saar LB

Informations et consignes de sécurité

relatives à la banque en ligne de la SaarLB et aux paiements sur internet avec la SaarLB Business Card (carte de crédit)

La banque régionale franco-allemande
Die deutsch-französische Regionalbank

être proche pour voir plus loin

Informations et consignes de sécurité relatives à la banque en ligne de la SaarLB et aux paiements sur internet avec la SaarLB Business Card (carte de crédit)

Version d'octobre 2018

Introduction à la banque en ligne de la SaarLB

La banque en ligne de la SaarLB vous permet d'effectuer vos transactions financières où et quand vous le souhaitez. La présente note vous donne une réponse aux principales questions sur le fonctionnement du système et sur ce que vous devez faire en termes de sécurité. Par ailleurs, nous sommes personnellement à votre disposition pour toute question.

Quels sont les avantages de la banque en ligne ?

- **Rapidité :** quelques clics suffisent pour virer de l'argent, définir des ordres permanents ou vérifier vos relevés de compte. Vous économisez ainsi beaucoup de temps.
- **Simplicité :** l'utilisation intuitive et la présentation claire vous aident à vous orienter. Vous pouvez immédiatement en profiter.
- **Confort :** vous pouvez accéder à votre compte courant lorsque vous en avez le temps, depuis chez vous, depuis votre poste de travail ou lorsque vous êtes en déplacement.
- **Sécurité :** la banque en ligne de la SaarLB fonctionne avec les normes de sécurité les plus rigoureuses. Votre argent est ainsi protégé de manière optimale.

De quoi ai-je besoin pour participer à la banque en ligne ?

- **Compte SaarLB :** si vous un avez un compte courant à la SaarLB, vous pouvez faire valider la banque en ligne à tout moment et gratuitement. Vous recevrez directement votre identifiant de connexion. Le code PIN (numéro d'identification personnel) vous sera envoyé par courrier postal. Vous pouvez alors immédiatement en profiter.
- **BankCard de la SaarLB (carte de débit) :** vous avez besoin d'une BankCard (carte de débit) de la SaarLB pour la banque en ligne. Vous utilisez cette carte pour valider les transactions effectuées en ligne.
- **Ordinateur, smartphone ou tablette :** pour la banque en ligne, vous avez besoin d'un ordinateur ou d'un autre terminal avec accès internet, par exemple d'un smartphone ou d'une tablette. Le Groupe financier des caisses d'épargne allemandes propose des applications pour l'utilisation sur smartphone, par exemple l'application « caisse d'épargne » (des informations plus détaillées figurent dans la rubrique « Puis-je également utiliser la banque en ligne avec mon mobile ? »).
- **Accès internet :** pour que vous puissiez utiliser la banque en ligne, votre terminal doit avoir accès à internet. La vitesse ne joue aucun rôle : la banque en ligne de la SaarLB fonctionne indépendamment de la connexion, que vous disposiez d'un réseau haute vitesse ou que vous surfiez sur votre mobile.
- **Sécurité :** il est judicieux d'installer, et pas seulement pour la banque en ligne, un navigateur internet récent, un logiciel antivirus et un « pare-feu ». Par ailleurs, vous définissez une fois pour toutes le système de sécurité que vous avez choisi pour la banque en ligne (plus d'informations dans la rubrique « Qu'entend-on par système de sécurité de la banque en ligne ? »).
- **Système de sécurité chip TAN :** vous avez besoin d'un « générateur TAN » pour effectuer des transactions via la banque en ligne de la SaarLB. Vous pouvez le commander facilement dans la boutique en ligne des caisses d'épargne allemandes : www.sparkassen-shop.de, menu « Chipkartenleser » (Lecteurs de cartes à puce), « TAN-Generatoren » (Générateurs TAN).
- **Système de sécurité HBCI :** vous avez besoin en plus non pas d'un générateur TAN, mais d'un lecteur de cartes HCBI et d'un logiciel bancaire spécial, par ex. « StarMoney ». Vous pouvez commander le lecteur et le logiciel dans la boutique en ligne des caisses d'épargne allemandes sous la rubrique www.sparkassen-shop.de, menu « Chipkartenleser/Secoder » (Lecteurs de cartes à puce) et « Online-Banking-Software » (Logiciel de banque en ligne).

Qu'entend-on par « système de sécurité de la banque en ligne » ?

Vous consultez le solde de votre compte, des relevés de compte, etc. dans un domaine protégé. Pour ce faire, vous utilisez un identifiant de connexion et un numéro d'identification personnel abrégé PIN.

Parallèlement au code PIN pour l'accès général, vous confirmez chaque transaction avant qu'elle ne soit exécutée pour vous protéger de tout abus. Vous pouvez procéder à cette confirmation de deux manières différentes en fonction du système de sécurité pour lequel vous optez. Vous convenez du système de sécurité avec la SaarLB une seule fois avant la première utilisation.

Quels systèmes de sécurité propose la SaarLB ?

Nous vous proposons deux systèmes de sécurité, chip TAN et HBCI. Ces deux systèmes sont actualisés régulièrement et vous offrent la meilleure protection possible. Le système de sécurité vous convenant le mieux dépend de la manière dont vous utilisez la banque en ligne.

Chip TAN – un système sûr avec carte et générateur TAN

Parallèlement au code PIN pour l'accès général, vous confirmez chaque transaction à l'aide d'un numéro de transaction (TAN). Dans le procédé chip TAN, vous générez vous-même ce TAN à l'aide de votre générateur TAN et de votre carte bancaire SaarLB (carte dedébit).

Avantages de chip TAN :

- Grande sécurité du fait de la validité limitée dans le temps du chip TAN
- Possibilité de contrôler les principales données relatives à l'ordre, affichées sur le générateur
- Abus pratiquement impossible puisque le chip TAN n'est valable que pour un ordre donné
- Vous n'avez pas besoin de code PIN spécial en plus du code PIN de la banque en ligne

- Si vous avez le générateur TAN sous la main, vous pouvez consulter votre compte en ligne depuis tout autre ordinateur (sécurisé)

A qui s'adresse chipTAN :

- Utilisation des fonctions de compte courant principalement en ligne
- Uniquement des comptes en Allemagne
- Opérations bancaires occasionnelles ou moyennement fréquentes

HBCI – la signature numérique

HBCI signifie « Homebanking Computer Interface » et est conçu pour tous ceux qui utilisent intensément la banque en ligne. Pour le système HCBI, vous avez besoin d'un logiciel bancaire spécial et d'un lecteur de carte spécial HCBI.

Avantage du système HBCI :

- Si vous utilisez un logiciel bancaire, vos données sont encore mieux protégées par une technique de cryptage de haut niveau.

A qui s'adresse HBCI :

- Petites et moyennes entreprises
- Particuliers effectuant des opérations bancaires très fréquentes
- Utilisation de la banque en ligne également pour des activités libérales sur le propre ordinateur

Comment utiliser la banque en ligne ?

Nous avons mis au point pour vous un « guide sur la banque en ligne de la SaarLB » comprenant une description détaillée étape par étape, avec des illustrations et du texte, depuis la première connexion jusqu'à la réalisation d'un virement. Vous trouvez ce guide à télécharger directement sous la case de connexion à la banque en ligne sur le site www.saarlb.fr.

Puis-je également utiliser la banque en ligne avec mon mobile ?

Les applications du Groupe financier des caisses d'épargne allemandes vous permettent d'effectuer en tout confort vos opérations bancaires à partir de votre mobile.

Application Caisse d'épargne allemande

Grâce à cette application gratuite, vous pouvez toujours et où que ce soit consulter vos soldes de compte actualisés, envoyer des virements ou payer confortablement vos factures par code QR. Scannez pour ce faire simplement le « code QR » sur votre facture et effectuez votre paiement sans avoir à taper les données relatives au virement. Vous pouvez également laisser l'application vous guider vers le distributeur de billets le plus proche.

Application Caisse d'épargne allemande+

L'application Caisse d'épargne+ vous permet d'ouvrir des comptes dans un nombre quelconque de caisses d'épargne allemandes et de banques. Grâce à l'application, vous voyez vos chiffres d'affaires, pouvez effectuer des virements ou payer des factures sans avoir à entrer les données relatives au virement grâce à la fonction « lire le code QR ».

Indications pour une plus grande sécurité de la banque en ligne

Avant d'utiliser la banque en ligne, prenez quelques minutes pour lire les informations importantes indiquées ci-dessous.

Comment me protéger le mieux possible des cyberattaques ?

- Actualisez régulièrement votre système d'exploitation, votre navigateur internet et les logiciels que vous utilisez.
- Ne travaillez pas avec des droits d'administrateur sur votre ordinateur.
- Mettez régulièrement à jour le pare-feu et le logiciel antivirus.
- Utilisez uniquement des logiciels provenant de sources sûres.
- Déconnectez-vous après avoir utilisé la banque en ligne et effacez l'historique du navigateur et le cache.
- N'effectuez jamais vos opérations bancaires et vos achats en ligne via un Wi-Fi externe.
- Déconnectez Bluetooth et le Wi-Fi lorsque vous n'en avez pas besoin.
- N'enregistrez pas de données d'accès personnelles sur des portails externes et ne les transmettez pas non plus à des tiers.
- Mémorisez votre code PIN et votre mot de passe au lieu de les écrire ou de les enregistrer.
- Veillez à n'effectuer vos opérations en ligne que via une liaison sécurisée.
- Entrez toujours manuellement l'adresse internet pour la banque en ligne ou les achats sur internet.
- Ne cliquez jamais sur des liens ou annexes dans des courriels dont vous ne connaissez pas l'expéditeur.
- Ne donnez jamais suite aux demandes de confirmation d'ordres de paiement que vous recevez par courriel ou téléphone.
- Enregistrez vos données régulièrement et effacez intégralement vos données si vous vendez votre appareil.

A quoi dois-je faire attention pour me protéger lorsque j'utilise la banque en ligne ?

Restez vigilant

L'entrée du numéro TAN confirme généralement un débit de votre compte. Pensez-y lorsque l'on vous demande des données bancaires ou un numéro TAN alors que vous ne souhaitez pas mandater de transaction.

Soyez méfiant lors de l'entrée du code PIN/ numéro TAN
N'indiquez jamais votre code PIN ou le numéro TAN à la suite de courriels. La SaarLB ne vous invitera jamais à indiquer vos données d'accès ou un numéro TAN pour des mises à jour de sécurité, des remboursements présumés ou autres cas similaires.

Vérifiez les données dans le générateur TAN
Les principales données de votre ordre apparaissent sur l'écran de votre générateur TAN. Si les données affichées ne correspondent pas à votre ordre, interrompez l'action en cours.

Faites attention à l'adresse dans le navigateur
Lorsque vous entrez vos données de connexion pour la banque en ligne, veillez à ce que le symbole de cadenas fermé apparaisse dans le navigateur internet et à ce que l'abréviation **https://** figure dans l'adresse.

Contrôlez vos transactions
Contrôlez régulièrement et rapidement vos transactions via la banque en ligne ou vos relevés de compte. C'est pour vous le seul moyen de découvrir des débits illicites et de réagir dans les délais.

Réduisez votre limite journalière
Pour votre sécurité, nous avons déjà fixé votre limite journalière au niveau standard que nous avons convenu avec vous pour la banque en ligne. Si vous le souhaitez, nous réduisons encore plus votre limite journalière personnelle. Vous serez alors encore mieux protégé des attaques illicites.

En cas de doute, bloquez votre accès
Si le masque habituel de votre banque en ligne vous semble suspect, bloquez votre accès. Adressez-vous pour ce faire directement à la SaarLB (du lundi au vendredi de 8h00 à 12h30 et de 13h30 à 16h00, **tél. +49 681 / 383 - 1595**) ou faites le numéro de blocage 24 h sur 24 (**tél. +49 116 116**). Vous pouvez également appeler le numéro de blocage depuis l'étranger.

Comment identifier les dangers provenant de l'internet ?

Hameçonnage (phishing)

Hameçonner, c'est un peu comme « pêcher des mots de passe ». Le fraudeur essaie de vous soutirer vos données d'accès à la banque en ligne. Le plus souvent, il se fait passer pour un collaborateur de la SaarLB dans le courriel qu'il vous adresse.

Sous un prétexte donné, il vous attire, par ex. via un lien internet dans son courriel, sur un site web falsifié de la SaarLB. Ce site ressemble à s'y méprendre à l'original. Vous êtes invité à entrer vos données d'accès et le numéro TAN. Sans que vous le remarquiez, le fraudeur utilise les données volées pour transférer de l'argent depuis votre compte.

L'aspect de courriels faux est souvent professionnel et intègre les logos d'établissements bancaires ou de boutiques en ligne. Certains indices devraient vous rendre méfiant :

- Adresse cryptique ou atypique de l'expéditeur
- Fautes d'orthographe dans le texte, trémas incorrects ou lettres cyrilliques
- Grammaire incorrecte
- Formule de politesse impersonnelle (par ex. « Cher client »).

Certains fraudeurs prennent également contact par fax ou téléphone. Quelle que soit la méthode utilisée : ne dévoilez jamais vos données confidentielles !

Cheval de Troie

Les chevaux de Troie sont de petits logiciels espions malveillants qui modifient le comportement de votre ordinateur lors de vos opérations bancaires en ligne. Ils parviennent sur votre ordinateur par ex. via des téléchargements à partir d'internet ou lorsque vous ouvrez des annexes à des messages électroniques.

Via un site falsifié par ex., les chevaux de Troie vous demandent des numéros TAN dès que vous vous êtes connecté. Ces numéros TAN sont communiqués aux fraudeurs qui, sans que vous le remarquiez, font par ex. un virement depuis votre compte.

Une variante de cheval de Troie particulièrement dangereuse manipule de manière pratiquement invisible le virement que vous avez entré. Faites donc attention aux anomalies sur la page d'entrée des numéros TAN.

Vous pouvez facilement identifier de telles tentatives de fraude au fait que les données ne correspondent pas à l'affichage sur le générateur TAN. Si vous découvrez des anomalies, ne communiquez pas de numéro TAN et contactez-nous ou le numéro de blocage sans délai (coordonnées au point « procédure à suivre en cas d'urgence »).

Les logiciels antivirus performants reconnaissent la plupart des chevaux de Troie. Une raison de plus pour que vous vérifiez régulièrement votre ordinateur avec un logiciel antivirus récent.

Dévoiement (pharming)

Dans le cas du dévoiement, vous êtes redirigé, sans que vous le remarquiez, vers un site web falsifié qui ressemble à s'y méprendre au site original. Le fraudeur a pour objectif d'espionner vos données bancaires et votre code PIN.

Vous reconnaissez souvent le dévoiement au fait que la page d'accueil n'affiche pas les caractéristiques de sécurité typiques :

- L'abréviation https manque dans l'adresse
- Les caractères et les symboles peuvent avoir une couleur ou une taille autres qu'habituellement

Attention : même l'entrée directe de l'adresse de la SaarLB dans la ligne réservée à l'adresse n'empêche pas que vous soyez redirigé vers un autre site.

Cependant, le dévoiement ne peut avoir de succès que si un logiciel malveillant a été installé auparavant sur votre ordinateur, par exemple via des chevaux de Troie que vous avez reçus dans une annexe jointe à un courriel. Veuillez donc respecter ici nos consignes de sécurité générales.

Comment puis-je communiquer avec la SaarLB avec la fiabilité requise ?

N'utilisez jamais de courriel non sécurisé pour nous envoyer un message. Ce courriel peut être lu par des tiers sur internet. Pour communiquer avec nous avec la fiabilité requise, veuillez nous envoyer un message via la filiale internet à la rubrique « Boîte postale/rédiger un message ».

Veuillez prendre acte de ce que suit : nous tenons à votre disposition, soit par voie postale soit sur le site **www.saarlb.de/sicherheitshinweise**, des informations importantes sur

- les modifications portant sur votre banque en ligne
- les méthodes de sécurisation utilisées
- les tentatives de fraude actuelles
- la manière d'identifier des tentatives de fraude
- la manière dont vous pouvez protéger votre ordinateur et votre accès internet
- des liens utiles sur le thème de la sécurité.

Toute communication sur l'utilisation correcte et sûre de la banque en ligne de la SaarLB, que vous recevez par une autre voie au nom de la SaarLB, n'est pas digne de confiance.

Dans de tels cas, nous ne vous informerons jamais par courriel. Ne réagissez donc jamais à des ordres ou demandes par courriel dont on a l'impression que nous les avons envoyés. N'ouvrez jamais les annexes jointes à de tels courriels.

Consignes de sécurité à respecter lorsque vous payez sur internet à l'aide de votre Business Card.

Lorsque vous faites des achats en ligne, la Business Card de la SaarLB est une méthode de paiement rapide et sûre. Nous répondons ci-dessous aux principales questions posées sur l'utilisation de la Business Card et sur les principales règles de sécurité.

Quelle est la sécurité que m'offre la Business Card de la SaarLB ?

- **Pour votre sécurité :** Verified by Visa est un service sécurisé que vous propose la SaarLB avec la Business Card de Visa. Le système innovant garantit que personne ne puisse faire des achats sur internet avec votre Business Card. Vous pouvez vous inscrire à tout moment, simplement et rapidement, avec votre Business Card de Visa et bénéficier immédiatement de tous les avantages. Vous n'avez pas besoin de logiciel supplémentaire.
- **Enregistrement rapide :** vous devez pour ce faire vous enregistrer. Indiquez votre mot de passe personnel et un message de sécurité que vous aurez choisi vous-même. Vous pouvez soit vous inscrire sur le site web de la SaarLB (mot clé « Verified by VISA ») soit vous inscrire directement chez le commerçant en ligne certifié. Lorsqu'à l'avenir vous ferez des achats dans des boutiques en ligne certifiées, les paiements se feront uniquement avec votre mot de passe. Enregistrez-vous dès la première demande pour continuer à faire vos achats avec la Business Card.

Comment fonctionne le paiement sur internet avec Verified by Visa ?

1. Faites vos achats comme d'habitude en ligne, choisissez vos articles et lancez la procédure de paiement.
2. Si vous entrez vos informations bancaires chez un commerçant certifié, une fenêtre avec le champ de saisie de Verified by Visa s'ouvre automatiquement.
3. Vous voyez ici votre message de sécurité. S'il est correct, vous savez que la SaarLB et personne d'autre vous demande votre mot de passe. Entrez votre mot de passe et cliquez sur « confirmer ».
4. Vous êtes identifié comme titulaire légitime de la carte et votre paiement est effectué comme d'habitude.

Enregistrez-vous et bénéficiez immédiatement d'une sécurité totale.

Vous seul connaissez votre mot de passe – ainsi, personne d'autre ne peut abuser de votre Business Card pour faire des achats en ligne. Enregistrez-vous dès que possible !

Qu'entend-on au juste par « cryptogramme » ?

Le système **Card Verification Value (CVV)** est une caractéristique de sécurité sur les cartes de crédit : le cryptogramme. Le cryptogramme rend plus difficile l'utilisation de données bancaires volées car il est possible de constater si une carte de crédit existe réellement. Le format usuel s'appelle CVV2. Il s'agit d'une

combinaison de chiffres imprimée sur la carte de crédit en plus du numéro de la carte de crédit. Elle n'est pas mise en relief. De ce fait, le cryptogramme ne peut pas être lu par une machine. Chez Visa (CVV2), les cryptogrammes se composent de trois chiffres et se trouvent au verso de la carte.

À quoi dois-je faire attention lorsque je manipule ma carte ?

Protégez votre carte de tout endommagement

- Ne mettez pas la carte dans votre poche sans protection.
- Ne conservez pas votre carte avec des objets tranchants.
- N'exposez pas votre carte à des températures élevées (par ex. dans une voiture placée en plein soleil).
- Demandez un étui de protection au service clientèle de la SaarLB.

Soyez vigilant

- Ne quittez pas votre carte des yeux lorsque vous payez dans un magasin, à la station service, à l'hôtel ou au restaurant. Si nécessaire, insistez pour accompagner le personnel.
- Contrôlez minutieusement les montants facturés avant de payer – à l'étranger, contrôlez également toujours la devise dans laquelle est facturé le montant.
- Faites en sorte que personne ne puisse vous espionner lorsque vous entrez votre code PIN.

Evitez les champs magnétiques

Les champs magnétiques peuvent endommager la bande magnétique au verso de la carte. La fonction de la carte est alors éventuellement perturbée. Eloignez la carte de téléphones mobiles, de postes de télévision, d'enceintes, de fermetures magnétiques sur des sacs, porte-monnaie, de tablettes rabattables dans les trains et des surfaces de sécurisation des marchandises sur les comptoirs de vente.

Protégez votre mot de passe

- Ne notez ou n'enregistrez pas votre mot de passe.
- N'inscrivez pas votre mot de passe sur votre carte.
- Veillez à ce que personne ne puisse vous espionner lorsque vous entrez votre mot de passe, par exemple en public.
- Soyez méfiant lorsque quelqu'un vous demande votre mot de passe. La SaarLB ou PLUSCARD ne vous demandera jamais votre mot de passe.

Procédure à suivre en cas d'urgence

Bloquez votre accès à la banque en ligne ou votre Business Card

En cas de doute, veuillez bloquer immédiatement votre accès à la banque en ligne ou votre carte de crédit si vous l'avez perdue, si elle vous a été volée ou si vous pensez qu'il y a eu abus de votre carte : dans ces trois cas, adressez-vous directement à la SaarLB ou faites le numéro de blocage (coordonnées, voir ci-contre). Le numéro de blocage peut également être joint depuis l'étranger. Veuillez vous informer avant de partir de l'indicatif « pays » éventuellement divergent (www.sperr-notruf.de).

À qui puis-je m'adresser ?

Hotline Banque en ligne de la SaarLB
(du lundi au vendredi de 8h30 à 12h30 et de 13h30 à 16h00)
+49 681 / 383 – 1595

Service PLUSCARD pour les titulaires de cartes
(tous les jours, 24 h sur 24)
+49 681 / 93764599

Hotline centrale de blocage pour comptes et cartes
(tous les jours, 24 h sur 24, également depuis l'étranger)
+49 116 116

Ce service est proposé au prix sur réseau fixe et/ou au prix depuis des téléphones mobiles convenus avec votre prestataire. Pour les appels effectués à partir des réseaux allemands de téléphonie mobile, le prix s'élève à 0,42 euro/minute au maximum.

saarLB

Landesbank Saar
Ursulinenstraße 2
66111 Saarbrücken

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

service@saarlb.de
www.saarlb.de

Finanzgruppe