Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Zahlungsmethoden für's Online-Shopping im Überblick

Die Tage, an denen man sich stundenlang durch überfüllte Kaufhäuser schlagen musste, sind schon lange vorbei. Heutzutage kann vieles in Online-Shops rund um die Uhr gekauft und von zu Hause aus bezahlt werden. Doch so bequem das Online-Shoppen auch ist, bringt es einige Gefahren mit sich. Bei der großen Auswahl an möglichen Zahlungsmethoden können Sie schnell die Übersicht verlieren. Welche Informationen müssen wirklich preisgegeben werden und wie steht es um die Sicherheit des jeweiligen Verfahrens? Wir stellen Ihnen gängige Zahlungsmethoden vor und zeigen auf, welche Sicherheitsaspekte zu beachten sind.

Grundsätzliche Regeln beim Online-Kauf

Achten Sie stets darauf, dass die Shops bei denen Sie einkaufen, **vertrauenswürdig** sind. **Prüfsiegel**, wie *Trusted Shops* oder *TÜV-Süd Safer Shopping* sind Anhaltspunkte dafür. Bei Online-Portalen wie *Ebay* oder *Amazon* kann man feststellen, wie sicher und vertrauenswürdig ein Verkäufer ist, indem man die **Verkäufer-Bewertungen sorgfältig liest**. Achten Sie besonders auf die Negativ-Bewertungen einzelner Käufer. Was wurde hier bemängelt?

Generell sollten Sie überprüfen, ob die Webseite, auf der Sie Ihre Zahlungs- oder Kontaktdaten eingeben, eine **SSL-Verschlüsselung** aufweist. Das können Sie zum einen daran erkennen, dass die Internetadresse mit *https* anstelle von *http* beginnt. Aktuelle Browser stellen eine verschlüsselte Verbindung mit Hilfe eines Schlosssymbols in der Statusleiste dar. Ein Klick darauf zeigt die Verschlüsselungsstärke sowie weiterführende Informationen zum so genannten ***SSL-Zertifikat*** an. Wird die Adresszeile zudem in Browsern wie dem *Mozilla Firefox* und Internet Explorer grün hinterlegt, nutzt die Webseite ein *Extended-Validation-SSL-Zertifikat*, kurz *EV-SSL-Zertifikat*. Ein *EV-SSL-Zertifikat* ist an eine strenge Vergabe gebunden, denn es wird nicht nur die Internetadresse, sondern auch das dahinterstehende Unternehmen von einer Zertifizierungsstelle überprüft, in dem unter anderem vor der Zertifikatsausstellung Kontakt mit der Personalabteilung aufgenommen wird. Um sicher zu gehen, dass Sie

Ihre Daten nicht über eine gefälschte Seite eingeben, vergleichen Sie daher die Organisation, für welche das Zertifikat ausgestellt ist, mit dem Namen des Unternehmens zu dem Sie Kontakt aufbauen wollen. So wird Ihnen zum Beispiel bei der Eingabe der Internetadresse: https://www.internet-sicherheit.de folgende Organisation im Zertifikat angezeigt, die die Domain internet-sicherheit.de betreibt: „Institut fuer Internet-Sicherheit (Fachhochschule Gelsenkirchen)“. Sollten Sie unsicher sein oder einen Unterschied feststellen, halten Sie **im Zweifelsfall telefonisch Rücksprache** mit dem Unternehmen oder Ihrer Bank. Sollten Sie eine E-Mail erhalten, in der Sie dazu aufgefordert werden, nach dem Klick auf einen scheinbar echten Link Ihrer Bank oder einer anderen Ihnen vertrauten Webseite, Bankdaten oder andere sensible Daten preiszugeben, handelt es sich aller Wahrscheinlichkeit nach um eine gefälschte Webseite. Klicken Sie auf keine Links in E-Mails, bei denen die Eingabe sensibler Daten gefordert wird. Geben Sie die Internetadresse Ihrer Bank und anderer sensibler Dienste immer von Hand in die Adresszeile Ihres Browsers ein.

Die Zahlungsmethoden im Überblick

Wer in Online-Shops einkauft, hat häufig die Wahl zwischen klassischen Zahlungsmethoden wie Überweisung und Lastschrift oder neuartigen Verfahren wie *PayPal* oder *giropay*. Wir bieten Ihnen eine Übersicht über die gängigsten Zahlungsmethoden mit einer Einschätzung von Sicherheitsaspekten und vorhandenen Risiken.

Überweisung

Bei der Überweisung müssen Sie als Käufer in der Regel nicht nur länger auf Ihre bestellten Waren warten, sondern der Online-Einkauf ist auch mit einem erhöhten Risiko behaftet. Sie treten in Vorkasse und geben dabei Ihre Bankverbindung preis. Der Verkäufer sendet die Ware in der Regel erst ab, nachdem er Ihre Zahlung erhalten hat. Betrüger könnten bis zum Zeitpunkt der Überweisung warten, das Geld dann abheben, jedoch die Ware nicht losschicken. Das Geld in diesem Fall zurück zu bekommen, ist in der Regel nicht möglich. Trifft die Bank nachweislich keine Schuld, muss sie das Geld nicht erstatten und Sie sind auf die Kulanz des Verkäufers angewiesen.

Eine spezielle Überweisungsmethode wird von Betreibern wie *Sofortüberweisung.de* angeboten. Dabei müssen Sie als Käufer Ihre PIN und TAN auf der Webseite des Betreibers eingeben. Der Betreiber leitet die Daten an Ihre Bank für die Zahlung weiter. Das bezahlte Geld wird auf das Konto des Verkäufers überwiesen, wie es bei einer normalen Überweisung der Fall ist. Zusätzlich erhält der Verkäufer eine Garantie über den Zahlungseingang vom Betreiber, sodass er die Ware in der Regel sofort versenden kann.

Zwar bestätigt der TÜV eine hohe Sicherheit bei der Geldüberweisung, die Eingabe sämtlicher Bankdaten inklusive der TAN auf der Homepage des Betreibers hinterlässt jedoch einen faden

Beigeschmack. Viele Banken sehen in der Eingabe der Daten außerhalb der eigenen Online-Banking-Seite einen Bruch der AGB. **Bei einem Missbrauch der TAN oder PIN haften Sie womöglich komplett für den entstandenen Schaden.** Für einen möglichen Betrugsfall bieten einige Dienste wie *Sofortüberweisung.de* eine Versicherung an, die es ermöglicht, das Geld wieder zu bekommen. Diese Überweisungsmethode lohnt sich demnach hauptsächlich für Online-Waren wie Tickets, die nach Möglichkeit zügiger geliefert werden sollen, als es bei herkömmlichen Überweisungen der Fall ist.

Lastschrift

Beim Lastschriftverfahren erteilen Sie dem Verkäufer eine Einzugsermächtigung und Ihr Konto wird mit dem zu bezahlenden Geldbetrag belastet. Analog zum Überweisungsverfahren müssen Sie bei der Einwilligung einer Lastschrift Ihre Bankverbindung offen legen. Achten Sie darauf, dass Ihr Bankkonto für die anstehende Abbuchung ausreichend gedeckt ist, andernfalls laufen Sie Gefahr, dass die Bank eine Rückstellungsgebühr von Ihnen verlangt. **Ein Sicherheitsaspekt beim Lastschriftverfahren ist der Schutz vor unberechtigten Abbuchungen. Sie können innerhalb von sechs Wochen gegenüber Ihrer Bank eine Rückbuchung des abgebuchten Betrags verlangen.**

Nachnahme

Bei der Zahlung per Nachnahme zahlen Sie erst, wenn Ihnen die Ware zugestellt wird. Daher müssen Sie oder eine von Ihnen beauftragte Person zur Warenübergabe anwesend sein und den Betrag bar bezahlen. In der Regel können Sie den Inhalt des Pakets jedoch nicht überprüfen. Das heißt auch, dass bei schadhafter Ware eine Rückbuchung des Geldes in der Regel nur auf Kulanz des Verkäufers oder bei einer nachweislich falschen Lieferung möglich ist. **Sie haben also eine Garantie darauf, dass die Ware ankommt, doch nicht darauf, dass die Ware unbeschädigt ist.** Je nach Zustellungsunternehmen und Größe des zugestellten Pakets fallen zudem Zusatzgebühren an.

Kreditkartenzahlung

Als Kreditkarteninhaber besitzen Sie einige Privilegien. Da die Überweisung über eine Kreditkartengesellschaft und nicht über die Bank erfolgt, müssen Sie beim herkömmlichen Verfahren der Kreditkartenzahlung nur den Namen der Gesellschaft sowie Ihre Karten- und Sicherheitsnummer angeben, was das Verfahren schnell und einfach macht. Darüber hinaus besteht die Möglichkeit, das bezahlte Geld zurück buchen zu lassen, wenn die gelieferte Ware beschädigt ist oder nicht ankommt.

Sie müssen jedoch mit Ihren Daten sehr vorsichtig umgehen. Zwar muss die Kreditkartenge-

sellschaft beweisen, dass Sie eine bestimmte Transaktion getätigt haben, doch fallen Ihre Kreditkartendaten in falsche Hände, ist nicht gewährleistet, dass Sie Ihr Geld zurückbekommen. **Überprüfen Sie daher Ihre Kreditkartenabrechnung regelmäßig und sehr sorgfältig.**

MasterCard und *Visa* bieten darüber hinaus die Möglichkeit an, im Internet ein so genanntes *3D Secure-Verfahren* anzuwenden, bei dem ein so genannter *Secure Code* für weitere Sicherheit sorgen soll. Das Verfahren ist jedoch umstritten, da es Betrügern gelingen kann, diesen Code unbemerkt per Schadsoftware auf dem PC abzugreifen oder, wenn die Betrüger im Besitz Ihrer Kreditkartendaten sind, selbst einen gültigen Code zu generieren. Anders als bei der herkömmlichen Kreditkartenzahlung trägt der Karteninhaber durch den Besitz des Codes ein zusätzliches Haftungsrisiko: Der Karteninhaber muss beweisen, nicht fahrlässig mit seinen Daten umgegangen zu sein. Diesen Beweis zu liefern, um eine Rückbuchung zu erwirken, kann in der Praxis schwierig bis unmöglich sein. **Im Vergleich bietet das herkömmliche Kreditkartenverfahren ohne *Secure Code* für den Karteninhaber damit weitaus größere Chancen gestohlenes Geld über die Kreditkartengesellschaft wieder zu erhalten.**

Auf den Punkt gebracht: Bei dem Umgang mit einer Kreditkarte steht der Schutz Ihrer Daten an erster Stelle: **Lassen Sie Ihre Kreditkarte niemals unbeaufsichtigt und geben Sie die Karte nur aus der Hand, wenn Sie den Bezahlprozess einsehen können. Achten Sie insbesondere bei der Kreditkartenzahlung auf die grundsätzlichen Regeln beim Online-Kauf (siehe zu Beginn des Tipps).**

Prepaid-Karten

Mit Guthaben-Karten, auch Prepaid-Karten genannt, können Sie oftmals ohne die Angabe sensibler Daten bezahlen, da bei einigen Anbietern, wie *Paysafecard*, keine Registrierung notwendig ist. Die Aufladung erfolgt durch Aktivierung eines PIN-Codes und ohne die Angabe Ihrer Bankdaten. Nachdem die Karte aktiv ist, können Sie mit dem Geld der Karte sofort bezahlen.

Nicht alle Online-Shops bieten die Zahlung via Guthaben-Karten an, vergewissern Sie sich im Vorfeld über die **akzeptierten Zahlungsarten**. Außerdem erheben einige Anbieter von Guthaben-Karten eine Aufladegebühr, durch die regelmäßig zusätzliche Kosten anfallen. Informieren Sie sich genau über den **Käuferschutz** des jeweiligen Anbieters von Guthaben-Karten. Wie garantiert der Anbieter die Erstattung des Geldes, sofern Sie die Transaktion rückgängig machen möchten? **Prepaid-Karten sind daher am ehesten empfehlenswert, wenn die Notwendigkeit einer Rückerstattung im Vorhinein als sehr gering eingeschätzt wird.**

Bezahlsysteme

Bezahlsysteme wie *Paypal*, *Moneybookers* oder *Click & Buy*, fungieren als **Vermittler zwischen Ihnen und dem Verkäufer**. Sie hinterlegen Ihre Bank- oder Kreditkartendaten bei dem Bezahlsys-

tem und müssen diese fortan nicht bei jedem Onlineshop einzeln angeben. Die Betreiber des Onlineshops können Ihre Bankdaten nicht einsehen. Die Kosten, die durch Einkäufe mit dem Bezahlsystem entstehen, werden per Lastschrift oder Überweisung von Ihrem Bankkonto abgebucht. **Informieren Sie sich vor der Entscheidung für ein Bezahlsystem genau darüber, welcher Käuferschutz geboten wird.**

Eine große Gefahr bei Bezahlsystemen wie *Paypal* besteht dann, wenn das Bezahlsystem-Konto ungenügend geschützt ist. **Bringen Betrüger Ihr Passwort in Erfahrung, können diese indirekt über Ihr Bankkonto verfügen.** Schützen Sie also Ihre Bezahlsystem-Konten unbedingt mit einem sicheren Passwort (siehe IT-Sicherheitstipp und Hintergrundinfos *Sichere Passwörter erstellen* [1]).

giropay und Online-Banking

Bei dem Verfahren *giropay* werden Sie vom Onlineshop bei der Bezahlung direkt auf die Online-Banking-Seite Ihrer Hausbank weiter geleitet. Dort loggen Sie sich mit Ihrer PIN und Ihrem Anmeldenamen an und bestätigen die Überweisung mit einer TAN. Vorteil: Die Bank sendet daraufhin die eingegangene Zahlungsbestätigung an den Verkäufer. Dieser wird somit unmittelbar über Ihre Zahlung in Kenntnis gesetzt und kann den Versand der Ware veranlassen.

Der eigentliche Bezahlvorgang via *giropay* ist so sicher, wie das Verfahren, dass Ihnen Ihre Bank in dem Zusammenhang bietet. Wird *giropay* oder Ihr Online-Banking nur mit dem klassischen PIN/TAN-Verfahren angeboten, besteht eine Schwachstelle beim Beschaffen einer TAN (siehe IT-Sicherheitstipp und Hintergrundinfos *Sicherheit beim Online-Banking* [1]). **Das klassische PIN/TAN-Verfahren, bei dem Sie im Vorfeld von Ihrer Bank eine Liste mit TANs zugeschickt bekommen, bietet heutzutage keine ausreichende Sicherheit mehr.** Sicherer sind Verfahren, bei denen die TAN speziell für einen Auftrag generiert und Ihnen auf einem **separaten Gerät**, wie einem **TAN-Generator** oder **Ihrem Mobiltelefon**, angezeigt wird.

Doch auch bei der Übermittlung von TANs auf das Mobiltelefon, dem so genannten *mTAN-Verfahren*, lauern Gefahren. Diese Methode ist nur sicher, wenn weder Ihr Mobiltelefon, noch Ihr PC infiziert sind. Verwenden Sie daher auch auf Ihrem Mobiltelefon, wenn möglich, immer eine **aktuelle Antivirensoftware** und geben Sie Ihre Mobiltelefonnummer nur bei der Registrierung auf einer **verschlüsselten Webseite Ihrer Hausbank** an. Auch die Handynummer gehört zu den Daten, die eine Bank niemals per E-Mail abfragen würde.

Fazit

Generell sollten Sie darauf achten, nur bei **vertrauenswürdigen Onlineshops** einzukaufen, die bestenfalls von einem renommierten Zertifikataussteller **zertifiziert** worden sind. Sicherheitsmerkmale, wie die Absicherung von Eingabeformularen über SSL und die Verwendung gültiger ***SS-***

L-Zertifikate sollten stets beachtet werden (siehe IT-Sicherheitstipp und Hintergrundinfos *Sicher Einkaufen im Internet* [1]). **Sichern Sie alle Zugangsaccounts durch die Vergabe sicherer Passwörter und wechseln Sie Ihre Passwörter regelmäßig**. Gehen Sie mit Ihren Bank- und Kreditkartendaten sehr sparsam um und geben Sie diese niemals bei einer Aufforderung per E-Mail preis. Informieren Sie sich im Vorhinein über die **Möglichkeiten einer Rückerstattung**, die Ihnen das jeweilige Verfahren bietet. Von einer Überweisung ist grundsätzlich dann abzuraten, wenn Ihnen der Shop nicht vertraut ist oder Sie teure Produkte kaufen. Eine höhere Sicherheit bieten Zahlungsmethoden wie Lastschrift oder die Kreditkartenzahlung, bei denen Sie **Ihr Geld wieder zurück buchen lassen können**, wenn die Ware nicht in Ordnung ist. Kaufen Sie in verschiedenen Onlineshops ein, so lohnt sich ein Vergleich der angebotenen Zahlungsmöglichkeiten. Bieten zwei oder mehr Plattformen, die Sie regelmäßig nutzen, gleiche Zahlungsmethoden an, kann sich ein Bezahlsystem oder eine Prepaid-Karte lohnen, **sofern der gebotene Käuferschutz Ihnen zusagt**. Sichern Sie auch besonders **Ihre Accounts bei Bezahlsystemen durch sichere Passwörter. Überprüfen Sie alle Abbuchungen und Abrechnungen regelmäßig auf Unstimmigkeiten.**

Autoren:

Mark Thiel, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen:

[1] http://ratgeber.it-sicherheit.de

http://www.ec-net.de

https://it-sicherheit.de

http://www.kmu-sicherheit.de

http://www.bsi.bund.de

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de