Sicheres Online Banking:
Es liegt in Ihrer Hand!

Machen Sie es Betrügern schwer - beachten Sie unsere Sicherheitshinweise!

Denken Sie an den Straßenverkehr: Es genügt nicht, nur ein sicheres Auto zu fahren. Erst eine achtsame Fahrweise, die Kenntnis von möglichen Risiken und das Befolgen von Verkehrsregeln ermöglichen eine gefahrlose Fahrt. Das gilt auch für das Internet! Nur durch das Zusammenspiel von sicherer Raiffeisen-Technik, einem angemessenen Risikobewusstsein und verantwortungsbewusstem Verhalten von Seiten der Nutzer, kann optimale Sicherheit gewährleistet werden.

So machen Sie Ihren Computer sicher:

» Installieren Sie ein **Anti-Virenprogramm** und halten Sie diese immer auf dem aktuellen Stand. Ein empfehlenswertes Schutzprogramm ist ROL Secure mit speziellem Banking-Schutz.

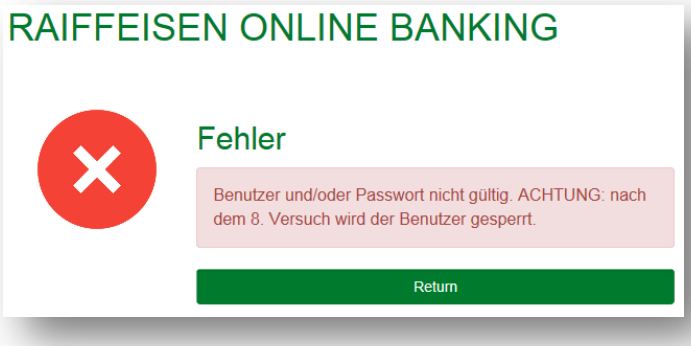
» Achten Sie stets darauf, ob neue **Sicherheitsupdates** für Ihr Betriebssystem, Ihren Browser oder andere genutzte Software bereitstehen und installieren Sie diese.

» Seien Sie vorsichtig beim **Öffnen von Dateien und Links** aus dem Internet oder bei E-Mail-Anhängen. Öffnen Sie nur Dateien, die aus vertrauenswürdigen Quellen stammen. Fragen Sie im Zweifelsfall ruhig beim Absender/Anbieter nach.

» **Programme aus dem Internet** können manipuliert sein. Beziehen Sie deshalb Software (z.B. Browser, Virenschutz etc.) nur direkt von den Internetseiten der Hersteller oder kaufen Sie diese direkt im Fachgeschäft.

» Besondere **Vorsicht ist an öffentlich zugänglichen Computern** (z.B. in Hotels, Internetcafés) geboten!
Geben Sie dort keine vertraulichen Daten ein.

Beim Password vertippt?
Bei der Eingabe eines falschen Passwortes erhalten Sie ausschließlich die angeführte Meldung.



Taucht eine andere Fehlermeldung auf?
Führen Sie keine weiteren Aktionen auf Ihrem Rechner durch und melden Sie sich umgehend bei uns!

So erkennen Sie eine mögliche Bedrohung:

Ist Ihr Computer bereits infiziert oder haben Hacker Sie auf eine manipulierte Webseite gelockt?

» Beobachten Sie Ihren Browser beim Online-Banking. Die Seite, die bei der Anmeldung in der Adressleiste Ihres Browsers angezeigt wird, beginnt immer mit http**s**://. Das **„s“** weist auf eine geschützte Verbindung hin. Geben Sie niemals sensible Daten ein, falls dieses **„s“** in der Adressleiste fehlt.

» Überprüfen Sie vor dem Versand einer Überweisung stets ein weiteres Mal die Daten. Gibt es Abweichungen zu den vorher eingegebenen Daten, informieren Sie umgehend Ihre Bank.

» In Ihrem Raiffeisen Online Banking wird Ihnen stets der Zeitpunkt des letzten Logins angezeigt. Kontrollieren Sie ob dieses Datum stimmt.

» Ihre Bank wird Sie nie per E-Mail um Passworteingaben oder andere Zugangsdaten bitten. Geben Sie diese in keinem Fall weiter. Antworten Sie auch nie auf E-Mails, in denen Ihnen bei Nicht- Befolgung von Anweisungen negative Konsequenzen (z.B. Konto sperre) angedroht werden.

» Falls Sie irgendwelche Zweifel haben oder Auffälligkeiten erkennen, melden Sie sich bei Ihrer Raiffeisenkasse und fragen nach!

» Aktivieren Sie den Informationsdienst Alert-SMS. Dieser Dienst informiert Sie über ausgewählte Transaktionen in Ihrem Raiffeisen Online Banking. Im Falle von unberechtigten Zugriffen können Sie sofort reagieren!

» Prüfen Sie laufend Ihre Kontoauszüge auf Unregelmäßigkeiten. Fragen Sie auch hier bei Unklarheiten nach!

Was Sie noch wissen sollten:

» Beim Anmelden in Ihrem Raiffeisen Online Banking ist immer nur ein Einmalpasswort erforderlich. Dies gilt auch für die Autorisierung einer Transaktion.

» Wenn Sie den Verdacht haben, dass ein Einmalpasswort in falsche Hände geraten ist, können Sie diesen durch die erneute Eingabe eines neuen Einmalpasswortes entwerten. Das neue Einmalpasswort sollte aus Sicherheitsgründen auf einem anderen Computer eingegeben werden.

Wir sind für Sie da:
In der Raiffeisenkasse vor Ort oder im Service Center
Tel.: 800 031 031
E-Mail: info@raiffeisen.it

Raiffeisen Meine Bank

Anleitung für eine sichere Nutzung der Online Banking-, CBILL- und CBI-Dienste

Bei den Diensten, die den telematischen Zugriff auf Geschäftsverbindungen ermöglichen, wendet die Bank die besten Maßnahmen der aktuellen Technologie an, greift auf verschiedenste Sicherheitsmaßnahmen zurück und stellt sichere Authentifizierungsmittel zur Verfügung. Trotz alledem ist es möglich, dass der Kunde Opfer eines Betruges durch elektronische Mittel wird. Folglich ist es, zusätzlich zu den von der Bank getroffenen Sicherheitsmaßnahmen erforderlich, dass der Kunde über ausreichende Kenntnisse verfügt, um den Internetzugang über das eigene Gerät sicher zu gestalten.

Das Hauptrisiko besteht darin, dass der Kunde Opfer eines Hackerangriffes werden kann, welcher über das vom Kunden verwendete Gerät erfolgt und z.B. den Diebstahl der Zugangsdaten, das Erstellen einer Bildschirmkopie, die veränderte Darstellung von Webseiten zwecks unrechtmäßiger Aneignung des Passworts und die Fernsteuerung des Computers bewirkt.

Es kann vorkommen, dass der Kunde eine E-Mail Nachricht erhält, welche die Graphik der Webseite der Bank imitiert. Diese Mail, welche zum Ziel hat, das Password des Kunden abzufragen, mit welchem die Zahlungen autorisiert werden, lädt den Empfänger der E-Mail ein, einem in der Nachricht enthaltenen Link zu folgen. Dieser Link führt dann allerdings nicht auf die offizielle Webseite der Bank, sondern auf eine gefälschte Seite, welche der offiziellen sehr ähnlich ist, sich aber auf dem von einer anderen Person kontrollierten Server befindet. Diese Art von Betrug über Internet, „Phishing“ genannt, kann auch über den Versand einer SMS durchgeführt werden.
Diesbezüglich wird darauf aufmerksam gemacht, dass die Bank nie Mitteilungen (E-Mail oder SMS) versendet, in denen sie den Kunden auffordert, seine Zugangsdaten einzugeben.

Zudem gibt es noch unterschiedliche Angriffsformen, die darauf abzielen, den Computer mit einem Schadprogramm zu infizieren (sogenannter Banking Trojan). Dies kann auf verschiedenste Art und Weise, wie z.B. mittels einer E-Mail mit Anhängen, eines in einer Email enthaltenen Links, welcher auf eine infizierende Webseite führt oder einfach über das Aufrufen einer manipulierten Webseite (sogenannter drive-by-download) erfolgen. Üblicherweise wird der Banking Trojan definitiv auf der Festplatte des Computers installiert. Es gibt aber auch andere Arten von Schadprogrammen, die sich im Systemspeicher des Computers befinden und somit auf der Festplatte keine Spuren hinterlassen. Ist das Schadprogramm einmal auf dem Computer aktiv geworden, stehen der kriminellen Organisation verschiedene Techniken zur illegalen Datenabfrage zur Verfügung, wie z.B. das Abfangen der Eingabefelder (Passwort oder Kreditkartendaten), die Darstellung von manipulierten Webseiten, die Blockierung des Zugangs zum Dienst, die Veränderung der Verbindung zwischen Webadresse und IP-Adresse, die Deaktivierung von installierten Antivirusprogrammen, die Veränderung der eingegebenen Daten (z.B. im Zuge einer Überweisung) und sogar die Fernsteuerung des Computers.

Aus diesen Gründen ist erforderlich, alle vorbeugenden Maßnahmen zu treffen, die die Durchführung von Aufträgen in einer infizierten Umgebung mit potentiellem Risiko eines Schadprogramms vermeiden.
Es wird davon abgeraten, Aufträge mit einem nicht bekannten Gerät durchzuführen (z.B. Verwendung eines PCs in einem Internetcafé).
Wird der Auftrag von einem eigenen elektronischen Gerät aus durchgeführt, ist es erforderlich, vor Zugriff auf die telematischen Dienste zu prüfen, ob das Gerät über ein mit allen Sicherheitspatches aktualisiertes Betriebssystem, über die aktuellsten Versionen der Benutzersoftware (z.B. Acrobat Reader) und über ein ständig aktualisiertes Antivirusprogramm verfügt.

Die genannten Voraussetzungen bilden Mindestvorkehrungen, die für eine wirksame Abwehr von eventuellen Hackerangriffen unverzichtbar sind. Es ist außerdem wichtig, dass der Kunde mit der Bank uneingeschränkt zusammenarbeitet und, vor allem im eigenen Interesse, dazu beiträgt, derartigen Angriffen vorzubeugen, indem er folgende Verhaltensregeln befolgt.

Im Allgemeinen ist es erforderlich,

• ein aktives und stets aktualisiertes Antivirusprogramm und entsprechende Firewall zu installieren;

• auf den Dienst von eigenen Geräten aus zuzugreifen, die periodisch kontrolliert werden;

• das eigene Gerät mit einem Passwort von mindestens acht , Zeichen, die nicht problemlos der Person zugeordnet werden können, zu schützen und dieses mindestens halbjährlich zu ersetzen;

• regelmäßig die Kontoauszüge und die über die Internetdienste ausgeführten Aufträge zu kontrollieren.

In Bezug auf die Nutzung des Dienstes ist es notwendig:

• die Authentifizierungsmittel mit höchster Sorgfalt zu verwahren und zu verwenden;

• einzelne Teile der Authentifizierungsmittel nicht gemeinsam aufzubewahren;

• die Authentifizierungsmittel nicht an Dritte weiterzugeben;

• den Diebstahl, den Verlust, die Zerstörung oder jegliche andere nicht erlaubte Verwendung des Zahlungsmittels und/oder der Authentifizierungsmittel zu melden;

• auf die verschiedenen Arten von potentiellen Hackerangriffen zu achten, unter anderem auf gefälschte E-Mails, gefälschte Mitteilungen bezüglich Ablauf von Fristen, die Aufforderung einen bestimmten Link zu verfolgen;

Anleitung für eine sichere Nutzung der Online Banking-, CBILL- und CBI-Dienste

Es wird empfohlen, die Zugänge zum Dienst und die erteilten Aufträge
mittels des SMS- und/oder E-Mail-Alert Dienstes zu überprüfen.

Zum Zeitpunkt des Zugangs zum Dienst ist es notwendig:

• die von der Bank im Handbuch erteilten Anweisungen zu befolgen;

• zu kontrollieren, ob das Internetprotokoll „https“ und das Symbol des Schlosses, welche charakteristisch für eine geschützte Webseite sind und sich vom Internetprotokoll „http“ unterscheiden, in der Status- bzw. Adressleiste aufscheinen;

• den Dienst nicht mehr zu nutzen und die Bank umgehend zu informieren - auch über die Grüne Nummer, welche auf der Webseite veröffentlicht ist - falls Unregelmäßigkeiten oder mangelnde Funktionstüchtigkeit des Systems festgestellt werden (z.B. wenn beim Login mehrere Einmalpasswörter verlangt werden);

• kein zweites oder drittes Einmalpasswort zu generieren, da das erste bis zur Annahme von Seiten des Systems Raiffeisen gültig ist;

• nach Ausführung der Aufträge die Anwendung mittels des entsprechenden Schaltknopfes („verlassen“) schließen.

Für Unternehmen ist es außerdem notwendig:

• auf den Dienst von professionell verwalteten Arbeitsplätzen aus zuzugreifen;

• im Bereich der Sicherheit bezüglich der Nutzung der Internet Banking-Dienste eine Unternehmenspolitik zu definieren und zu verbreiten;

• die zur Nutzung des Internet Banking-Dienstes ermächtigten Personen festzulegen und ihre Zugangsprofile zu verwalten;
• innerhalb des Unternehmens für die ermächtigten Nutzer des Internet Banking-Dienstes periodische Informations- und/oder Bildungsveranstaltungen zum Thema Sicherheit zu organisieren;

• die ermächtigten Nutzer über die Kommunikationskanäle mit der Bank zu informieren, um eventuelle Anomalien /Leistungsunfähigkeiten, welche bei der Durchführung der Aufträge festgestellt werden, schneller abwickeln zu können und zeitnah Verhaltensanweisungen und Angaben zur Anwendung angemessener Maßnahmen zu erhalten;

• das Surfen im Internet und die Möglichkeit, Programme zu installieren deren Herkunft nicht festgestellt werden kann, einzuschränken;

• die Nutzerprofile auf Grundlage des Handlungsbedarfs zu unterscheiden und auf den einzelnen Arbeitsplätzen die Administratorenrechte einzuschränken/ zu entfernen - als Alternative alle Bankbewegungen von einem PC aus auszuführen, auf welchem die Verwendung der elektronischen Post und das Surfen im Internet besonders streng definiert und kontrolliert sind;

• die Mindestanforderungen an Sicherheit einzuhalten, wie sie von den gesetzlichen Datenschutzbestimmungen vorgeschrieben sind (Legislativdekret Nr. 196/2003 - Anlage B).