DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

Filiale Düsseldorf

Postfach 10 20 30
40011 Düsseldorf

Benrather Str. 8
40213 Düsseldorf

Zentrale
Tel. +49 (0)211 867 28 0
Fax +49 (0)211 867 28 22

Kundenabteilung
Tel. +49 (0)211 210 90 898
Fax +49 (0)211 863 25 377

BIC DHBNDEDDXXX
www.dhbbank.de
dusseldorf@dhbbank.com

Sicherheit und DHB NET BANKING

DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

Index

DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

1 Sicherheitsmaßnahmen im DHB Net Banking

Dir DHB Bank verwendet aktuelle und moderne Internet-Sicherheitstechnologien, die weltweit von Finanzdienstleistern eingesetzt werden, um Ihre Transaktionen im Internet mit der DHB Bank ebenso sicher wie bequem zu gestalten. Unsere Infrastruktur hilft uns, eine der besten verfügbaren Schutzmaßnahmen anzubieten, um zu verhindern, dass Ihre Daten von nicht autorisierten Personen gelesen oder manipuliert werden. Diese Technologien sind so konzipiert, dass Sie Ihre Daten während des gesamten von Ihrem Computer ausgehenden Prozesses durch die DHB bankeigene Systeme schützen.

Das Internet-Sicherheitssystem der DHB Bank besteht aus zwei Elementen:

1. Ihrem Benutzernamen

2. IhremPasswort

Die DHB Bank verwendet unterschiedliche Methoden, um Ihre wertvollen Daten zu schützen:

Die neueste Verschlüsselungs- und Verteidigungstechnologie
Unsere Sicherheitstechnologien erstrecken sich von der starken Datenverschlüsselung bis zu unseren Hochleistungs-Firewalls.

Ihr persönlicher Benutzername und Ihr Passwort
Nur Ihr gültiger Benutzername und Ihr Passwort ermöglichen es Ihnen, sich anzumelden. Während des Anmeldungsprozesses wählen Sie Ihren eigenen Benutzernamen und Ihr eigenes Passwort aus. Selbst unser Personal wird nicht in der Lage sein, Ihr Passwort in Erfahrung zu bringen.

Automatische Sperre
Sie müssen die richtige Kombination in der richtigen Reihenfolge eingeben, um sich ins Online Banking einzuloggen. Nach mehr als drei aufeinanderfolgenden erfolglosen Anmeldeversuchen sperrt das System Ihren Zugriff. In dem Fall müssen Sie sich mit der Kundenbetreuung (Helpdesk) in Verbindung setzen.

Automatisches Ausloggen
Wenn über einen Zeitraum von 10 Minuten keine Eingabe erfolgt, so wird Ihre Verbindung automatisch beendet und Sie werden aus Sicherheitsgründen ausgeloggt. In dem Fall melden Sie sich bitte nochmals an, um Ihre Bankgeschäfte fortzusetzen.

Sicherheits-Upgrades
Der Schutz Ihrer Privatsphäre ist wichtig. Wir werten die neuesten Sicherheitstechnologien kontinuierlich aus und erweitern unsere Systeme stetig. Alle von Ihnen gespeicherten Daten werden nach dem deutschen Datenschutzgesetz gespeichert.

Wir möchten Sie jedoch daran erinnern, zusätzlich zu diesen Technologien einige Sicherheitsmaßnahmen zu ergreifen, auf die Sie achten sollten. Bitte lesen Sie unser Handbuch "*Sicherheit und DHB Net Banking*", um weitere detaillierte Informationen zu erhalten.
Wenn Sie weitere Fragen oder Probleme im Zusammenhang mit unserer Standortsicherheit haben, zögern Sie bitte nicht uns zu kontaktieren.

2 Probleme der Computer-Sicherheit

Als DHB Net Banking-Team arbeiten wir daran, für Sie eine sichere Online-Banking-Umgebung zu gewährleisten. Es kann jedoch einige Aspekte der Computer-Sicherheit geben, die wir nicht kontrollieren können. Bitte beachten Sie diese Probleme im Zusammenhang mit Ihrer täglichen Computer-Nutzung sowie für Ihren Gebrauch des DHB-Net-Bankings.

Sie sollten daher sicherstellen, dass Ihre Computerumgebung niemandem die Gelegenheit gibt, Zugriff auf Ihre Daten zu erhalten (insbesondere nicht auf Ihren Benutzernamen und Ihr Passwort).

Bitte überzeugen Sie sich davon, dass die Geräte, die Sie benutzen keine elektronische Überwachung oder Aufzeichnung Ihrer Aktivitäten ermöglichen. Der System-Administrator Ihrer Computerumgebung sollte in der Lage sein, Ihnen dies mitteilen zu können.

Darüber hinaus empfehlen wir, dass Sie von Ihrem System-Administrator die Erlaubnis/ Bevollmächtigung einholen, wenn Sie beabsichtigen, das DHB Net Banking von einem Computer am Arbeitsplatz aus zu nutzen.

2.1 Grundsätzliche Computer Sicherheit

- Verwenden Sie ein Passwort, um Ihren PC vor unerwünschtem Zugriff zu schützen. Sie können in praktisch allen Computern Anschalt-Passwörter verwenden. Bitte denken Sie daran, dass die Anmeldungs-Passwörter einiger Betriebssysteme (wie z.B. Win9x) keine wirkliche Sicherheitsfunktion haben und somit nicht vollkommen zuverlässig sind.
- Lassen Sie Ihren Computer nicht unbeaufsichtigt, während Sie zu Hause, am Arbeitsplatz oder in öffentlichen Plätzen DHB Net Banking benutzen.
- Speichern Sie sensible Daten (Kontonummern, PINs, Benutzernamen, Passwort etc...) niemals auf Ihrer Festplatte ab. Die Informationen könnten von Angreifern ausgelesen und missbraucht werden.
- Öffnen Sie keine E-Mails von unbekannten Absendern. Wenn Sie in Bezug auf den Absender einer E-Mail Zweifel haben, ist es grundsätzlich besser, sie zu löschen, ohne ihren Inhalt zu lesen, da dieser ein Virus enthalten könnte.
- Überprüfen Sie neue Daten oder Software immer regelmäßig auf Viren. Dazu müssen Sie ein Anti-Virus-Programm installieren. Setzen Sie sich mit Ihrem örtlichen Computer-Händler in Verbindung, der Sie im Hinblick auf den Kauf eines geeigneten Anti-Virus-Programmes beraten kann.
- Achten Sie darauf, dass Sie Programme aus dem Internet nur aus vertrauenswürdigen Quellen wie zum Beispiel bekannten Portalen herunterladen. Prüfen Sie zur Sicherheit jeden Download mit einem Virenscanner, bevor Sie die entsprechende Datei ausführen.
- Halten Sie Ihr Betriebssystem sowie Ihren Browser auf dem aktuellen Stand. Nutzen Sie regelmäßig die Windows-Update-Funktion, um zu überprüfen, ob Sicherheitsupdates zur Verfügung stehen.
- Wenn Sie eine Kabel-/adsl-(oder ähnliche) Internetverbindung verwenden und wenn Sie ständig mit dem Internet verbunden sind, verwenden Sie bitte eine Firewall-Hardware oder -Software, um Ihren Computer gegen Hacker zu schützen. Setzen Sie sich mit Ihrem örtlichen Computer-Händler in Verbindung, der Sie im Hinblick auf den Kauf eines geeigneten Firewall-Systems beraten kann.

2.2 Sicherheitsmaßnahmen im DHB Net Banking

- Lassen Sie Ihren Computer niemals unbeaufsichtigt, während Sie angemeldet sind.
- Bitte teilen Sie Ihren Benutzernamen oder Ihr Passwort unter gar keinen Umständen jemand anderem mit. Sorgen Sie dafür, dass Sie sicher und geheim aufbewahrt werden und von niemand anderem oder für betrügerische Zwecke verwendet werden können.
- Nennen Sie Ihr Passwort niemals in E-Mails, Briefen oder Telefongesprächen, selbst nicht gegenüber Angestellten der DHB Bank.
- Schreiben Sie Ihren Benutzernamen oder Ihr Passwort nicht in einer Weise auf, die es ermöglicht, dass es von jemand anderem verstanden wird. Verwenden Sie keins davon für andere Zwecke.
- Bitte ändern Sie Ihr Passwort regelmäßig. Wenn Sie sich anmelden, sorgen Sie dafür, dass keine Person über Sie hinweg sehen kann.
- Wenn Sie wissen oder den Verdacht haben, dass jemand anderes Ihre Zugangsdaten in Erfahrung gebracht hat, so können Sie Ihren Zugang zum Internetbanking unter der Rufnummer 0211-210 90 898 werktags von 08.00 bis 17.30 Uhr oder per E-Mail an dhbnetbanking.de@dhbbank.com mit Hilfe eines Kundenbetreuers der DHB Bank sperren lassen.
- Überprüfen Sie regelmäßig Buchungen und Transaktionen. Wenn Sie eine Transaktion entdecken, an deren Durchführung Sie sich nicht erinnern können oder wenn unerwartet Bargeld abgehoben wird, so bitten wir Sie die genauen Details zu notieren und uns die Unstimmigkeiten umgehend mitzuteilen.

2.3 Verwendung eines Computers, den Sie mit anderen zusammen oder am Arbeitsplatz oder an einem öffentlichen Platz nutzen.

- Denken Sie immer daran, Ihren DHB Net Banking-Service und Web-Browser abzuschalten und den Cache-Speicher zu löschen, da Ihr PC Daten speichern könnte.
- Lassen Sie keine Ausdrucke von Kontoauszügen herumliegen oder in Papierkörben. Sie sollten auch dafür sorgen, dass Sie Ausdrucke von öffentlichen oder gemeinschaftlich genutzten Druckern mitnehmen.
- Wenn Sie am Arbeitsplatz sind, sorgen Sie dafür, dass Ihre Firma Ihnen Online-Banking erlaubt. Einige Unternehmen erlauben keine persönliche Internet-Nutzung. Führen Sie mit Ihrem System-Administrator immer eine Prüfung durch, bevor Sie Online-Banking von einem PC oder Mac am Arbeitsplatz aus nutzen.
- Wenn Sie das DHB Net Banking beendet haben, vergewissern Sie sich, dass Sie den Speicher gelöscht und sich abgemeldet haben insbesondere an öffentlichen Plätzen, wie dem Arbeitsplatz, dem Internet-Café, in Bibliotheken, Flughäfen usw. Diese können Sie wie folgt vornehmen:

  Microsoft®Internet Explorer (8-er Versionen) -In dem Browser-Menü klicken Sie auf "Internet-Optionen". Wählen Sie die Karteikarte "Allgemeines" und in dem Bildschirmteil "Temporäre Internet-Dateien" klicken Sie auf die Tasten "Dateien löschen" und setzen einen Haken bei „Alle Offlineinhalte löschen". Anschließend klicken Sie im selben Bildschirmteil auf „ Cookies löschen" und bestätigen diese mit " OK" und schließen dann das Fenster.
- Der Microsoft®Internet Explorer (8-er Versionen) verfügt über eine Funktion mit der Bezeichnung "Automatisches Ausfüllen", die Benutzer hilft, sich an Formulareinträge und Passwörter für das Internet zu erinnern. Wir raten Ihnen dringend, diese Funktion zu deaktivieren und die vorhandenen Dateien zu löschen. Die Deaktivierung erfolgt wie folgt:

  Microsoft®Internet Explorer (8-er Versionen) -In dem Browser- Menü klicken Sie auf "Tools>Internet-Optionen". Wählen Sie die Karteikarte "Inhalte" und in dem Bildschirmteil "Persönliche Daten" klicken Sie auf die Taste "AutoComplete". Deaktivieren Sie alle, außer "Web-Adressen", in dem Teil "AutoComplete verwenden für". Dann klicken Sie auf "Formulare löschen" beziehungsweise "Passwörter löschen". Bitte beachten Sie, dass alle Formulare und Passwortinformationen, die bereits in Ihrem Computer gespeichert sind, gelöscht werden. Klicken Sie zweimal auf die Taste "OK", um aus dem Programm herauszugehen.

2.4 HÄUFIG GESTELLTE FRAGEN

2.4.1 Über DHB Net Banking

- *Wie kann ich mit der Nutzung von DHB Net Banking beginnen?*

  Sie können sich einfach von unserer Website aus bei DHB Net Banking anmelden. Ihr Antrag wird bearbeitet und Ihnen zwecks Unterschrift zugesandt. Danach können Sie DHB Net Banking innerhalb von einigen Tagen nutzen!

  Sie werden Folgendes benötigen, um DHB Net Banking nutzen zu können:

  - Einen Computer,
  - Internet-Zugang und
  - einen unterstützten Browser (Internet Explorer oder Mozilla Firefox)

- *Was kann ich mit DHB Net Banking tun?*

  DHB Net Banking ermöglicht Ihnen:

  - Geldüberweisungen auf Ihr vorher mitgeteilte Referenzkonto
  - Geldüberweisungen zwischen DHB Konten
  - Die Prüfung Ihrer Kontosalden
  - Die Einsichtnahme in Ihre Transaktionsgeschichte
  - Festgeldanlagen online umbuchen
    Änderung der Kontaktdaten
  - Die Einsicht in Ihren Freistellungsauftrag bzw.
    Nichtveranlagungsbescheinigung

- *Wie viel kostet DHB Net Banking?*

  DHB Net Banking ist völlig kostenlos.

- *Steht DHB Net Banking 24 Stunden zur Verfügung?*

  Sie können jederzeit, an jedem Wochentag auf DHB Net Banking zugreifen.

- *Kann ich von anderen Computern aus auf DHB Net Banking zugreifen?*

  Sie können DHB Net Banking auch von anderen Computern aus nutzen.

- *Sind meine Transaktionen limitiert?*

  Das tägliche Limit beträgt bei der DHB Bank N.V. € 25.000,-. Eine Änderung des Online-Überweisungslimits ist durch Einreichung des entsprechenden Formulares bis 50.000€ möglich. Den Vordruck finden Sie in unserem Formularcenter.

2.4.2 Die Nutzung von DHB Net Banking

- *Kann ich eine Transaktion annullieren, wenn ich meine Meinung geändert habe?*

Um eine Transaktion zu veranlassen, werden Sie zweimal gebeten, diese zu bestätigen. Sollten Sie Ihre Meinung vor der zweiten Bestätigung ändern, können Sie die gesamte Transaktion immer noch abbrechen. Wenn Sie jedoch das zweite Mal bestätigt haben, wird die Transaktion wirksam.

- *Was geschieht, wenn ich mein Passwort vergessen habe?*

Wenn Sie Ihr Passwort vergessen, sollten Sie das Call Center der DHB Bank während den Betriebszeiten (08.00 -17.30 Uhr) unter der Rufnummer 0211-210 90 898 zwecks Unterstützung anrufen. Außerhalb dieser Zeiten, können Sie auch eine E-Mail an dhbnetbanking.de@dhbbank.com zusenden.

- *Was sollte ich tun, wenn ich nach dem Anklicken eines Hyper-Links oder eines Icons keine Reaktion erhalte?*

Das Internet wird zu manchen Zeiten zwangsläufig zu langsam, um zu reagieren. Wenn es eine Verzögerung gibt, warten Sie bitte. Klicken Sie bitte nicht mehrfach auf einen bestimmten Link. Alternativ können Sie eine Bildauffrischung durchführen und es noch einmal versuchen.

- *Wie kann ich in Erfahrung bringen, ob meine Transaktionen durchgeführt wurden, wenn mein Computer abstürzt oder meine Verbindung mit dem Internet auf halbem Wege unterbrochen wird?*

Sie brauchen sich nur neu anzumelden, um Ihren Kontosaldo zu überprüfen oder die Transaktion neu einzugeben, falls dies erforderlich ist. Wenn Sie jedoch Zweifel oder Fragen haben, rufen Sie einfach das Call Center der DHB Bank während den Betriebszeiten (08.00 -17.30 Uhr) unter 0211-210 90 898 zwecks Statusüberprüfung an.

Sie können sicher sein, dass jede Transaktion, für die Sie einen Bestätigungsbildschirm erhalten haben, bearbeitet wird. Wenn mitten in Ihrer Finanztransaktion ein Systemfehler auftritt und Sie Ihre Bestätigung noch nicht erhalten haben, sollten Sie die Buchungen und Transaktionen überprüfen, die noch bearbeitet werden, nachdem das System wieder hochgefahren wird. Wenn Sie die fragliche Transaktion nicht finden, müssen Sie sie neu eingeben.

- *Meldet das System sich ab, wenn das Auszeit-Limit erreicht ist, auch wenn ich die Transaktionen nicht beendet habe?*

Solange es Aktivität gibt, werden Sie nicht abgemeldet. Eine unserer Sicherheitsfunktionen ist, dass Sie nach 10 Minuten Inaktivität automatisch abgemeldet werden, um eine unautorisierte Einsichtnahme in Ihr Konto zu verhindern.

- *Warum ist der Zugriff auf DHB Net Banking zu manchen Zeiten langsamer?*

Dies hängt von dem Netzverkehr zum Zugriffszeitpunkt ab. Wenn es viel Verkehr gibt, wird der Zugriff langsam, weil viele Benutzer gleichzeitig auf eine limitierte Kapazität auf der Internet-Datenautobahn zugreifen.

2.4.3 Über Sicherheit

- *Wie sicher ist DHB Net Banking?*

DHB Net Banking verwendet moderne Internet-Technologien, die weltweit von Finanzdienstleistern eingesetzt werden, um das Internet-Banking ebenso sicher wie bequem zu gestalten. Diese Technologien sind so konzipiert, dass Sie Ihre Daten während des gesamten von Ihrem Computer ausgehenden Prozesses durch die DHB Bankeigenen Systeme schützen. Ihre Kontodaten sind bei DHB Net Banking sicher.
Bitte lesen Sie die Seite "Sicherheit und DHB Net Banking", um weitere Informationen zu erhalten.

- *Was sollte ich tun, um DHB Net Banking so sicher wie möglich zu machen?*

Während die DHB Bank daran arbeitet, Ihre Banking-Daten zu schützen, spielen Sie bei dem Schutz Ihrer Konten ebenfalls eine Rolle. Es gibt einige Maßnahmen, mit denen Sie dafür sorgen können, dass Ihr Internet - Banking sicher ist.

Fünf Maßnahmen, mit denen Sie sich schützen können:

1. Als Erstes und Wichtigstes, wählen Sie einen Benutzernamen und ein Passwort, die für andere nicht leicht zu erraten sind. Für die Auswahl eines schwer zu erratenden Passworts, sollten Sie bitte keine Eigennamen, wohl bekannte Begriffe, Wiederholungen einzelner Zeichen („AAAAA“) oder Tastaturfolgen („qwertz“) vermeiden. Geben Sie Ihren Benutzernamen oder Ihr Passwort an niemand anderen weiter. Ihr Benutzername und Ihr Passwort sind dafür da, die Privatsphäre Ihrer Bankdaten zu schützen. Bitte wechseln Sie Ihre Zugangsdaten umgehend, wenn Sie Grund zur Annahme haben, dass irgendjemand Ihre Zugangsdaten erfahren haben könnte.

2. Gehen Sie nicht von Ihrem Computer weg, wenn Sie sich inmitten einer Verbindung befinden.

3. Nachdem Sie Ihre Bankgeschäfte erledigt haben, melden Sie sich unbedingt wieder ab. Klicken Sie dazu immer auf den Button „Abmelden“. Somit wird die Verbindung zum OnlineBanking Rechner getrennt. So stellen Sie sicher , dass kein Unberechtigter Zugriff auf Ihr Konto erhält.

4. Wenn Ihr Computer wahrscheinlich von anderen Personen genutzt wird, löschen Sie Ihren Cache-Speicher oder schalten Sie ihn aus und reinitiieren Sie Ihren Browser, um Kopien von Web-Seiten zu eliminieren, die auf Ihrer Festplatte gespeichert wurden. Wie Sie Ihren Cache-Speicher löschen, ist von dem Browser und der Version abhängig, die Sie besitzen. Diese Funktion findet sich im Allgemeinen in Ihrem Präferenz-Menü.

5. Ändern Sie Ihr Passwort regelmäßig.

DHB Bank empfiehlt dringend, dass Sie einen Browser mit einer 128-Bit-Verschlüsselung verwenden, um sichere Finanztransaktionen über das Internet durchführen zu können.

- *Was kann man tun, wenn ich den Verdacht habe, dass jemand einen nicht autorisierten Zugriff auf mein Konto hat?*

Rufen Sie unverzüglich unsere Kundenbetreuer unter 0211-210 90 898 an und teilen Sie Ihren Verdacht mit.

- *Was sollte ich tun, wenn ich glaube, dass online auf mein Konto zugegriffen wurde?*

Kontaktieren Sie bitte umgehend unsere Kundenbetreuer unter 0211-210 90 898. Wenn Sie sich nicht an Ihren Benutzernamen oder Ihr Passwort erinnern können, werden unsere Mitarbeiter Ihr Konto blockieren und Ihre Benutzer-ID und Ihr Passwort sperren, um sicherzustellen, dass niemand diese Details in Zukunft missbrauchen kann. Wenn Sie den Verdacht haben, dass jemand Ihr DHB Net Banking-Konto ohne Ihre Erlaubnis genutzt hat, ist es besser, die Kundenbetreuung um Rat zu fragen, als Ihren Verdacht zu ignorieren.

- *Ich empfinde es als schwierig, mir mein Net Banking Passwort zu merken. Was kann ich tun?*

Wenn Sie Ihr Passwort oder sogar Ihren Benutzernamen vergessen haben, rufen Sie die Kundenbetreuung an. Nachdem Sie sich identifiziert haben, wird man dort veranlassen, dass Ihnen Ihr Passwort-Erinnerungstext nach Wunsch mitgeteilt wird. Damit Sie sich besser an Ihr Passwort erinnern können, verbinden Sie diesermit Zahlen, Daten oder Namen, die für Sie persönlich sind. Schreiben Sie diese nicht auf.

- *Was tue ich, wenn ich eine unbekannte E-Mail erhalte?*

Wenn Sie Zweifel haben, öffnen Sie keine unerbetenen E-Mails, wenn Sie sich nicht sicher sind, wer sie abgeschickt hat. Wenn Sie eine solche E-Mail erhalten, löschen Sie sie einfach, ohne sie zu öffnen.

- *Welche Informationen sollte ich nie in einer E-Mail erwähnen?*

Geben Sie in einer E-Mail niemals Ihre persönlichen (Login) Daten (wie Ihre Kontonummer, Ihr Geburtsdatum oder Ihr Passwort) weiter.

- *Sind meine vertraulichen Informationen sicher?*

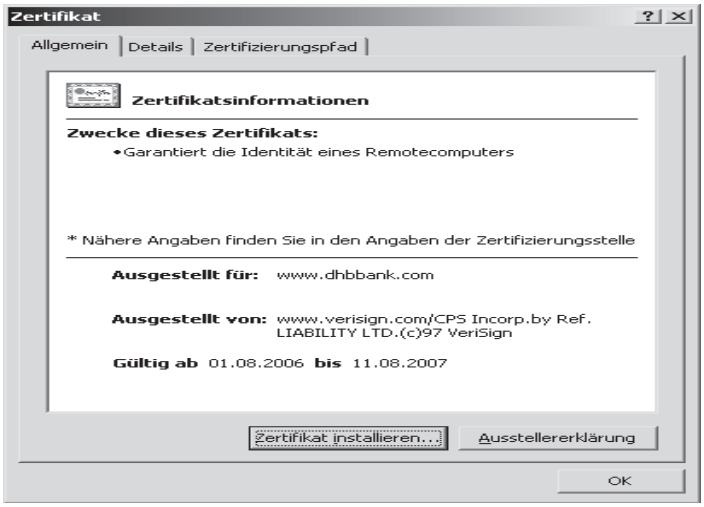
Jedes Mal, wenn Sie auf Kontoinformationen in einem Ihrer sicheren Online-Bereiche zugreifen oder diese mitteilen, werden diese Informationen durch eine Technologie namens Secure Sockets Layer, häufig abgekürzt als SSL verschlüsselt. Die SSL-Technologie codiert und versteckt Daten, wenn sie zwischen Ihrem Computer und den DHB Bank-Systemen verschickt werden, und hilft dabei sicherzustellen, dass die Informationen vertraulich bleiben. Die Verwendung von SSL erfordert zwei Komponenten: einen SSL-kompatiblen Browser und einen Web-Server, die den "Schlüsselaustausch" durchführen können, der eine SSL-Verbindung mit dem DHB Bank-Webserver-System herstellt.

DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

- *Wie überprüfe ich das Sicherheitszertifikat der DHB Bank?*

Damit Sie sicher sein können, dass die DHB NetBanking Bank Seiten nicht gefälscht sind, besitzen die Seiten spezielle Zertifikate, die automatisch vom Browser überprüft werden, sobald Sie die Seiten aufrufen.

Das Schloss-Symbol erscheint bei einer sicheren Verbindung in der Statusleiste unten rechts. Durch Doppelklick auf dieses Symbol öffnet sich das Dialogfenster mit Eigenschaften und Inhalten des Zertifikate. Unter „Allgemein" muss ausgeführt sein, dass das Zertifikat für www.dhbbank.com ausgestellt ist, von www.verisign.com ausgestellt wurde und aktuell noch gültig ist.



Unter Details erhält man weitere Informationen zur Echtheit des DHB Bank Zertifikats.

- Das Datum im Feld „Gültig bis" muss in der Zukunft liegen
- Als „Antragsteller" muss die DHB Bank genannt sein
- Im Feld „Fingerabdruck" muss der Ausdruck "B0A2 A853 EEFE 7C98 7DAA 61D0 4EC1 3BFB AB06 A98A" stehen.

- *Welchen Browser-Typ benötige ich?*

Um von der SSL-Technologie zu profitieren, benötigen Sie einen SSL-fähigen Browser. Zu den Beispielen für SSL-Browser gehören Mozilla Firefox, Microsofts Internet Explorer (Bitte beachten Sie, dass einige ältere Browser-Versionen SSL-Verbindungen nicht unterstützen). Wenn Sie noch keinen SSL-fähigen Browser haben, können Sie von einem der folgenden Links einen SSL-fähigen Browser herunterladen.

- Mozilla Firefox
- Microsoft's Internet Explorer

- *Welche Art Verbindung benötige ich?*

Fast alle Internet Service Provider (ISPs) geben die oben beschriebene SSL- Verbindung frei. Wenn Sie die interne Verbindung Ihrer Firma für den Internet-Zugang verwenden, und nicht mit einem oben beschriebenen SSL- Browser auf die gesicherten DHB Bank-Seiten zugreifen können, kann es sein, dass Ihre Firma den Zugriff mittels einer "Firewall" blockiert. Bitte besprechen Sie weitere Details über den Internetzugang Ihres Netzes mit dem System-Administrator, der für den Internetzugang Ihrer Firma zuständig ist.

- *Was soll ich tun, wenn ich meinen Zugriff auf vertrauliche Daten beendet habe?*

Wenn Sie die Nutzung eines sicheren Bereiches des Online-Service der DHB Bank beendet haben, vergewissern Sie sich, dass Sie immer das rote Link "Sicheren Bereich verlassen" anklicken, das auf der linken Seite jeder gesicherten Seite erscheint. Wenn Sie dies anklicken, erhalten Sie die Option, Ihre sichere Verbindung zu beenden. Es können dann keine weiteren sicheren Transaktionen durchgeführt werden, ohne dass Sie Ihre Benutzer-ID und Ihr Passwort erneut eingeben.

- *Warum kann ich noch immer einige meiner Kontodaten sehen, obwohl ich die Verknüpfung "Sichere Abmeldung" angeklickt habe?*

Die Browser-Software "versteckt" häufig Seiten, die Sie ansehen, das heißt, dass einige Seiten in dem temporären Speicher Ihres Computers gespeichert werden. Daher könnten Sie denken, dass das Klicken der Schaltflächen "Zurück" Ihnen eine gespeicherte Version einer zuvor angesehenen Seite zeigt. Bitte beachten Sie, dass das "Verstecken" die Sicherheit Ihrer vertraulichen Benutzer-ID oder Ihres Passworts in keiner Weise beeinflusst. Wenn Sie ein PC an einem öffentlichen Ort verwenden, lesen Sie bitte den folgenden Absatz "Was sollte ich tun, wenn ich einen "öffentlichen" Computer benutze?"

- *Was sollte ich tun, wenn ich einen öffentlichen Computer benutze?*

Wenn Sie einen Computer benutzen, an dem auch andere arbeiten und Sie das ungute Gefühl haben, dass diese eventuell "versteckte" Seiten einsehen könnten, nachdem Sie die Station verlassen haben, beenden/verlassen Sie Ihre Browser-Software, bevor Sie weggehen. Andere Benutzer werden ohne Ihre Benutzer-ID und Ihr Passwort online nicht auf Ihre Kontoinformationen zugreifen können.

DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

Viren

- *Was ist ein Virus und wie arbeitet es?*

Computerviren sind Programme, die sich selbst reproduzieren und sich beispielsweise per E-Mail über das Internet weiterverbreiten können. Viren können auf den infizierten PCs teilweise erhebliche Schäden anrichten.

- *Wie entferne ich ein Virus?*

Wenn Sie ein Anti-Virus-Programm installieren, scannt und löscht es Viren normalerweise. Setzen Sie sich mit Ihrem örtlichen Computer-Händler in Verbindung, der Sie im Hinblick auf den Kauf eines geeigneten Anti-Virus- Programmes beraten kann.
Es ist jedoch überaus wichtig, dass Sie regelmäßige Viren-Scans durchführen, um mit zu der Sicherheit beizutragen, dass Ihr PC so rein und frei von Viren bleibt, wie möglich. Wenn Sie nicht sicher sind, wie oft Sie einen Virus-Scan durchführen müssen, setzen Sie sich bitte mit Ihrem Software-Anbieter in Verbindung.

Hacker

- *Kann ein Hacker meine Kontoinformationen wiederfinden und sie an jemand anderen schicken?*

Um Kontoinformationen zu entschlüsseln, muss ein Hacker Milliarden von Sequenzen und Kombinationen ausprobieren.

Die DHB Bank verwendet leistungsfähige Verschlüsselungsniveaus, um zu der Gewährleistung beizutragen, dass die Informationen, die zwischen Ihrem PC und der Bank übertragen werden, sicher sind. Darüber hinaus setzt die DHB Bank den neuesten Firewall-Schutz ein, um Hacker aufzuspüren und Ihre Kontoinformationen in unseren Systemen zu schützen.

Einige Hacker können versuchen, durch "Trojaner" (eine von Hackern verwendete Software) auf den PC einer Person zuzugreifen. Diese Software kann zum Beispiel dazu verwendet werden, die betätigten Tasten und somit die Informationen, die der Person über die Tastatur eingibt, zu kopieren - hierunter könnten auch persönliche Dokumente oder auch persönliche Details sein.

Wir möchten Kunden warnen, immer sehr vorsichtig zu sein, wenn Sie E-Mails aus unbekannten Quellen öffnen. Dies ist der wahrscheinlichste Weg, auf dem dieser Art von Betrug versucht werden könnte.

Das Befolgen der Ratschläge in dieser Anleitung sollte dabei behilflich sein, die Wahrscheinlichkeit zu senken, dass Hacker Zugriff auf Ihre persönlichen Dokumente oder Kontoinformationen erhalten.

DHB Bank
DEMİR-HALK BANK (NEDERLAND) N.V.

Glossar

Cache

Ein Cache ist ein Zwischenspeicher auf der Festplatte eines Computers oder eines externen Rechners.

Cookie

Ein Cookie ist eine kleine Textdatei, die der Web-Browser auf Anweisung eines Web-Servers in dem PC des Anwenders speichert und die zum Beispiel Angaben über dessen Web-Anfragen enthält. Cookies dienen hauptsächlich als elektronischer Merkzettel für den Server, um benutzerspezifische Browser-Abfragen festzuhalten, zum Beispiel welche Web-Seite ein Nutzer wie häufig und wie lange besucht hat oder ob die angeforderte Web-Seite in einer bestimmten, vom Nutzer festgelegten Version übersandt werden soll.

Firewall

Als Firewall bezeichnet man Rechner, die den Datenverkehr zwischen einem lokalen Netz oder einem allein stehenden Rechner und anderen Netzwerken, zum Beispiel dem Internet, regeln. Die Firewall soll das lokale Netz bzw. den allein stehenden Rechner vor unbefugten Zugriffen schützen. Unter einer persönlichen Firewell wird ein Programm verstanden, das auf Ihrem PC eine Firewall realisiert, dass heißt Ihren PC ohne Einsatz eines Zusatzrechners vor unerwünschten Zugriffen bewahrt.

Phishing

Angriffsmethode, bei der ein Angreifer die E-Mail-Adresse oder die Internetseite von Banken und Dienstleistern wie Internetserviceprovidern oder Internetkaufhäusern vortäuscht. Die Kunden werden aufgefordert, ihre Kontodaten sowie dazugehörige PINs, TANs und Passwörter auf einer gefälschten Internetseite einzugeben.

Pharming

Unter Pharming oder auch DNS Spoofing bezeichnet man eine Attacke, bei der ein Angreifer die IP-Adresse eines bekannten Domain-Namens durch seine eigene ersetzt. Bei einem solchen Angriff wird die URL richtig dargestellt, obwohl sich der Nutzer auf einer falschen Seite befindet.

Trojanische Pferd (Trojaner)

Unter dem Stichwort "Trojanische Pferde" versteht man Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

Spyware

Als Spyware werden Softwareprogramme bezeichnet, die Informationen über den PC des Nutzers, dessen Surfgewohnheiten oder auch dessen persönliche Daten (zum Beispiel geheime Zugangsdaten für Online Banking) ohne dessen Wissen oder gar Zustimmung an Dritte senden.

Stand: 09-2018