Ist Ihr Online-Banking sicher?

Zahlreiche Unternehmen nutzen das Online-Banking-Angebot ihrer Bank, um bequem vom Büro aus und unabhängig von Öffnungszeiten der Bankfilialen ihren Zahlungsverkehr abzuwickeln. Doch ist der Online-Geldtransfer auch immer sicher?

Stellen Sie sich vor, Sie überweisen Geld über das Internet – und nichts kommt an! Was generell für das Internet gilt, ist insbesondere auch beim Online-Banking zu beachten: Kriminelle versuchen, Konto- und Kreditkartendaten auszuspähen und so an Ihr Geld zu kommen. Umfangreiche Schutzmaßnahmen helfen, das Online-Banking sicher zu machen.

Sie haben es in der Hand

Sicheres Online-Banking funktioniert nur, wenn auch Sie einige Regeln beachten und u.a. gewährleistet ist, dass Ihr Computer sicher ist. Es darf sich z.B. keine Schadsoftware darauf befinden, die es Kriminellen leicht macht, Überweisungen zu manipulieren.

Die meisten Banken fordern ihre Kunden inzwischen auf, Anti-Viren-Software und Firewall auf dem PC zu installieren. Zahlreiche Institute haben diese Forderung sogar in ihre Allgemeinen Geschäftsbedingungen aufgenommen. Wenn Sie auf der sicheren Seite sein wollen, sollten Sie Vorkehrungen für die Sicherheit Ihres Computers treffen und die Vorsorgeregeln für sicheres Online-Banking beachten.

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 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 unparteiischer 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.

Netzwerk Elektronischer Geschäftsverkehr

www.ec-net.de

Praxistipps

Aus der Praxis für die Praxis

Sicheres Online-Banking

10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Netzwerk Elektronischer Geschäftsverkehr

TeleTrusT

TeleTrusT – Bundesverband IT-Sicherheit e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische“ rund um das Thema Informationssicherheit.

TeleTrusT ist mit mehr als 130 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.

TeleTrusT
Pioneers in IT security.

Impressum

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:
TeleTrusT – Bundesverband IT-Sicherheit e.V.,
Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:
Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:
Karl-Heinz Kottenhahn

Druck:
Buersche Druck- und Medien GmbH

Bildnachweis:
Dron/Fotolia.com, Frog 974/Fotolia.com,
V. Yakobchuk/Fotolia.com

Stand: 12/2011

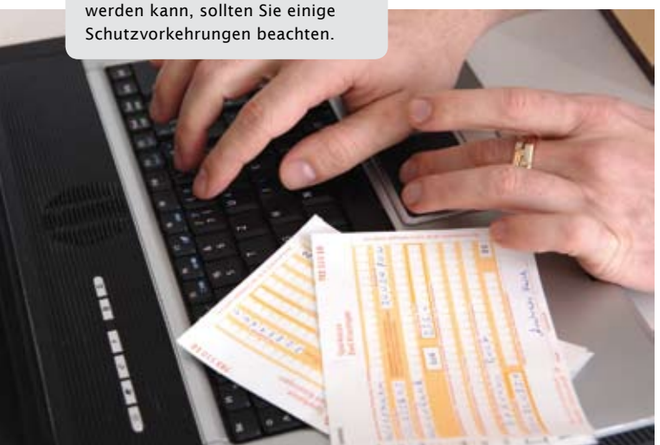
10 Tipps, die wirklich helfen

Sicheres Online-Banking im Unternehmen

10 grundlegende Praxistipps helfen Ihnen, Ihr Online-Banking sicher zu gestalten.

Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema Sicheres Online-Banking finden Sie unter www.ec-net.de und www.kmu-sicherheit.de.

Damit in Ihrem Unternehmen Online-Banking sicher durchgeführt werden kann, sollten Sie einige Schutzvorkehrungen beachten.



Wie mache ich meinen Rechner fit für das Online-Banking?

Voraussetzung ist ein „sauberer“ Computer, auf dem sich garantiert keine schädliche Software, wie etwa Viren oder Trojaner, befindet. Sobald sich Schadsoftware auf dem PC befindet, sollten Sie von diesem Gerät aus auf keinen Fall mehr Online-Banking betreiben.

Ein unsicherer Rechner ist das Einfallstor für Kriminelle. Mit Hilfe von Schadsoftware können Ihre Passwörter kopiert, die Sicherheitssoftware ausgeschaltet oder kurz Ihr gesamter Rechner kontrolliert werden. Besondere Vorsicht ist angebracht, wenn Sie den Computer nicht kennen, mit dem Sie Online-Banking machen wollen, denn Sie wissen dann nicht, ob sich nicht etwa Schadsoftware darauf befindet.

Tipp 1: Schutzsoftware installieren
Installieren Sie Schutzsoftware mit Viren- und Spyware-Erkennung und einer Firewall. Halten Sie diese, wie auch Ihr Betriebssystem und den Internetbrowser, immer auf dem neuestem Stand.

Tipp 2: Benutzerkonten einrichten
Richten Sie gesonderte Benutzerkonten an Ihrem PC ein. Wenn Sie ständig als Administrator an Ihrem PC angemeldet sind, können Schadprogramme größtmögliches Unheil anrichten.

Wie nehme ich eine sichere Überweisung vor?

Ähnlich wie am Geldautomaten ist auch im Internet Vertraulichkeit oberstes Gebot – das gilt im besonderen Maße auch für die Verwendung der Transaktionsnummern (TAN), Kennwörter und PINs. Und speichern Sie keine Zugangs- und Transaktionsdaten

auf Ihrem PC oder Smartphone – auch nicht in einem Passwort-Manager.

Kriminelle versuchen gerne durch das Vortäuschen der Bankseite und der Aufforderung zur Eingabe von PINs, Kennwörtern und TANs (sogenanntes Phishing) Ihre wertvollen Zugangsdaten abzugreifen und dann Ihr Konto zu plündern. Ihre Bank wird Sie niemals auffordern, Ihre persönlichen Daten per E-Mail oder Telefon einzugeben und wird Sie auch niemals um die Eingabe mehrerer TANs gleichzeitig bitten.

Tipp 3: Vorsicht bei PIN- und TAN-Eingabe
Folgen Sie niemals einem Link (Verweis) in einer E-Mail zu einer Webseite, in der Sie aufgefordert werden, Ihre PIN oder TAN einzugeben.

Tipp 4: Vorsicht bei den Zugangsdaten
Schützen Sie Ihre Zugangsdaten, wie z.B. TAN-Liste oder Chipkarte, und verwenden Sie ein sicheres Passwort für Ihren Zugang.

Tipp 5: Tageslimit einrichten
Richten Sie für zusätzliche Sicherheit ein Tageslimit für Überweisungen ein. So kann nicht Ihr komplettes Guthaben auf einmal abgehoben werden.

Tipp 6: Auf verschlüsselte Übertragung achten
Achten Sie auf eine SSL-Verschlüsselung der Seite, auf der Sie Transaktionen tätigen wollen. Ein „https“ in der Adresszeile sowie ein Schlosssymbol in der Statusleiste Ihres Browsers sind hierfür sichtbare Zeichen.

Tipp 7: Sicherheit mit HBCI-Chipkarte
Wenn Sie beim Online-Banking mit der HBCI-Chipkarte arbeiten, haben Sie ein relativ hohes Sicherheitsniveau.

Was mache ich, wenn ich einen Betrugsverdacht habe?

Online-Banking wird durch die Verwendung neuer Verfahren immer sicherer. Dazu zählen mTans, die aufs Handy gesendet werden oder chipTANs, die mit Chipkarte und Kartenleser funktionieren. Sollten Sie dennoch von einem Betrugsversuch betroffen sein, gilt es schnell und überlegt zu handeln.

Tipp 8: Im Notfall Zugangsdaten sperren
Sollten Sie Unregelmäßigkeiten feststellen, kontaktieren Sie Ihre Bank. Sperren Sie den Online-Zugang zu Ihrem Konto, indem Sie z.B. mehrfach eine falsche PIN eingeben. Sollte von Ihrem Konto bereits Geld verschwunden sein, erstatten Sie Anzeige bei der Polizei.

Tipp 9: Computer wieder sicher machen
Machen Sie Ihren Computer wieder sicher. Dazu gehört die Neuinstallation des Betriebssystems, der Schutzsoftware und Ihrer Anwendungen.

Tipp 10: Zugangsdaten ändern
Ändern Sie sofort alle Ihre Zugangsdaten, sowohl die für Ihren eigenen Rechner als auch für andere Internetdienste, z.B. Online-Shops, soziale Netzwerke und andere Kreditinstitute.