Was wir für Ihre Sicherheit tun

Wichtiger Sicherheitshinweis Die Bank Austria Creditanstalt sichert Ihre Daten und Transaktionen mit einem der besten Sicherheitsstandards, der SSL-Verschüsselung.

Aufgrund eines Fehlers bei den Microsoft Betriebssystemen und Mac-Applikationen (IE, Office und Outlook Express für Mac) kann es zu Sicherheitsproblemen bei diesen speziell gesicherten, SSL-verschlüsselten Internetseiten kommen. Seitens der Bank wurden alle notwendigen Sicherheitsmaßnahmen getroffen. Auf die von Ihnen verwendete Software haben wir jedoch keinen Einfluss. Ein Update seitens des Users ist jedoch notwendig, um die Korrektur dieses Fehlers zu erreichen.

Microsoft hat die entsprechenden patches (Reparatur-Update) für die betroffenen Systeme erstellt. Durch die Installierung des entsprechenden patches wird der Fehler behoben!

Die Bank Austria Creditanstalt möchte Ihnen Unterstützung bei der Behebung dieses Problems bieten und empfiehlt Ihnen, den entsprechenden patch zu installieren.

Eine Beschreibung des Problems und die Patches, die dieses Problem beheben, finden Sie im Microsoft Security Bulletin MS 02-050 auf der Homepage von Microsoft.

Für eventuelle Fragen stehen Ihnen unsere OnlineB@nking Hotline unter der Telefonnummer 050505 - 26150 (zum Ortstarif aus ganz Österreich) sowie der Technische Support von Microsoft unter 0900 35 35 35 (kostenpflichtige Rufnummer!) gerne zur Verfügung.

128 bit Verschlüsselung

Die Sicherheit Ihrer Daten und Transaktionen hat bei uns höchste Priorität. Daher verschlüsseln wir alle Daten, die während einer Sitzung übertragen werden, mit einem der besten Sicherheitsstandards, der 128 bit -Verschüsselung. Dieser Schlüssel wird als unknackbar eingestuft. Denn es gibt genau 340.282.366.920.938.463.463.374.607.431.768.211.456 mögliche Kombinationen. Zwar gelang es amerikanischen Wissenschaftlern vor kurzem, einen vergleichsweise unsicheren 56 bit Schlüssel zu knacken, allerdings brauchten deren Rechner dazu ganze drei Monate. Aber ein Schlüssel gilt immer nur für die Dauer einer Sitzung, in der Regel nur drei bis höchstens fünf Minuten. Experten gehen davon aus, dass das Entschlüsseln des 128 bit Code über 10 Billionen Jahre dauern würde.

Das https-Verschlüsselungssymbol in Ihrem Browser

Sie können jederzeit erkennen, ob gerade eine verschlüsselte Sitzung vorliegt oder nicht. Bevor die Verbindung mit unserem Bank-Rechner aufgebaut wird, erhalten Sie ggf. einen Hinweis, dass Sie im Begriff sind, eine sichere Verbindung aufzubauen. Sobald eine sichere Kommunikation gewährleistet ist, erscheint in der unteren Statuszeile des Browsers ein kleines, abgesperrtes Schloss. Ein Doppelklick auf das Icon verrät Ihnen Details zur Verschlüsselung und Schlüssellänge. Achtung: Falls kein Schloss erscheint, werden Ihre Daten nicht verschlüsselt übertragen.

Weiters können Sie auch den Zertifizierungspfad überprüfen: Der Eintrag in der 3. Zeile lautet im Zertifizierungspfad entweder online1.ba-ca.com oder online2.ba-ca.com

Ihre Daten werden sicher verwahrt

Das Computer-System, auf dem Ihre Kontodaten gespeichert sind, ist mehrstufig ausgelegt und verfügt über die modernsten Sicherheitsmechanismen. Firewalls

sowie andere zuverlässige Sicherheitsbarrieren schützen Ihre Daten mit den derzeit höchsten Sicherheitsstandards. Dabei können nur Sie selbst Ihre PIN und TANs einsehen, nicht einmal Ihr Betreuer in der Filiale ist dazu in der Lage.

Unsere Internet-Server werden ständig auf ihren ordnungsgemäßen Betrieb hin überprüft. Bereits der Versuch, die Firewall zu umgehen, wird registriert. Und sofort leiten wir wirksame Gegenmaßnahmen ein.

Unterschiedliche Sicherheitsmechanismen

Bei Ihren Online-Bankgeschäften gehen wir durch das PIN/TAN-Verfahren auf Nummer sicher. Jede einzelne Transaktion wird durch die nur Ihnen bekannten Transaktionsnummern (TAN) geschützt. Nur mit der PIN, Ihrer persönlichen Identifikationsnummer, erhalten Sie Zugang zu Ihrem Konto. Noch mehr Sicherheit bietet Ihnen ein weiterer Schutzmechanismus: die automatische Abmeldung. Wenn länger als 15 Minuten keine Online-Aktivitäten auf unserer Website festgestellt werden, melden wir Sie automatisch ab.

Was Sie für Ihre Sicherheit tun können

PIN und TANs sicher verwahren

Die besten Sicherheitssysteme sind wertlos, wenn Sie Ihre geheimen PIN oder TANs an Dritte weitergeben. Denn nur mit diesen beiden Schlüsseln ist es möglich, auf Ihre Kontodaten zuzugreifen und Transaktionen durchzuführen. Sollten Ihre PIN oder TANs einmal in falsche Hände geraten, können Sie diese über die OnlineB@nking-Hotline der Bank Austria Creditanstalt sofort sperren lassen. So können Sie verhindern, dass Ihre PIN und TANs von Dritten missbraucht werden. Achten Sie also darauf, dass Sie Ihre TAN-Liste immer sicher verwahren!

PIN häufig ändern

Sie schützen sich wirksam vor Hackern, wenn Sie Ihre PIN regelmäßig ändern. Sollte ein Hacker einmal an Ihre PIN kommen, nützt sie ihm nichts, wenn die PIN schon längst nicht mehr gültig ist. Ein wichtiger Punkt ist, dass Sie eine sichere PIN wählen. Vermeiden Sie eine PIN, die leicht zu erraten ist, z.B. "11111", "12345", das eigene Geburtsdatum, das Geburtsdatum Ihres Lebenspartners oder die letzten Ziffern Ihrer Handynummer. Verwenden Sie auch nie Ihr Standard-Passwort für das OnlineB@nking. Denn manche Computerprogramme verschlüsseln das Passwort nicht mit der nötigen Sicherheit.

PIN und TANs nicht auf dem PC speichern

Wichtig ist auch, dass Sie keinesfalls Ihre PIN und TANs auf Ihrem PC speichern. Unter Umständen kann ein Unbefugter Zugriff auf Ihren PC bekommen und sich so unbemerkt Ihre PIN und TANs kopieren und für seine Zwecke einsetzen.

Immer aktuellste Virenscanner einsetzen

Eine große Gefahr geht von Viren oder Trojanischen Pferden aus. Ein Hacker hat die Möglichkeit, auf Ihrem Rechner einen Trojaner zu installieren. Dadurch kann er beispielsweise sämtliche Tastatureingaben abfangen (z.B. die Eingabe Ihrer PIN oder TAN). Sie können sich aber relativ leicht vor Trojanern und Viren schützen, indem Sie einen Virenscanner einsetzen. Ein Virenscanner überprüft ständig sämtliche Dateien auf Viren oder Trojaner und eliminiert sie selbstständig. Verwenden Sie hierzu immer die aktuellste Version. Viele Hersteller bieten Updates über das Internet an.

Eine grundsätzliche Gefahr sind Programme, die Sie sich aus dem Internet herunterladen. Sie könnten Viren oder Trojaner enthalten, die sich beim Start des heruntergeladenen Programms selbstständig und unbemerkt installieren. Laden

Sie sich Software oder Spiele immer nur von der Original-Website der Hersteller herunter. Auch sollten Sie Ihren Browser so konfigurieren, dass keine Software ohne Ihre ausdrückliche Zustimmung installiert werden kann, auch keine ActiveX Controls.

Personal Firewall einsetzen (besonders bei Standleitungen wie Kabel-Modem oder ADSL)

Standleitungsartige Verbindungen ins Internet via Kabel-Modem oder ADSL erhöhen die Gefahr, dass ihr Computer von Hackern über sogenannte Backdoors oder Trojanern mißbraucht wird. Deshalb empfehlen wir Ihnen solche Systeme mit einer Personal Firewall auszustatten. Diese verhindert, daß einerseits vom Internet aus mit auf Ihrem Computer versteckten Programmen Verbindung aufgenommen werden kann und andererseits unberechtigte Programme nicht von Ihnen unbemerkt von sich aus von Ihrem Computer aus Verbindung mit dem Internet aufnehmen können.

Bank Austria Creditanstalt OnlineB@nking nur über www.ba-ca.com

Achten Sie darauf, dass sich Ihr Computer nur mit der Bank Austria Creditanstalt und nicht mit irgendeinem Dritten unterhält! Geben Sie daher immer zuerst unsere Internetadresse www.ba-ca.com ein, bevor Sie mit dem OnlineB@nking beginnen. (Das gilt nicht für das Bezahlen im Internet mittels OnlineP@ying). Denn obwohl die Bank Austria Creditanstalt auch gegen solche Täuschungsmanöver von Hackern, genannt "spoofing", Maßnahmen ergriffen hat, schützen Sie sich so am einfachsten und wirkungsvollsten.

Zusätzliche Informationen zum Thema Sicherheit

Weiterführende Informationen rund um das Thema Datenschutz, Sicherheit im Internet, Viren, Trojaner und vieles mehr finden Sie auch auf den Seiten des Bundesminitsteriums für Inneres (BMI) http://www.bmi.gv.at/, dem deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik) oder http://www.sicherheit-im-internet.de.