



Mitteilung SICHERHEIT IM INTERNET

Sicheres Arbeiten mit Hypo Online Banking

Richtiger Umgang mit Ihren Zugangsdaten

- Schützen Sie Ihre persönlichen Zugangsdaten (PIN, Verfügernummer, Verfügernamen, iTAN-Brief) vor unberechtigtem Zugriff. Geben Sie die geheimen Zugangsdaten niemals einem Dritten bekannt.
- Speichern Sie diese sensiblen Daten insbesondere nicht auf der Festplatte ab. Dies könnte sonst an PCs, die nicht ausschließlich von Ihnen benutzt werden, wie zum Beispiel am Arbeitsplatz oder in einem Internetcafé, dazu führen, dass Dritte die von Ihnen gespeicherten Daten einsehen können. Auch spezielle Programme, die auf Ihren Rechner gelangt sind, könnten diese Daten ausspähen und zum Beispiel per E-Mail versenden. Wenn Sie zur Erhöhung der Sicherheit zusätzliche Ausrüstung wie z.B. einen Chipkartenleser mit PIN-Eingabetastatur benutzen, geben Sie die dafür vorgesehenen vertraulichen Daten nur dann ein, wenn Sie von dem Gerät dazu aufgefordert wurden.
- Vergewissern Sie sich bei jeder Eingabe Ihrer persönlichen Zugangsdaten, dass es sich beim Adressaten um die Hypo Tirol Bank handelt. Wir werden Sie niemals z.B. per E-Mail oder auch telefonisch kontaktieren, um nach Ihren geheimen Zugangsdaten wie PIN und TAN fragen. Beantworten Sie solche E-Mails nicht und folgen Sie auch nicht den dort angegebenen Instruktionen - selbst wenn Ihnen mit negativen Konsequenzen wie beispielsweise einer Kontosperrung gedroht wird.
- Sollten Sie solche E-Mails erhalten, kontaktieren Sie uns bitte - von Montag bis Freitag von 08.30 bis 16.30 Uhr - unter der Nummer +39 0471 066 319.

Auftragslimits vereinbaren

- Für Ihre Inlandsaufträge bzw. EU-Standard-Überweisungen via Hypo Online Banking wurde von der Hypo Tirol Bank ein Standardlimit definiert. Geht bei der Auftragserstellung Ihr zu überweisender Betrag über dieses Standardlimit, so bekommen Sie eine Hinweismeldung im Hypo Online Banking angezeigt. Aufträge über diesem Limit können nicht autorisiert werden.
- Dieses Limit können wir für Sie jederzeit über- aber auch untersteuern. Vereinbaren Sie mit uns ein individuell an Ihre Bedürfnisse angepasstes Auftragslimit. Kontaktieren Sie uns hierzu einfach unter der Nummer +39 0471 066 319.
- Durch ein gemeinsam mit uns fixiertes Auftragslimit können Sie sicherstellen, dass Betrüger nicht unbemerkt hohe Summen von Ihrem Konto abbuchen.

Kontobewegungen beobachten

- Wer die Bewegungen auf seinem Konto regelmäßig überprüft, kann schneller reagieren und die Bank sofort auf Unregelmäßigkeiten hinweisen. So lässt sich im Fall des Falles das Geld vielleicht noch retten.

Unerwartete E-Mails ignorieren

- Die Hypo Tirol Bank wird Sie niemals nach Ihren Kontoangaben oder Ihren persönlichen Zugangsdaten (z.B. Ihre PIN bzw. Ihre iTANs) per E-Mail fragen. Bitte beantworten Sie solche E-Mails nicht und folgen Sie auch nicht den dort angegebenen Instruktionen. Dies selbst wenn man Ihnen mitteilt, dass Ihr Konto gesperrt oder gelöscht wird oder Ihnen mit einer Geldstrafe gedroht wird.
- Sollten Sie solche E-Mails erhalten, kontaktieren Sie uns bitte - von Montag bis Freitag von 08.30 bis 16.30 Uhr - unter der Nummer +39 0471 066 319.

Überprüfen Sie das Sicherheitszertifikat der Hypo Tirol Bank

Internet Explorer

Bereits beim Login zu unseren Hypo Online Produkten erscheint das Schloss-Symbol in der Statusleiste unten rechts. Dieses Schloss kennzeichnet eine sichere, verschlüsselte und zertifizierte Verbindung. Durch Doppelklick auf dieses Symbol öffnet sich das Dialogfenster mit Eigenschaften und Inhalten des Zertifikats. Unter "Allgemein" ist aufgeführt, für wen ("**hbn01.cedacri.it**" - Cedacri, Informationssystem der Hypo Tirol Bank Italien AG), von wem (www.verisign.com) das Zertifikat ausgestellt ist und bis wann es gültig ist („das aktuelle Zertifikat ist gültig bis ...“). Das Datum im Feld "Gültig bis" muss in der Zukunft liegen.

Firefox

Bereits beim Login zu unseren Hypo Online Produkten erscheint das Schloss-Symbol in der Statusleiste unten rechts. Dieses Schloss kennzeichnet eine sichere, da verschlüsselte und zertifizierte Verbindung. Mit Klick auf das Schloss-Symbol in der Statusleiste öffnet sich das Dialogfenster mit den Sicherheitsinformationen. Über die Schaltfläche "Anzeigen" können Sie sich das Verfallsdatum ("Validität" - "Läuft ab am ...") anzeigen lassen und sehen, ob das Zertifikat für Cedacri, Informationssystem der Hypo Tirol Bank Italien AG ("Herausgegeben für ...") ausgestellt ist. Das Datum im Feld "Gültig bis" muss in der Zukunft liegen

Überprüfen Sie den elekt. Fingerabdruck unseres Sicherheitszertifikats

Der elektronische Fingerabdruck ist ein Code, der aus mehreren Ziffern und Buchstaben besteht und eine Seite eindeutig verifiziert. Zur Überprüfung gehen Sie bitte wie folgt vor:

Internet Explorer

Nachdem Sie das Zertifikat aufgerufen haben, finden Sie als letzten Eintrag unter "Details" den Fingerabdruck. Der angezeigte Code muss identisch sein mit folgendem SH1-Code: a1 49 34 3d 82 09 32 ed 38 25 51 d9 1a c6 15 db 2b 84 96 80.

Firefox

Nach Klick auf das Schloss-Symbol finden Sie in den Sicherheitsinformationen über die Schaltfläche "Anzeigen" den Eintrag "Fingerabdruck". Der hier angezeigt "MD5-Fingerprint" muss identisch sein mit dem folgenden Code: 06 95 7A 56 F5 97 13 93 FF 6B 1F 39 67 5F AD BB.

Die gängigsten Betrüger Methoden

Phishing

Leider verwenden Kriminelle das Internet, um an Ihre persönlichen Daten zu gelangen: Eingesetzt werden z.B. E-Mails, die als Absender einen bekannten Serviceanbieter bzw. eine Bank vortäuschen. Diese E-Mails sehen täuschend echt aus und werden als Phishing E-Mails bezeichnet.

Merkmale einer Phishing E-Mail:

Die Absenderadressen sind zumeist gefälscht. Die Erkennung des gefälschten Absenders ist kaum möglich.

- Die Anrede ist unpersönlich gehalten ("Lieber Kunde der x-Bank").
- Dringender Handlungsbedarf wird signalisiert ("Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren...").
- Drohungen! ("Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren...").
- Vertrauliche Daten (z. B. PINs und TANs) werden abgefragt, z.B. in einem Formular innerhalb der E-Mail.
- Die E-Mails enthalten Links, die geöffnet werden sollen.
- Die Nachrichten sind manchmal (aber nicht immer!) in schlechtem Deutsch verfasst. Die Gründe dafür: Sie werden manchmal von Computerprogrammen aus anderen Sprachen automatisch übersetzt.
- Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste bzw. fehlende Umlaute (z. B. nur "a" statt "ä" bzw. "ae").

Löschen Sie verdächtige E-Mails, ohne sie zu öffnen.

Auch wenn sie eine E-Mail von einer Ihnen scheinbar bekannten E-Mail-Adresse erhalten, öffnen Sie bitte keine verdächtigen Anhänge.

Spionage Programme

Kriminelle setzen auch so genannte Spyware (Trojaner, Key-Logger) ein.

Merkmale einer Infizierung Ihres PCs mit einem Spionage-Programm

- Der PC funktioniert außergewöhnlich langsam, besonders beim Surfen im Internet.
- Der Internet Explorer öffnet Werbefenster, die in keinem erkennbaren Zusammenhang zu von Ihnen besuchten Websites stehen.
- Ihre Browser-Startseite wurde geändert.
- Im Favoritenordner finden Sie Links, die nicht von Ihnen gespeichert wurden.
- Ihr PC verbindet sich selbstständig mit dem Internet.
- Ihre Firewall meldet laufend Versuche von Programmen, die eine Verbindung zum Internet herstellen wollen.

Computer-Hacking

Hacker dringen gezielt in fremde Systeme ein, um dort Schaden anzurichten. Sie löschen, verändern oder missbrauchen geschützte Datenbestände oder Programme. Durch solche Eingriffe können materielle Schäden in Millionenhöhe entstehen.

Sicheres Arbeiten im Internet

Wer braucht welchen Schutz?

Die fünf "Goldene Regeln", die Sie stets beachten sollten:

- Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Halten Sie Kennwörter und Benutzernamen sowie Zugangsdaten für Dienste (z.B. beim Hypo Online Banking) unter Verschluss und speichern Sie diese nicht auf die Festplatte.
- Installieren Sie ein Virenschutzprogramm; halten Sie dieses immer auf dem aktuellsten Stand.
- Setzen Sie eine Personal Firewall ein und aktualisieren Sie diese regelmäßig.
- Achten Sie darauf, ob es Sicherheitsupdates für Ihr Betriebssystem und sonstige von Ihnen installierte Software gibt und führen Sie diese durch.
- Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs unterschiedliche Benutzerkonten ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff anderer geschützt.

Ein sicherer Browser

- Damit Sie sich sicher im Internet bewegen können, müssen Sie Ihren Browser immer auf dem neuesten Stand halten. Denn nur die aktuellste Version bietet die höchsten Sicherheitsstandards. Mindestens ebenso wichtig: Auch diese neuesten Browser müssen immer wieder aktualisiert werden.
- Ihr Internet-Browser kann noch so aktuell sein, ein großes Sicherheitsrisiko für Ihren Browser können die so genannten "aktiven Inhalte" darstellen. Auch auf die Risiken durch Plug-ins und falsche Einstellungen sollte Rücksicht genommen werden.
- Unter aktiven Inhalten versteht man kleine Programme, die in Webseiten integriert sind und beim Besuch einer solchen Seite auf Ihren PC heruntergeladen werden. Damit erscheinen Seiten bunter und dynamischer. Leider sind damit auch enorme Risiken verbunden. Denn Sie als Internetsurfer haben nur wenig oder gar keine Kontrolle darüber, wie diese Programme auf Ihrem Rechner arbeiten und was sie bewirken.
- Wer wirklich sicher gehen will, sollte deshalb im Browser alle aktiven Inhalte wie - **Java** und **ActiveX** - nur nach Bestätigung aktivieren.

Um ein problemloses Arbeiten mit Hypo Online Banking garantieren zu können, bitten wir Sie unsere sicheren Seiten <https://hbn02.cedacri.it> in die "vertrauenswürdigen Seiten" Ihres Browsers einzutragen.

Festplatte regelmäßig auf Viren überprüfen

7 Tipps zum Virenschutz:

- Sichern Sie regelmäßig Ihre Daten.
- Bewahren Sie die Sicherheitskopien sorgfältig auf.
- Verwenden Sie Anti-Viren-Software und aktualisieren Sie diese regelmäßig.
- Überprüfen Sie neue Datenträger, die Sie verwenden, mit dem Anti-Viren-Programm.
- Erstellen Sie einen Notfall-Datenträger (z. B. CD-ROM).
- Stellen Sie den Systemwiederherstellungszeitpunkt fest.
- Schützen Sie Ihren Computer und alle Datenträger vor fremder Benutzung.

Sichere Passwörter wählen

Ein gutes Passwort sollte mindestens acht Zeichen lang sein. Tabu sind allerdings Namen von Familienmitgliedern, des Haustiers usw. Wenn möglich sollte das Wort auch nicht in Wörterbüchern vorkommen. Dabei sollten allzu gängige Varianten vermieden werden, also nicht 123abc usw. Auch nicht empfehlenswert ist das Anhängen von einfachen Ziffern am Ende des Passworts.

Aber wie merkt man sich ein solches Passwort? Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten, etc.). Hier ein Beispiel: "Ich war am Freitag mit Hape beim Surfen." Nur die 1. Buchstaben: "IwaFmHbS". Auf diese Weise hat man sich eine "Eselbrücke" gebaut.

Weitere Hinweise zu Ihren Passwörtern:

- Ändern Sie Ihre Passwörter in regelmäßigen Zeitabständen.
- Notieren Sie keine Passwörter, auch wenn es bei selten genutzten Zugangsdaten schwer fällt.
- Speichern Sie vor allem Ihr Passwort für den Anwahlvorgang nicht ab.
- Verwenden Sie keine einheitlichen Passwörter für verschiedene Anwendungen.
- Ändern Sie bei einer Erstinstallation eventuell vorhandene Default-Passwörter sofort ab.
- Sichern Sie Tastatur und Bildschirm beim Verlassen Ihres Arbeitsplatzes durch Eingabe einer Passwortsicherung.

Sicheres Bezahlen im Internet

Seriöse Anbieter geben auf ihren Seiten stets ein vollständiges Impressum an und nennen Möglichkeiten, mit ihnen in Kontakt zu treten. Nehmen Sie Abstand von Unternehmen, die sich hinter Postfachadressen oder an sehr exotischen Orten verstecken.

- Lassen sie sich niemals auf Anbieter ein, die Ihnen nicht vor dem Kauf die vollständigen Geschäftsbedingungen (AGB) nennen und diese zur Speicherung zur Verfügung stellen. Liefer- und Zahlungsbedingungen sowie Rückgaberecht sollten möglichst auf Deutsch sein.
- Die Übertragung sämtlicher Daten, vor allem die der Kreditkartendaten, sollte verschlüsselt erfolgen. Achten Sie darauf!
- Unseriös arbeitende Unternehmen und Anbieter werden oft sehr schnell im Internet bekannt. Ihnen kann man über Abfragen - etwa in der Suchmaschine Google - auf die Spur kommen.