber mangelhaft war. Ihr Kreditkartenunternehmen wird Ihnen sagen, welche Informationen es in einem solchen Fall von Ihnen benötigt. Beachten Sie, dass Sie jedes Verhalten, das Ihnen als Mitverschulden ausgelegt werden kann, unterlassen sollten. Halten Sie daher insbesondere die im konkreten Fall gegebenen Reklamationsfristen gegenüber Ihrem Vertragspartner ein!

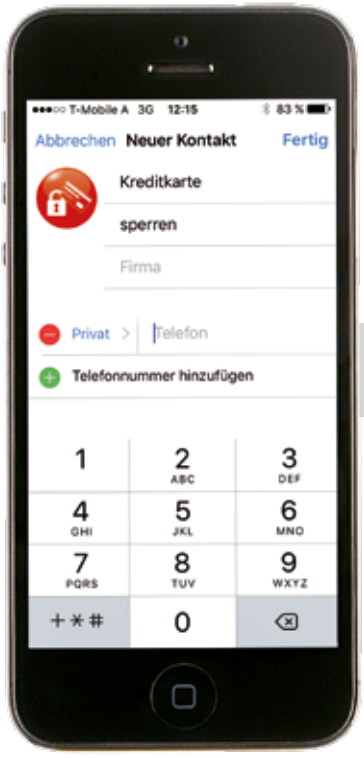
Vorsichtsmaßnahmen

- Achten Sie darauf, beim Online-Bezahlen mit Kreditkarte ausschließlich über das HTTPS-Protokoll zu kommunizieren. Dieses Protokoll wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im WWW verwendet. Ohne diese Verschlüsselung sind Ihre Kreditkarten-Daten für jeden als Klartext lesbar!
- Besonders riskant wird es, wenn Sie unterwegs sind und mobil über einen WLAN-Hotspot kommunizieren.
- Auch der Hinweis, dass Sie ab einem bestimmten Moment der Transaktion über SSL („Secure Socket Layer") kommunizieren, gibt Ihnen die Sicherheit, dass unerwünschte „Mitleser" Ihre Daten nicht auslesen können.

Foto: Yulia Grigoryeva / Shutterstock.com

Foto: graja / Shutterstock.com

- Beachten Sie auch die Hinweise, die Sie mittels Pop-up bekommen, dass Ihr Gegenüber über kein Sicherheitszertifikat verfügt, bzw. die Warnung, dass Sie die Website, auf der Sie sich gerade befinden, nicht benutzen sollen, und stellen Sie die Sicherheitseinstellungen in Ihrem Browser auf die höchste Stufe.
- Bei der Zahlung über Visa oder Mastercard hilft der Hinweis „Verified by Visa" bzw. „MasterCard SecureCode": Das bedeutet, dass der Händler beim Kreditkartenunternehmen registriert ist, verschafft Ihnen also die Sicherheit, dass es diesen Händler tatsächlich gibt, und gibt dem Händler andererseits die Sicherheit, dass Sie tatsächlich derjenige sind, als der Sie sich mit der Kreditkarte ausweisen (es sei denn, Sie hätten den Zugangscode weitergegeben, was nicht empfehlenswert ist).
- Wenn Sie daher im Internet mittels Kreditkarte einkaufen, so empfiehlt es sich, alle Fakten (am besten mit Screenshots) zu dokumentieren (Händler, Ware, zugesicherte Eigenschaften, Datum der Transaktion, E-Mail-Verkehr mit dem Händler), um dann, wenn etwas schiefgeht, dem Kreditkartenunternehmen präzise alle Details mitteilen zu können. Das Kreditkartenunternehmen wird dann vorbehaltlich der Erledigung zu Ihren Gunsten eine Rückbuchung vornehmen. Gelingt es Ihnen nicht, das Kreditkartenunternehmen von der Richtigkeit Ihrer Behauptungen zu überzeugen, würde die Rückbuchung abermals rückgängig gemacht, Ihr Konto also endgültig belastet werden.



Was passiert bei Missbrauch?

Die Allgemeinen Geschäftsbedingungen (AGB) der Kreditkartenunternehmen sehen im Allgemeinen vor, dass im Fall eines Kartenmissbrauchs – wenn also einer Transaktion in Wahrheit gar keine Zahlungsanweisung des Karteninhabers zugrunde lag – das Kartenunternehmen den angelasteten Betrag unverzüglich rückerstattet und das belastete Zahlungskonto wieder auf den ursprünglichen Stand bringt. Der erste Schritt sollte also sein, dass Sie in einem solchen Fall die Kreditkarte sperren lassen (wozu das Kreditkartenunternehmen verpflichtet ist), um in weiterer Folge die Rückbuchung zu verlangen.

Der Anspruch auf Rückbuchung (sogenannter Berichtigungsanspruch) besteht jedenfalls, sobald der Kunde behauptet und schlüssig darlegt, dass die konkrete Zahlung nicht von ihm autorisiert war. Ihn trifft diesbezüglich eine sogenannte „Rügeobliegenheit", d.h., er muss unverzüglich nach der Feststellung (etwa durch Kontrolle des Kontoauszuges) bzw. längstens binnen 13 Monaten das Kreditkartenunternehmen darauf hinweisen. Dann hat der Kunde Anspruch darauf, dass die fraglichen Beträge zurückgebucht werden.

Davon zu unterscheiden ist allerdings die Frage, wen der Schaden letztlich trifft bzw. wer dafür haftet: Trifft den Kunden an der missbräuchlichen Verwendung seiner Kundendaten oder der Zahlungskarte nämlich keinerlei Verschulden, kann er auch nicht zur Haftung herangezogen werden. Hier empfiehlt es sich, die Geschäftsbedingungen des jeweiligen Kartenunternehmens durchzulesen, in denen grundsätzlich beschrieben wird, wie man seine Karte sicher im Internet nutzen kann bzw. welche Sicherheitsvorkehrungen einzuhalten sind. Trifft den Kunden allerdings ein Verschulden an der missbräuchlichen Nutzung seiner Kundendaten durch Dritte, dann gelten folgende Haftungsregelungen: Das Kreditkartenunternehmen muss das Verschulden behaupten und beweisen. Bei Vorsatz und grober Fahrlässigkeit des Karteninhabers haftet dieser für den gesamten Schaden, bei leichter Fahrlässigkeit bis 150 Euro; in beiden Fällen nur bis zur (unverzüglichen) Meldung des Verlustes der Karte bzw. der Kartendaten. Nach der Meldung haftet der Kunde nicht mehr. Der Kunde haftet auch nicht, wenn das Kreditkartenunternehmen auf die Meldung des Verlustes bzw. auf den Wunsch nach Sperre der Karte nicht ordnungsgemäß reagiert.

Tipp: Speichern Sie die Notrufnummern zur Kartensperre von Bank bzw. Kreditkartenorganisation in Ihrem Handy ab.

Bezahlen mit PayPal

Wem Online-Überweisungen und Zahlung per Kreditkarte zu unsicher sind oder wer seine Daten nicht dem Verkäufer direkt bekannt geben möchte, der kann auf PayPal zurückgreifen. Dabei muss der Kunde sein PayPal-Konto irgendwie dotieren, sei es durch Bareinzahlung oder mittels Kreditkarte, durch Abzug mittels Lastschriftverfahren oder über Giropay vom eigenen Bankkonto. Der Zahlungsdienst tritt als eine Art Vermittler zwischen Verkäufer und Endkunde auf: PayPal streckt den Kaufpreis vor, überweist ihn dem Verkäufer und bucht ihn erst danach dem Kunden von seinem Konto ab. Der Verkäufer hat den Vorteil, dass er die Ware unmittelbar nach der Bestellung abschicken kann, weil er sofort die Zahlung erhält, und PayPal kassiert vom Verkäufer Provision für jeden Auftrag. Für den Kunden hat diese Zahlungsmethode den Vorteil, dass er seine Bankdaten nicht irgendeinem Onlinehändler bekannt geben muss, sondern ausschließlich PayPal. Er muss auf der Website des Verkäufers nur mehr seine PayPal-Zugangsdaten eingeben, um zu bezahlen.

So weit, so gut, was die Sicherheit anbelangt – es besteht allerdings immer noch die Möglichkeit, dass es Internetbetrügern gelingt, Ihre PayPal-Zugangsdaten auszuspionieren. Um zu verhindern, dass derjenige dann über den PayPal-Zugang Abbuchungen von Ihrem Bankkonto vornehmen kann, ist es ratsamer, PayPal keinen Lastschriftauftrag zu erteilen. Die sicherste Methode ist, bei Bedarf Geld auf das PayPal-Konto zu überweisen und nur auf diesem Weg zu bezahlen. Gelangt jemand in den Besitz der Zugangsdaten, kann er dann nur auf den Betrag auf dem PayPal-Konto zugreifen – und nicht über den Umweg der PayPal-Zahlung das Bankkonto leer räumen.

Käuferschutz. Als zusätzlichen Service lockt PayPal Kunden mit dem sogenannten „Käuferschutz", bei dem es allerdings in manchen Fällen – so unsere Erfahrungen im EVZ – immer wieder Probleme gibt. Der Zahlungsdienst erstattet dem Kunden, falls die Ware nicht oder mangelhaft geliefert wird, den Kaufpreis mitsamt den Versandkosten zurück und regelt die Rückforderung des Kaufpreises direkt mit dem Verkäufer – so weit das Versprechen. Während der Verkäufer die erfolgte Kreditkartenrückbuchung anficht, belastet PayPal einstweilen das Konto des Verkäufers mit dem entsprechenden Betrag und untersucht den Fall. Wird die Untersuchung zugunsten des Verkäufers abgeschlossen, entschädigt das Kreditkarteninstitut PayPal für die Kreditkartenrückbuchung, und PayPal schreibt den zurückerhaltenen Betrag wieder dem Verkäufer gut.
Das kann natürlich dauern – und was bei dieser Untersuchung herauskommt, steht in den Sternen. Wurde der Kauf aber mit einer gestohlenen Kreditkarte bezahlt, so hat der Verkäufer Pech. Einer Erstattung muss zunächst PayPal zustimmen (und das nach einer oft wochenlangen Prüfung); nicht selten verlangt PayPal auch noch relativ lange Zeit nach der Transaktion Belege oder sogar, dass der angeblich Geschädigte den Verkäufer strafrechtlich anzeigt (viel Glück damit in einem weit entfernten Land!); außerdem wird zunächst das Konto des Geschädigten mit den Gebühren der Rückabwicklung belastet. Natürlich sollte man in allen Fällen des Online-Betrugs Strafanzeige erstatten. Sitzt der Geschäftspartner jedoch im Ausland, dann kann es schon schwierig werden.
Bei entsprechend achtsamer Handhabung handelt es sich bei PayPal um eine verlässliche und risikoarme Zahlungsmethode. Bei Onlinekäufern zählt PayPal zu den beliebtesten Arten, zu bezahlen, und auch Verkäufer bieten den Dienst verstärkt an.

Tipp für Konsumenten, wenn sie als Verkäufer auftreten. Dokumentieren Sie den Verkauf möglichst detailliert und sammeln Sie verlässliche Daten über den Käufer. PayPal als Zahlungsmethode zu akzeptieren, kann für den Verkäufer mit einigem Risiko verbunden sein.

Das Zahlungsmittel Bitcoins

„Bitcoin" ist ein Kunstwort, das sich am ehesten mit „digitale Münze" übersetzen lässt, und bezeichnet ein experimentelles Zahlungsmittel, das sich erst in den letzten Jahren entwickelt hat. Es handelt sich um eine digitale Währung, die nicht aus Münzen oder Scheinen besteht, sondern nur aus Daten. Mit steigender Popularität der digitalen Münzen steigt auch die Anzahl der Onlineshops, in denen man damit bezahlen kann.

Dafür muss man sich eine virtuelle Geldbörse zulegen: Software, die auf dem Computer oder dem Smartphone installiert wird und die Aufbewahrung und Verwendung von Bitcoins möglich macht. Die Münzen können dann über Zwischenvermittler an jeden Bitcoin-Nutzer gesendet werden, dessen Adresse man kennt. Vorsicht ist dabei aber allemal geboten, die Zahlung kann nämlich nicht rückgängig gemacht werden. Außerdem birgt das digitale Geld, vor allem für unerfahrene Nutzer, große Sicherheitsrisiken. Bitcoins sind ein beliebtes Ziel für Hackerangriffe und Datendiebstahl. Es ist daher für Neueinsteiger in diese Zahlungsmethode unerlässlich, sich ausreichend über geeignete Sicherheitsmaßnahmen zu informieren.

Foto: igorstevanovic / Shutterstock.com

Rat und Hilfe für Verbraucher in Europa ECC-Net

Finanziell unterstützt durch die Europäische Union

Eine Initiative der Europäischen Kommission und des VKI

Sicher zahlen im Internet – Die wichtigsten Tipps

Daten verschlüsseln. Achten Sie darauf, dass die Seite, auf der Sie Ihre Daten bekannt geben, mit „https" beginnt. Das „s" steht für verschlüsselten Datentransfer und sollte bei allen Bank- und Geldtransaktionen Pflicht sein.

Security-Paket aktualisieren. Achten Sie darauf, dass auf Ihrem Computer oder Mobilgerät ein Sicherheitspaket installiert ist, und aktualisieren Sie es regelmäßig.

Schadenshöhe limitieren. Bei Prepaid-Karten oder beispielsweise der Paysafecard ist das Guthaben begrenzt, dadurch ist auch die Schadenshöhe bei missbräuchlicher Verwendung von vornherein limitiert.

Datenweitergabe begrenzen. Benutzen Sie (anonyme) Alternativen zu Kreditkarte & Co, bringen Sie Ihre Daten so wenig wie möglich in Umlauf – vor allem bei Lieferanten, bei denen Sie Zweifel haben.

Vorsicht vor Datennachfrage. Beantworten Sie keine Anfragen zu Ihren Codes – weder telefonisch, schriftlich noch per E-Mail (Phishing-Mails).

Karten sperren. Lassen Sie Ihre Karten bei Verlust, Diebstahl bzw. missbräuchlicher Verwendung sofort sperren! Speichern Sie die Notrufnummern in Ihrem Handy.

Auszüge kontrollieren. Kontrollieren Sie Ihre monatlichen Kontoauszüge, Kreditkarten-Abrechnungen sowie Ihre aktuellen Kartenzahlungen.

So gut wie möglich dokumentieren. Dokumentieren Sie alle Einkäufe und Bezahlvorgänge im Internet durch Screenshots.

Lassen Sie den Hausverstand walten. „Zu schön, um wahr zu sein" – was unglaublich gut klingt, ist meist auch im Internet mit einem Haken verbunden.

Rat & Hilfe kostenlos

Europäisches Verbraucherzentrum Österreich

Mariahilfer Straße 81
A-1060 Wien
www.europakonsument.at
www.facebook.com/europakonsument.at

EUROPA-HOTLINE: 01 / 588 77 81
Mo bis Fr von 9 bis 15 Uhr
E-Mail: info@europakonsument.at

Weitere hilfreiche Adressen

http://onlinesicherheit.gv.at
Österreichisches Portal mit Informationen zum Thema Sicherheit in der Informations- und Kommunikationstechnologie

http://ec.europa.eu/consumers/ecc/index_de.htm
Europäische Kommission; Netz der Europäischen Verbraucherzentren

www.konsumentenfragen.at
Das Konsumentenportal des Bundesministeriums für Arbeit, Soziales und Konsumentenschutz

www.vki.at
Verein für Konsumenteninformation

www.verbraucherrecht.at
Informationen zum Verbraucherrecht in Österreich

www.saferinternet.at
ÖIAT; unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren Umgang mit digitalen Medien

https://webgate.ec.europa.eu/odr
Plattform der Europäischen Union zur Online-Streitbeilegung

Impressum

Herausgeber und Medieninhaber
Verein für Konsumenteninformation
Mariahilfer Straße 81, 1060 Wien
ZVR-Zahl 389759993

Verlags- und Herstellungsort Wien

Grafische Gestaltung VKI/Herstellung

Cover-Foto Juergen Faelchle / Shutterstock.com

Druck Leykam Druck GmbH & Co KG, 7201 Neudörfl

Diese Broschüre entstand im Rahmen der „Action 670702 – ECC-Net AT FPA", für welche das EVZ Österreich Förderungen aus den Mitteln des Verbraucherprogrammes der EU (2014-2020) erhält.

Weitere Informationen zum ECC-Net finden Sie im Internet unter: http://ec.europa.eu/consumers/ecc/index_de.htm