Sicherheitshinweise

Unsere Online Services umfassen das OnlineBanking mit chipTAN, smsTAN und pushTAN (ab Juli 2016) sowie das OnlineBanking mit elektronischer Signatur (HBCI) und die telefonischen Verfügungsmöglichkeiten über das TelefonBanking und das Haspa-DIREKT-Cashkonto. Ihre personalisierten Sicherheitsmerkmale gelten einheitlich für alle Online Services, für deren Nutzung Sie sich entschieden haben. Bitte beachten Sie in diesem Zusammenhang die folgenden Sicherheitshinweise:

Umgang mit Ihren personalisierten Sicherheitsmerkmalen

- Ihre PIN und eventuelle Passwörter sind personenbezogene Legitimationsmittel. Diese sollten weder notiert, gespeichert noch direkt anderen Personen und Institutionen mitgeteilt werden.
- Falls Sie den Verdacht haben, dass Unberechtigte Zugang zu Ihren Legitimationsmitteln erlangt haben, veranlassen Sie bitte unmittelbar eine Sperre. Bitte nehmen Sie in diesem Fall sofort Kontakt zu unserer Hotline auf, Tel. 040 3579-7426 bzw. 040 3579-0 außerhalb der Geschäftszeiten (kostenpflichtig gemäß Ihrem Telefonvertrag). Notfalls können Sie Ihren Zugang auch mit einer dreimaligen PIN-Fehleingabe sperren.
- Ändern Sie regelmäßig Ihre PIN und Passwörter, um möglichen unberechtigten Personen den Zugang zu Ihren Konten und Depots in den Online Services zu erschweren. Dabei sollten Sie keine leicht zu erratende Zahlenkombination wie z. B. Geburtsdaten, keine Namen aus der Verwandtschaft, Städtenamen, Geburtsdaten, usw. verwenden. Grundsätzlich gilt: Je mehr Zeichen Ihre PIN/Passwort hat, desto schwieriger ist es zu erraten.
- Haben mehrere Nutzer dasselbe Identifikationskonto angegeben, so werden bei dreimaliger falscher PIN-Eingabe durch einen Nutzer oder einen Dritten alle Nutzer mit diesem Identifikationskonto gesperrt.
- Eine Sperre von Legitimationsmitteln gilt für alle genutzten Online Services.
- Bitte beachten Sie bei der Nutzung des Telefons, dass die Sicherheit Ihrer PIN/Passwörter gewährleistet ist (z. B. Einsehbarkeit des Telefondisplay, Wahlwiederholungstaste).
- Die Haspa wird Sie niemals per E-Mail, per Fax, telefonisch oder persönlich zu Aktionen auffordern, in deren weiteren Verlauf die Angabe Ihrer Legitimationskontonummer oder PIN erforderlich wird. Bei allen von der Haspa - im Rahmen der Online Services - angebotenen Textnewslettern werden nur Verlinkungen zu weiterführenden Inhalten aufgeführt, die mit der URL „http://haspa.de/“ bzw. „http://joker.haspa.de/“ beginnen.

Umgang mit Schlüsseln der elektronischen Signatur

- Wir weisen ausdrücklich darauf hin, dass der Schlüssel der elektronischen Signatur auf einem externen Medium und nicht auf der Festplatte zu speichern ist, da ansonsten ein erhöhtes Sicherheitsrisiko besteht.

Umgang mit chipTAN

- Bitte prüfen Sie, ob die auf dem Display des TAN-Generators angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte chipTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.

Umgang mit smsTAN

- Bitte prüfen Sie, ob die auf dem Handy-Display angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte smsTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.
- Bitte denken Sie daran, dass die Sicherheit beim smsTAN-Verfahren darauf beruht, dass die Dateneingaben zum OnlineBanking und die Übermittlung der smsTAN auf getrennten Wegen erfolgen. Wenn Sie ein Smartphone verwenden und das OnlineBanking über dieses Smartphone nutzen, werden diese Informationen auf dem gleichen Gerät zusammengeführt und bieten somit ein Angriffspotential für Phishing-Angriffe.

Umgang mit pushTAN

- Bitte prüfen Sie, ob die in der pushTAN-App angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte pushTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.
- Bitte denken Sie daran, dass die Sicherheit beim pushTAN-Verfahren auch darauf beruht, dass Sie ein originales und aktuelles Betriebssystem auf Ihrem Smartphone nutzen.

Handys/Smartphones

- Für die smsTAN ist keine Installation von zusätzlicher Software auf dem Handy/Smartphone erforderlich.
- Die Haspa wird Sie nie nach der IMEI Ihres Handys/Smartphones (die 15-stellige Seriennummer des Gerätes) fragen.
- Nutzen Sie für Ihr Handy/Smartphone möglichst eine Sicherheitssoftware. Sie können Ihr Handy/Smartphone wie einen PC schützen.

IMEI und andere Angaben zu Ihrem Handy/Smartphone werden zur Manipulation des Gerätes benötigt. Im Zweifelsfall brechen Sie den Vorgang sofort ab und nehmen Kontakt mit unserer Hotline auf.

Virenschutzprogamm und Firewall einsetzen

Verschiedene Arten von Schadprogrammen („Trojanische Pferde“, „Viren“, usw.) bedrohen die Sicherheit Ihres Computers und folglich des OnlineBanking/OnlineBrokerage. Zum Schutz Ihres Computers setzen Sie bitte unbedingt Virenschutz- und Firewall-Software ein. Halten Sie die Softwareprodukte stets aktuell. Näheres finden Sie auf den Herstellerseiten.

Betriebssystem und Anwendungssoftware

Bitte achten Sie darauf, dass sich Ihr Betriebssystem sowie die Anwendungssoftware (z. B. Browser, Acrobat Reader usw.) auf dem aktuellsten Stand befindet. Näheres finden Sie auf den Herstellerseiten.

Online Service / OnlineBanking-Software niemals unbeaufsichtigt lassen

Beenden Sie die Online Services immer über die dafür vorgesehenen Schaltflächen – z. B. „Logout“ und schließen Sie Ihr OnlineBanking-Programm, sobald Sie Ihren Computer verlassen, auch wenn es nur für kurze Zeit ist.

OnlineBanking-Limite festlegen

Vereinbaren Sie Überweisungshöchstbeträge (Limite). Nutzen Sie hierfür im Sicherheitsbereich die entsprechenden Geschäftsvorfälle.

Daten aus dem OnlineBanking/OnlineBrokerage exportieren

Wenn Sie die Exportfunktionen nutzen, werden persönliche Daten, z. B. Kontoumsätze, auf dem Computer gespeichert. Diese sind durch andere Nutzer des Rechners einsehbar. Löschen Sie bitte ggf. die exportierten Daten, wenn Sie diese nicht mehr benötigen, damit Dritte keinen Zugriff auf die Daten erhalten.

Allgemeine Hinweise zum Verhalten im Internet

- Wir empfehlen, neben den Online Services keine weiteren Internet-Seiten parallel zu öffnen.
  Während der gesamten Zeit, in der Sie unsere Online Services über www.haspa.de (OnlineBanking/OnlineBrokerage) nutzen, muss in der Adresszeile Ihres Browsers die Internetadresse „https://banking.haspa.de/banking/...“ vorangestellt sein. Zusätzlich nutzen die Browser spezifische Symbole („Schloss“) für die Anzeige der gesicherten Datenübertragung. Ist eines der vorgenannten Merkmale nicht erfüllt schließen Sie Ihren Browser und beenden unverzüglich die Internetverbindung.
- Der Aufruf der Online Services über www.haspa.de sollte generell immer durch die Eingabe der Internetadresse im Browser erfolgen. Von der Nutzung von Verlinkungen aus E-Mails und von Fremdseiten wird dringend abgeraten.
- Eine besondere Gefahr besteht bei Downloads aus dem Internet und beim Öffnen von E-Mail-Anhängen. Laden Sie nur solche Programme herunter, die Sie wirklich benötigen und deren Quelle Sie vertrauen. E-Mail-Anhänge fragwürdiger Herkunft sollten nicht geöffnet und unverzüglich gelöscht werden.
- Deaktivieren Sie Funktionen wie „AutoVervollständigen“ oder „Passwort speichern“, die wiederkehrende Eingaben wie Webadressen, Formularinhalte, Benutzernamen und Passwörter automatisch ausfüllen.
- Je Transaktion ist immer nur **eine** TAN erforderlich. Werden mehrere TAN gleichzeitig abgefragt, geben Sie bitte auf keinen Fall eine TAN ein, sondern brechen Sie den Vorgang ab und informieren Sie die Hotline.

Diese und weitere wichtige Hinweise finden Sie auf www. haspa.de unter dem Suchbegriff „Sicherheitstipps“.

Januar 2017 **Hamburger Sparkasse AG**