Informationen und Sicherheitshinweise

zum SaarLB Online-Banking und zu Internetzahlungen mit der SaarLB Business Card (Kreditkarte)

Die deutsch-französische Regionalbank
La banque régionale franco-allemande

WEITSICHT DURCH NÄHE

Informationen und Sicherheitshinweise zum SaarLB Online-Banking und zu Internetzahlungen mit der SaarLB Business Card (Kreditkarte)

Fassung Oktober 2018

Einführung in das Online-Banking der SaarLB

Mit dem Online-Banking der SaarLB können Sie Ihre Finanzgeschäfte erledigen, wann und wo Sie möchten. Auf die wichtigsten Fragen, wie das funktioniert und was es zu Ihrer Sicherheit zu beachten gibt, möchten wir mit dieser Übersicht Antwort geben. Natürlich stehen wir Ihnen darüber hinaus persönlich für Ihre Fragen zur Verfügung.

Welche Vorteile bietet mir Online-Banking?

- **Schnell:** Mit wenigen Klicks können Sie Geld überweisen, Daueraufträge einrichten oder Kontoauszüge prüfen. So sparen Sie viel Zeit.
- **Einfach:** Die intuitive Bedienung und übersichtliche Gestaltung helfen Ihnen, sich zurechtzufinden. Sie können direkt loslegen.
- **Bequem:** Sie können dann auf Ihr Girokonto zugreifen, wenn es in Ihren Zeitplan passt, von zu Hause aus, vom Arbeitsplatz aus oder auch von unterwegs.
- **Sicher:** Das Online-Banking der SaarLB arbeitet mit höchsten Sicherheitsstandards. So ist Ihr Geld optimal geschützt.

Was benötige ich zur Teilnahme am Online-Banking?

- **SaarLB-Konto:** Wenn Sie ein Girokonto bei der SaarLB haben, können Sie das Online-Banking jederzeit kostenlos freischalten lassen. Sie erhalten umgehend Ihren Anmeldenamen. Die PIN (Persönliche Identifikationsnummer) erhalten Sie per Post zugesandt und können direkt loslegen.
- **SaarLB-BankCard (Debitkarte):** Für das Online-Banking benötigen Sie eine SaarLB-BankCard (Debitkarte). Diese Karte setzen Sie für die Freigabe von Transaktionen im Online-Banking ein.
- **Computer, Smartphone oder Tablet:** Für das Online-Banking benötigen Sie einen Computer oder ein anderes internetfähiges Endgerät, wie etwa ein Smartphone oder einen Tablet-PC. Speziell für die Nutzung auf Smartphones bietet die Sparkassen-Finanzgruppe eigene Apps an, beispielsweise die App „Sparkasse“ (nähere Informationen unter „Kann ich mein Online-Banking auch mobil nutzen?“).
- **Internetzugang:** Um das Online-Banking nutzen zu können, muss Ihr Endgerät über eine Verbindung mit dem Internet verfügen. Dabei kommt es nicht auf die Geschwindigkeit an: Das Online-Banking der SaarLB funktioniert unabhängig davon, ob Sie über ein Highspeed-Kabelnetz oder mit Ihrem Handy surfen.
- **Sicherheit:** Nicht nur für das Online-Banking ist die Installation eines aktuellen Internetbrowsers, eines Virenschutzprogramms und einer „Firewall“ sinnvoll. Daneben legen Sie einmalig das von Ihnen gewählte Sicherheitsverfahren für das Online-Banking fest (nähere Informationen unter „Was ist ein Online-Banking-Sicherheitsverfahren?“).
- **Beim Sicherheitsverfahren chipTAN:** Für die Durchführung von Transaktionen im Online-Banking der SaarLB benötigen Sie zusätzlich einen „TAN-Generator“. Diesen können Sie bequem im Online-SparkassenShop bestellen: **www.sparkassenshop.de**, Menüpunkt Chipkartenleser/TAN-Generatoren.
- **Beim Sicherheitsverfahren HBCI:** Statt eines TAN-Generators benötigen Sie ein HBCI-Kartenlesegerät und eine spezielle Bankingsoftware, z. B. „StarMoney“. Beides können Sie bequem im Online-SparkassenShop bestellen unter **www.sparkassenshop.de**, Menüpunkt Chipkartenleser/Secoder bzw. Menüpunkt Online-Banking-Software.

Was ist ein „Online-Banking-Sicherheitsverfahren“?

Sie rufen Ihren Kontostand, Ihre Kontoauszüge etc. in einem geschützten Bereich ab. Dafür nutzen Sie einen Anmeldenamen und eine persönliche Identifikationsnummer, kurz PIN.

Neben der PIN für den allgemeinen Zugang bestätigen Sie jede einzelne Transaktion vor der Ausführung, um vor Missbrauch geschützt zu sein. Diese Bestätigung können Sie auf zwei verschiedene Arten durchführen, je nachdem, für welches Sicherungsverfahren Sie sich entscheiden. Das Sicherungsverfahren vereinbaren Sie mit der SaarLB einmalig vor der ersten Nutzung.

Welche Sicherheitsverfahren bietet die SaarLB an?

Wir bieten Ihnen mit chipTAN und HBCI zwei unterschiedliche Sicherheitssysteme. Beide sind immer auf dem neuesten Stand und bieten Ihnen höchstmöglichen Schutz. Welches Sicherungssystem für Sie das richtige ist, hängt von Ihren Nutzungsgewohnheiten im Online-Banking ab.

chipTAN – sicher mit Karte und TAN-Generator

Neben der PIN für den allgemeinen Zugang bestätigen Sie jede Transaktion mit einer Transaktionsnummer (TAN). Im chipTAN-Verfahren erzeugen Sie mithilfe Ihres TAN-Generators und Ihrer SaarLB-BankCard (Debitkarte) selbst diese TAN.

Vorteile chipTAN:

- hoher Schutz durch zeitlich begrenzte Gültigkeit der chipTAN
- Kontrollmöglichkeit durch Anzeige der wichtigsten Auftragsdaten
- nahezu kein Missbrauch möglich, da die chipTAN nur für einen speziellen Auftrag gültig ist
- keine zusätzliche PIN neben der Online-Banking-PIN notwendig
- bei griffbereitem TAN-Generator Zugriff auf Ihr Online-Konto von jedem anderen (gesicherten) Rechner aus

Für wen ist chipTAN geeignet:

- Nutzung der Girokonto-Funktionen vorwiegend online
- nur Konten im Inland
- gelegentliche bis durchschnittlich häufige Veranlassung von Kontobewegungen

HBCI – die digitale Unterschrift

HBCI steht für „Homebanking Computer Interface“ und ist für Intensivnutzer des Online-Bankings geeignet. Für das HBCI-Verfahren benötigen Sie eine spezielle Bankingsoftware und ein spezielles HBCI-Kartenlesegerät.

Vorteil HBCI:

- Bei Nutzung einer Bankingsoftware sind Ihre Daten durch eine hohe Verschlüsselungstechnik zusätzlich geschützt.

Für wen ist HBCI geeignet:

- kleine bis mittlere Gewerbetreibende
- Privatpersonen mit sehr häufiger Veranlassung von Kontobewegungen
- Nutzung Online-Banking auch für freiberufliche Tätigkeiten am eigenen PC

Wie nutze ich das Online-Banking?

Eine ausführliche Schritt-für-Schritt-Anleitung in Bild und Text von der Erstanmeldung bis zur Durchführung einer Überweisung haben wir für Sie in einem eigenen „Leitfaden Online-Banking SaarLB“ zusammengefasst. Sie finden diesen Leitfaden als Download direkt unter dem Anmeldebutton zum Online-Banking unter www.saarlb.de.

Kann ich mein Online-Banking auch mobil nutzen?

Mit den Apps der Sparkassen-Finanzgruppe können Sie Ihre Bankgeschäfte auch bequem mobil erledigen.

App Sparkasse

Mit dieser kostenlosen App können Sie immer und überall Ihre aktuellen Kontostände einsehen, Überweisungen abschicken oder Ihre Rechnungen bequem mit Girocode zahlen. Einfach den „QR-Code“ auf Ihrer Rechnung einscannen und zahlen – ohne lästiges Eintippen der Überweisungsdaten. Oder Sie lassen sich von der App zum nächstgelegenen Geldautomaten lotsen.

App Sparkasse+

Mit Sparkasse+ können Sie Konten von beliebig vielen Sparkassen und Banken einrichten. Mit der App haben Sie Ihre Umsätze im Blick, können Überweisungen vornehmen oder Rechnungen ohne Eingabe von Überweisungsdaten mit der Funktion „QR-Code einlesen“ bezahlen.

Hinweise für mehr Sicherheit im Online-Banking

Bevor Sie Online-Banking nutzen, nehmen Sie sich bitte einige Minuten Zeit für die nachfolgenden wichtigen Informationen.

Wie kann ich mich gegen Angriffe aus dem Internet bestmöglich schützen?

- Aktualisieren Sie regelmäßig Ihr Betriebssystem, Ihren Internetbrowser und Ihre eingesetzten Programme.
- Arbeiten Sie nicht mit Administratorrechten auf Ihrem Computer.
- Halten Sie Firewall und Virenscanner immer aktuell.
- Nutzen Sie nur Software aus sicheren Quellen.
- Melden Sie sich nach dem Online-Banking ab und löschen Sie den Browserverlauf und Cache.
- Erledigen Sie Bankgeschäfte und Online-Einkäufe nie über ein fremdes WLAN.
- Schalten Sie Bluetooth und WLAN ab, wenn Sie sie nicht benötigen.
- Speichern Sie keine persönlichen Zugangsdaten auf fremden Portalen und geben Sie sie auch nicht an Dritte weiter.
- Merken Sie sich Ihre PIN und Ihr Passwort statt sie aufzuschreiben oder abzuspeichern.
- Achten Sie darauf, dass Sie Online-Geschäfte nur über eine verschlüsselte Verbindung tätigen.
- Geben Sie für Online-Banking oder Einkäufe im Internet die Internetadresse immer von Hand ein.
- Klicken Sie nie auf Links oder Anhänge in E-Mails mit unbekanntem Absender.
- Folgen Sie nie Aufforderungen zur Bestätigung von Zahlungsaufträgen, die Sie per E-Mail oder Telefon erhalten.
- Sichern Sie Ihre Daten regelmäßig und löschen Sie Ihre Daten vollständig, wenn Sie Ihr Gerät verkaufen.

Was sollte ich zu meinem Schutz im Online-Banking beachten?

Bleiben Sie achtsam

Mit der Eingabe der TAN wird im Regelfall eine Abbuchung von Ihrem Konto bestätigt. Denken Sie daran, wenn Sie nach Ihren Bankdaten oder einer TAN gefragt werden, ohne dass Sie eine Transaktion in Auftrag geben wollen.

Seien Sie misstrauisch bei PIN-/TAN-Eingabe

Geben Sie niemals Ihre PIN oder TAN infolge von E-Mails ein. Ihre SaarLB wird Sie niemals auffordern, Ihre Zugangsdaten zu nennen oder eine TAN für Sicherheits-Updates, vermeintliche Rücküberweisungen oder ähnliche Fälle einzugeben.

Prüfen Sie die Daten im TAN-Generator

Auf dem Display Ihres TAN-Generators werden Ihnen die wichtigsten Auftragsdaten angezeigt. Falls die Anzeigedaten nicht mit Ihrem Auftrag übereinstimmen, brechen Sie die Aktion ab.

Achten Sie auf die Adresszeile im Browser

Wenn Sie Ihre Anmeldedaten zum Online-Banking eingeben: Achten Sie auf das geschlossene Schloss-Symbol im Internetbrowser und auf das Kürzel **https://**in der Adresszeile.

Kontrollieren Sie Ihre Kontoumsätze

Kontrollieren Sie regelmäßig und zeitnah Ihre Kontoumsätze via Online-Banking oder Kontoauszüge. Nur so erkennen Sie unberechtigte Abbuchungen rechtzeitig und können fristgerecht reagieren.

Grenzen Sie Ihr Tageslimit ein

Zu Ihrer Sicherheit haben wir Ihr Online-Banking bereits auf das mit Ihnen vereinbarte Standard-Tageslimit begrenzt. Auf Ihre Anfrage setzen wir Ihr persönliches Tageslimit gerne weiter herunter. So sind Sie noch besser vor unberechtigten Zugriffen geschützt.

Sperren Sie im Zweifel Ihren Zugang

Falls Ihnen an der gewohnten Maske Ihres Online-Bankings etwas verdächtig vorkommt, sperren Sie Ihren Zugang. Wenden Sie sich dazu direkt an Ihre SaarLB (Mo-Fr 8:00-12:30, 13:30-16:00, **Tel. +49 681 / 383 - 1597**) oder wählen Sie den 24-Stunden-Sperr-Notruf (**Tel. +49 116 116**). Auch aus dem Ausland ist der Sperr-Notruf erreichbar.

Wie erkenne ich Gefahren aus dem Internet?

Phishing

Phishing bedeutet so viel wie „Passwort-Fischen“. Der Betrüger versucht, Ihnen Ihre Online-Banking-Zugangsdaten zu entlocken. Meist gibt er sich Ihnen gegenüber per E-Mail als SaarLB-Mitarbeiter aus.

Unter einem Vorwand lockt er Sie – z. B. via Internetlink in seiner E-Mail – auf eine gefälschte Internetseite der SaarLB. Sie sieht dem Original verblüffend ähnlich. Sie werden aufgefordert, dort Ihre Zugangsdaten und die TAN einzugeben. Von Ihnen unbemerkt nutzt der Betrüger die gestohlenen Daten, um Geld von Ihrem Konto zu transferieren.

Das Aussehen von falschen E-Mails wirkt oft professionell und integriert die Logos von Geldinstituten oder Online-Shops. Warnhinweise können hier sein:

- kryptische und untypische Absenderadresse
- Rechtschreibfehler im Text bzw. falsche Umlaute oder kyrillische Buchstaben
- falsche Grammatik
- keine namentliche Anrede (z. B. „Lieber Kunde“).

Manche Betrüger melden sich auch per Fax oder Telefon. In jedem Fall gilt: Geben Sie niemals Ihre geheimen Daten preis!

Trojaner

Trojaner sind kleine Spionageprogramme, die das Verhalten Ihres PCs beim Online-Banking verändern. Sie gelangen z. B. via Internetdownloads oder beim Öffnen von E-Mail-Anhängen auf Ihren PC.

Trojaner fragen z. B. über eine gefälschte Abfrageseite direkt nach der Anmeldung TANs von Ihnen ab. Diese TANs fließen dann an die Betrüger, die so unbemerkt z. B. eine Überweisung von Ihrem Konto durchführen.

Eine besonders gefährliche Variante der Gattung Trojaner manipuliert fast unsichtbar die von Ihnen eingegebene Überweisung. Achten Sie daher auf Unstimmigkeiten auf der Seite zur Eingabe der TAN.

Gut zu erkennen sind solche Betrugsversuche daran, dass die Daten nicht mit der Anzeige im TAN-Generator übereinstimmen. Entdecken Sie Unstimmigkeiten, geben Sie keine TAN ein und kontaktieren Sie uns bzw. den Sperr-Notruf bitte sofort (Kontaktdaten unter „Vorgehen im Notfall“).

Gute Virenscanner erkennen die meisten Trojaner. Deshalb sollten Sie Ihren PC regelmäßig mit einem aktuellen Virenscanner überprüfen.

Pharming

Beim Pharming werden Sie unbemerkt auf eine gefälschte Internetseite umgeleitet, die der Originalseite täuschend ähnlich sieht. Ziel des Betrügers ist es, Ihre Kontodaten und PIN auszuspionieren.

Sie erkennen Pharming oft daran, dass die Startseite nicht die typischen Sicherheitsmerkmale aufweist:

- In der Adresszeile fehlt das Kürzel https.
- Eventuell haben Schrift und Symbole andere Farben oder eine andere Größe als sonst.

Achtung: Selbst die Eingabe der SaarLB-Adresse direkt in die Adresszeile des Browsers schützt in diesem Fall nicht vor der Umleitung.

Pharming gelingt jedoch nur, wenn zuvor eine Schadsoftware auf Ihrem Computer installiert wurde, zum Beispiel über Trojaner, die Sie über einen E-Mail-Anhang erhalten haben. Beachten Sie daher auch hier unsere allgemeinen Sicherheitstipps.

Wie kann ich sicher mit der SaarLB kommunizieren?

Nutzen Sie für Ihre Mitteilung an uns bitte keine unverschlüsselte E-Mail. Sie kann im Internet von Dritten mitgelesen werden. Zur sicheren Kommunikation senden Sie uns eine Nachricht über die Internetfiliale unter „Postfach/Nachricht verfassen“.

Bitte beachten Sie: Wichtige Informationen zu

- Veränderungen rund um Ihr Online-Banking
- verwendeten Sicherungsverfahren
- aktuellen Betrugsversuchen
- wie Sie Betrugsversuche erkennen können
- wie Sie Ihren Computer und Internetzugang absichern
- nützlichen Links zum Thema Sicherheit

stellen wir Ihnen immer postalisch oder unter **www.saarlb.de/sicherheitshinweise** bereit.

Jede Nachricht zur korrekten und sicheren Nutzung des SaarLB-Online-Bankings, die Sie im Namen der SaarLB auf anderem Wege erhalten, ist nicht vertrauenswürdig.

Wir werden Sie in solchen Fällen auch nie über E-Mail informieren. Bitte reagieren Sie daher niemals auf Aufträge oder Anfragen per E-Mail, in denen der Eindruck vermittelt wird, dass diese von uns zugestellt worden sind. Öffnen Sie bitte niemals Anhänge, die solchen Mails beigefügt sind!.

Sicherheitshinweise zum Bezahlen mit Ihrer Business Card im Internet

Beim Online-Einkauf bietet die SaarLB-Business Card eine schnelle und sichere Bezahlmöglichkeit. Wir geben Antworten auf die wichtigsten Fragen zum Umgang mit der Business Card und zu den wesentlichen Sicherheitsregeln.

Welche Sicherheit bietet mir die Business Card der SaarLB?

- **Für Ihre Sicherheit:** Verified by Visa ist ein Sicherheits-Service, den Ihre SaarLB mit der Business Card von Visa anbietet. Das innovative Verfahren stellt sicher, dass niemand unberechtigt mit Ihrer Business Card im Internet einkaufen kann. Sie können sich jederzeit einfach und schnell mit Ihrer vorhandenen Business Card von Visa dafür anmelden und sofort alle Vorteile genießen. Sie benötigen keine zusätzliche Software.
- **Schnelle Registrierung:** Voraussetzung ist Ihre Registrierung. Dabei geben Sie Ihr persönliches Kennwort und eine selbst gewählte Sicherheitsmitteilung an. Sie können sich entweder auf der Internetseite der SaarLB (Stichwort „Verified by Visa“) anmelden oder Sie melden sich direkt beim zertifizierten Online-Händler an. Wenn Sie künftig bei zertifizierten Online-Shops einkaufen, werden Zahlungen nur noch mit Ihrem Kennwort ausgeführt. Registrieren Sie sich gleich bei der ersten Aufforderung, um weiter mit Ihrer Business Card einkaufen zu können.

Wie funktioniert die Internetzahlung mit Verified by Visa?

1. Gehen Sie, wie gewohnt, online shoppen, wählen Sie Ihre Artikel aus und starten Sie dann den Bezahlvorgang.
2. Geben Sie bei einem zertifizierten Händler Ihre Kartendaten ein, dann öffnet sich automatisch ein Fenster mit dem Eingabefeld von Verified by Visa.
3. Hier sehen Sie Ihre persönliche Sicherheitsmitteilung. Wenn diese korrekt ist, wissen Sie, dass Ihre SaarLB und niemand sonst nach Ihrem Kennwort fragt. Geben Sie jetzt einfach Ihr Kennwort ein und klicken Sie auf „Bestätigen“.
4. Sie werden nun als rechtmäßiger Karteninhaber identifiziert und Ihre Zahlung wird wie gewohnt veranlasst.

Einfach registrieren und sofort den vollen Schutz genießen.

Sie allein kennen Ihr Kennwort – so kann kein anderer Ihre Business Card missbräuchlich für Online-Käufe verwenden. Registrieren Sie sich am besten direkt.

Was hat es mit der „Kartenprüfnummer“ auf sich?

Der **Card Verification Value (CVV)** ist ein Sicherheitsmerkmal auf Kreditkarten: die Kartenprüfnummer. Die Prüfnummer erschwert die Nutzung von gestohlenen Kreditkartenangaben, da sich feststellen lässt, ob eine Kreditkarte tatsächlich vorliegt. Das aktuell gebräuchliche Format heißt CVV2. Es handelt sich dabei um eine Zahlenkombination, die zusätzlich zur Kreditkartennummer auf der Kreditkarte aufgedruckt ist. Sie ist nicht eingeprägt. Dadurch ist die Prüfnummer nicht maschinenlesbar. Bei Visa (CVV2) sind die Prüfnummern jeweils dreistellig und befinden sich auf der Rückseite der Karte.

Worauf muss ich beim Umgang mit meiner Business Card achten?

Schützen Sie Ihre Karte vor Beschädigungen

- Stecken Sie Ihre Karte nicht lose in die Tasche.
- Bewahren Sie Ihre Karte nicht zusammen mit scharfkantigen Gegenständen auf.
- Setzen Sie Ihre Karte keinen hohen Temperaturen aus (z. B. in einem in der Sonne abgestellten Auto).
- Fragen Sie beim Kundenservice Ihrer SaarLB nach einer Schutzhülle.

Seien Sie wachsam

- Lassen Sie im Handel, beim Tanken, im Hotel oder Restaurant die Karte nicht aus den Augen. Wenn nötig, bestehen Sie darauf, das Personal zu begleiten.

- Kontrollieren Sie die Rechnungsbeträge vor dem Bezahlen genau – im Ausland prüfen Sie bitte immer auch die Abrechnungswährung.
- Stellen Sie sicher, dass niemand die PIN-Eingabe beobachten kann.

Meiden Sie Magnetfelder

Durch magnetische Felder kann der Magnetstreifen auf der Kartenrückseite beschädigt werden. Die Funktion der Karte wird ggf. beeinträchtigt. Halten Sie die Karte von Handys, Fernsehern, Lautsprecherboxen, Magnetverschlüssen an Taschen, Geldbörsen, Bahnklapptischen und Warensicherungsflächen von Verkaufstheken fern.

Schützen Sie Ihr Kennwort

- Schreiben Sie Ihr Kennwort nicht auf und speichern Sie es auch nicht ab.
- Schreiben Sie Ihr Kennwort nicht auf Ihre Karte.
- Achten Sie darauf, dass niemand die Eingabe Ihres Kennworts sieht, beispielsweise in der Öffentlichkeit.
- Seien Sie misstrauisch, wenn jemand Sie nach Ihrem Kennwort fragt. Die SaarLB oder PLUSCARD wird Sie niemals nach Ihrem Kennwort fragen.

Vorgehen im Notfall

Sperren Sie Ihren Online-Banking-Zugang oder Ihre Business Card

Sperren Sie im Zweifelsfall bitte sofort Ihren Online-Banking-Zugang oder Ihre Kreditkarte bei Verlust, Diebstahl oder Verdacht auf Missbrauch: Wenden Sie sich in beiden Fällen dazu direkt an die SaarLB oder wählen Sie den Sperr-Notruf (Kontaktdaten siehe unten). Auch aus dem Ausland ist der Sperr-Notruf erreichbar. Bitte informieren Sie sich vor Reiseantritt über eine möglicherweise abweichende Ländervorwahl (www.sperr-notruf.de).

An wen kann ich mich wenden?

SaarLB-Online-Banking-Hotline
(Mo - Fr: 8.30-12:30 und 13:30-16:00 Uhr)
+49 681 / 383 – 1597

PLUSCARD-Karteninhaber-Service
(täglich, rund um die Uhr)
+49 681 / 93764599

Zentrale Sperr-Hotline für Konto und Karten
(täglich, rund um die Uhr, auch aus dem Ausland)
+49 116 116

Es fallen die mit Ihrem Anbieter vereinbarten Festnetz- bzw. Mobilfunkpreise an. Bei Anrufen aus deutschen Mobilfunknetzen beträgt der Preis maximal 0,42 EUR/min.

saarLB

Landesbank Saar
Ursulinenstraße 2
66111 Saarbrücken

FON +49 681 383-01
FAX +49 681 383-1200

service@saarlb.de
www.saarlb.de

Finanzgruppe