Informations et consignes de sécurité

concernant la banque en ligne SaarLB
et les paiements sur Internet avec la
carte de crédit SaarLB et
la SaarLB BusinessCard (carte de crédit)

WEITSICHT DURCH NÄHE

Die deutsch-französische Regionalbank
La banque régionale franco-allemande

Banque en ligne – quand et où vous le souhaitez

Introduction à la banque en ligne de la SaarLB

Grâce à la banque en ligne de la SaarLB, vous pouvez effectuer vos transactions financières quand et où vous le souhaitez. Dans ce relevé, nous souhaitons vous apporter des réponses aux principales questions, à la manière dont fonctionne la banque en ligne et à ce que vous devez faire pour garantir votre sécurité. Nous sommes bien entendu à votre disposition pour toute question dépassant ce cadre.

Quels sont les avantages que m'offre la banque en ligne ?

Rapide : quelques clics suffisent pour virer de l'argent, enregistrer des ordres permanents ou contrôler des relevés de compte. Vous gagnez ainsi beaucoup de temps.

Simple : l'utilisation intuitive et la structure claire vous aident à mieux vous orienter. Vous pouvez commencer directement.

Confortable : vous pouvez accéder à votre compte courant lorsque votre emploi de temps vous le permet, depuis votre domicile, depuis votre bureau ou lorsque vous êtes en déplacement.

Sûre : 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 avez un compte courant à la SaarLB, vous pouvez à tout moment faire valider gratuitement la banque en ligne. Vous recevrez immédiatement votre nom d'utilisateur. Le code PIN (numéro d'identification personnel) vous est envoyé par la poste. Dès que vous le recevez, vous pouvez démarrer directement.

Banque en ligne – rapide, simple, sûre et confortable

SaarLB-BankCard (carte de débit) : pour la banque en ligne, vous avez besoin d'une SaarLB-BankCard (carte de débit). Vous utilisez cette carte pour valider des transactions dans la banque 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 un smartphone ou une tablette. Si vous souhaitez utiliser un smartphone, le Groupe financier des caisses d'épargne propose ses propres applis, par exemple l'appli « Sparkasse » (vous trouverez des informations plus détaillées dans la rubrique « Puis-je également utiliser la banque en ligne pour le paiement mobile ? »).

Accès Internet : pour que vous puissiez utiliser la banque en ligne, votre terminal doit disposer d'une connexion à l'Internet. La vitesse ne joue pas de rôle déterminant ici. La banque en ligne de la SaarLB fonctionne, que vous naviguiez sur un réseau câblé haut débit ou avec votre mobile.

Sécurité : l'installation d'un navigateur Internet actuel, d'un logiciel antivirus et d'un « pare-feu » est judicieuse, pas seulement pour la banque en ligne. Parallèlement, vous enregistrez, dans le cadre d'une opération que vous n'aurez à faire qu'une seule fois, la procédure de sécurité que vous avez choisie pour la banque en ligne (vous trouverez des informations plus détaillées dans la rubrique « Qu'entend-on par procédure de sécurité dans la banque en ligne ? »).

Procédure de sécurité chipTAN : pour effectuer des transactions dans la banque en ligne de la SaarLB, vous avez besoin en plus d'un « générateur TAN ». Vous pouvez le commander aisément dans la boutique Online-Sparkassen.

La sécurité de votre patrimoine est notre priorité absolue.

Qu’entend-on par « procédure de sécurité dans la banque en ligne » ?

Vous consultez votre compte, vos relevés de compte, etc. dans un espace sécurisé. Vous utilisez pour cela votre nom d’utilisateur et votre numéro d’identification personnel, abrégé PIN.

En plus du code PIN pour l’accès général, vous confirmez chaque transaction avant de l’effectuer, pour vous protéger de tout abus. Vous pouvez procéder à cette confirmation de deux manières différentes, en fonction de la procédure de sécurité que vous choisissez. Vous convenez de la procédure de sécurité avec la SaarLB une fois avant la première utilisation.

Quelle procédure de sécurité propose la SaarLB ?

Avec chipTAN, nous vous proposons un système de sécurité qui est toujours à jour et vous offre la meilleure protection possible.

Avec chipTAN, nous vous offrons la meilleure protection possible.

ChipTAN – une procédure sûre avec carte et générateur TAN

En plus du code PIN pour l'accès général, vous confirmez chaque transaction par un numéro de transaction (TAN). Dans la procédure chipTAN, vous générez vous-même ce numéro TAN à l'aide de votre générateur TAN et de votre SaaarLB-BankCard (carte de débit).

Les avantages de chipTAN :

- grande protection grâce à la validité limitée dans le temps du chipTAN
- possibilité de contrôle par l'affichage des principales données de l'ordre
- pratiquement aucun abus possible car le chipTAN n'est valable que pour un ordre spécial
- pas de code PIN supplémentaire, outre le PIN pour la banque en ligne
- si vous avez le générateur TAN à proximité, vous avez accès à votre compte en ligne depuis tout autre ordinateur (sécurisé)

À qui s'adresse chipTAN :

- utilisation des fonctions du compte courant principalement en ligne
- uniquement des comptes en Allemagne
- transactions bancaires occasionnelles ou moyennement fréquentes

Vous êtes informé toujours et partout de vos comptes

Comment utiliser la banque en ligne ?

Nous avons établi pour vous une instruction détaillée (images et textes) étape par étape depuis la première connexion jusqu'à la réalisation d'un virement sur une propre page web www.saarlb.de/banking.

Puis-je également utiliser la banque en ligne pour le paiement mobile ?

Avec l'appli du groupe financier des caisses d'épargne, vous pouvez également effectuer aisément vos opérations bancaires à partir d'un mobile.

Appli Sparkasse

Grâce à cette appli gratuite, vous pouvez toujours et partout consulter votre compte, envoyer des virements ou payer aisément vos factures par Girocode. Scanner simplement le « code QR » sur votre facture et payer – sans avoir à taper fastidieusement les données relatives au virement. Ou encore : laissez l'appli vous guider vers le distributeur de billets le plus proche.

Ce que vous pouvez faire pour votre sécurité

Informations pour une plus grande sécurité dans la banque en ligne

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

Comment puis-je me protéger le mieux possible des cyber-attaques ?

- 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.
- Actualisez régulièrement le pare-feu et le scanner antivirus.
- N'utilisez que des logiciels provenant de sources fiables.
- Déconnectez-vous après avoir effectué vos opérations bancaires en ligne et effacez l'historique du navigateur et la mémoire cache.
- N'accomplissez vos opérations bancaires et achats en ligne jamais via un WiFi externe.
- Désactivez Bluetooth et WiFi 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 sur un bout de papier ou de les enregistrer.
- Veillez à n'effectuer vos opérations en ligne que via une connexion cryptée.
- Pour vos opérations bancaires en ligne ou lorsque vous faites des achats sur Internet, introduisez toujours l'adresse Internet manuellement.
- Ne cliquez jamais sur des liens ou sur des annexes dans des messages électroniques lorsque vous ne connaissez pas l'expéditeur.
- Ne suivez jamais les invitations à confirmer des ordres de paiement que vous avez reçues par message électronique ou par téléphone.
- Sauvegardez vos données régulièrement et effacez vos données complètement lorsque vous vendez votre appareil.

Ce que vous pouvez faire pour votre sécurité

À quoi dois-je faire attention dans la banque en ligne pour ma propre protection ?

Restez vigilant

En entrant le numéro TAN, vous confirmez en général un débit de votre compte. Pensez-y si l'on vous demande vos données bancaires ou un numéro TAN alors que vous ne voulez pas mandater de transaction.

Soyez méfiant lorsque vous entrez un code PIN/un numéro TAN

N'entrez jamais votre code PIN ou un numéro TAN à la suite de messages électroniques. Votre SaarLB ne vous demandera jamais d'indiquer vos données d'accès ou un numéro TAN pour des mises à jour de sécurité, de prétendus reversements ou des cas similaires.

Vérifiez les données affichées sur le générateur TAN

Les principales données de l'ordre sont affichées sur l'écran de votre générateur TAN. Si les données affichées ne correspondent pas à votre ordre, interrompez l'action.

Faites attention à la barre adresse du 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 l'abréviation https:// dans la barre adresse.

Ce que vous pouvez faire pour votre sécurité

Contrôlez vos transactions

Contrôlez régulièrement et rapidement vos transactions via la banque en ligne ou des relevés de compte. Ce n'est qu'ainsi que vous pourrez découvrir à temps des prélèvements non autorisés et réagir dans les délais requis.

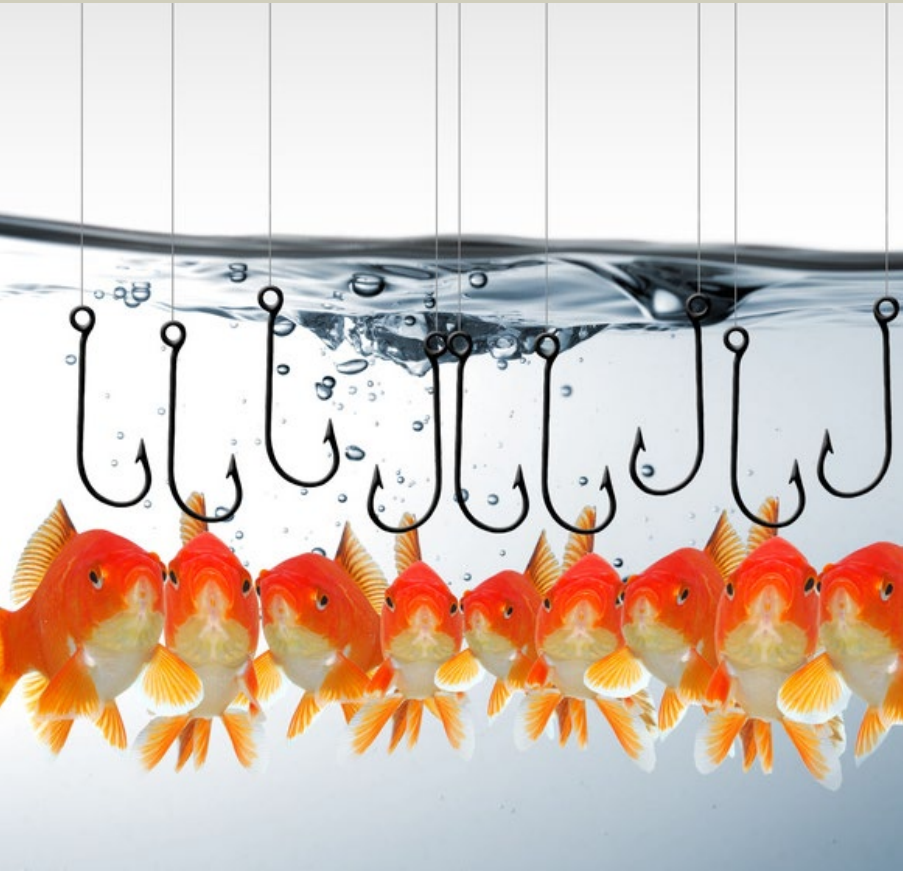
Rabaissez votre limite journalière

Pour votre sécurité, nous avons déjà rabaissé votre banque en ligne à la limite journalière standard dont nous avons convenu. Si vous le souhaitez, nous rabaisserons plus encore votre limite journalière personnelle. Vous serez ainsi encore mieux protégé contre tout accès non autorisé.

Bloquez votre accès en cas de doute

Si l'aspect habituel de votre banque en ligne vous semble suspect, n'hésitez pas à bloquer votre accès. Pour ce faire, adressez-vous directement à votre SaarLB (du lundi au vendredi de 8h00 à 12h30 et de 13h30 à 16h00, tél. +49 681 383-3300) ou composez le numéro d'urgence 24/24 pour blocage de comptes (tél. +49 116 116) Le numéro d'urgence de blocage est également joignable depuis l'étranger.

Voici comment vous protéger de l’hameçonnage, des chevaux de Troie et du dévoiement



Comment reconnaître les dangers que présente l’Internet ?

Ph Hameçonnage (Phishing)

Le mot anglais Phishing signifie à peu près « aller à la pêche aux mots de passe ». Le fraudeur essaie de vous amener à divulguer vos données d’accès à la banque en ligne. Le plus souvent, il se fait passer pour un collaborateur de la SaarLB par message électronique.

Sous un prétexte quelconque, il vous attire – p. ex. via un lien internet dans son message électronique – sur un site internet falsifié de la SaarLB. Ce site falsifié ressemble à s’y méprendre à l’original. Il vous invite à indiquer vos données d’accès et le numéro TAN. À votre insu, le fraudeur utilise les données volées pour transférer de l’argent depuis votre compte.

L’aspect de faux messages électroniques est souvent professionnel et intègre les logos d’instituts bancaires ou de boutiques en ligne. Des avertissements peuvent se présenter comme suit :

- adresse cryptique et atypique de l’expéditeur
- fautes d’orthographe dans le texte et trémas incorrects ou caractères cyrilliques
- erreurs de grammaire
- pas de mention du nom (p. ex. « cher client »).

Certains fraudeurs prennent également contact par fax ou par téléphone. Conduite à adopter en tout cas : **ne dévoilez jamais vos données secrètes !**

Chevaux de Troie

Les chevaux de Troie sont de petits logiciels espions qui modifient le comportement de votre ordinateur dans le cadre de la banque en ligne. Ils parviennent sur votre ordinateur p. ex. via des sites de téléchargement ou si vous ouvrez des annexes dans des messages électroniques.

Dès que vous vous êtes connecté, les chevaux de Troie vous demandent les numéros TAN, p. ex. via une page falsifiée. Les fraudeurs récupèrent alors ces numéros TAN qui, à votre insu, effectuent p. ex. un virement depuis votre compte.

Voici comment vous protéger de l’hameçonnage, des chevaux de Troie et du dévoiement

Une variante particulièrement dangereuse du genre Chevaux de Troie manipule de manière presque invisible le virement que vous introduisez. Faites donc attention aux incohérences ou anomalies sur la page dans laquelle vous entrez les numéros TAN.

De telles tentatives d’escroquerie sont relativement faciles à reconnaître car les données ne sont pas conformes à celles affichées sur le générateur TAN. Si vous découvrez des anomalies, abstenez-vous d’entrer un numéro TAN et contactez-nous ou appelez immédiatement le numéro d’urgence pour blocage du compte (coordonnées sous la rubrique « Procédure à suivre en cas d’urgence »).

Les programmes antivirus de bonne qualité reconnaissent la plupart des chevaux de Troie. N’oubliez donc pas de contrôler régulièrement votre ordinateur à l’aide d’un antivirus actuel.

Dévoiement (Pharming)

Dans le cas du dévoiement, vous êtes redirigé à votre insu vers un site internet falsifié qui ressemble à s’y méprendre à l’original. Le fraudeur a pour objectif d’espionner les données relatives aux comptes et les codes PIN.

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

- il manque l’abréviation https dans la barre adresse.
- Les polices de caractères et les symboles ont éventuellement une autre couleur ou une autre taille qu’à l’habitude.

Attention : dans ce cas, même le fait d’entrer l’adresse de la SaarLB directement dans la barre adresse du navigateur ne vous protège pas du dévoiement.

Toutefois, le dévoiement ne peut avoir de succès que si un logiciel malveillant a été installé auparavant sur votre ordinateur, p. ex. via des chevaux de Troie que vous avez reçus via une annexe dans un message électronique. Veuillez donc tenir compte ici aussi de nos conseils généraux de sécurité.

Comment communiquer en toute sécurité

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

N’utilisez pas de message électronique non crypté pour nous communiquer des informations. Il peut être lu par des tiers sur internet. Pour une communication sûre, veuillez nous envoyer un message via la filiale internet sous la rubrique « Boîte postale/rédiger un message ». Dans de tels cas, nous ne vous informerons jamais par message électronique. Ne réagissez donc jamais à des ordres ou demandes par courrier électronique donnant l’impression que nous vous les avons envoyés. N’ouvrez jamais les annexes jointes à de tels messages électroniques !

Achat sûr en ligne.
Code 3D-Secure

Consignes de sécurité pour le paiement avec votre carte de crédit SaarLB / SaarLB BusinessCard (carte de crédit) sur internet

Pour les achats en ligne, la carte de crédit de la SaarLB / la SaarLB BusinessCard (carte de crédit) offre un moyen de paiement rapide et sûr. Nous répondons aux principales questions sur la manière d'utiliser la carte de crédit et sur les principales règles de sécurité.

Quelle sécurité m'offre la carte de crédit de la SaarLB ?

- **Pour votre sécurité :** le Code 3D-Secure est un service sécurisé que vous propose la SaarLB avec les cartes de crédit de MasterCard et de Visa. La procédure innovante garantit que personne ne puisse faire des achats sur Internet avec votre carte de crédit sans y être autorisé. Vous pouvez vous enregistrer simplement et rapidement, lorsque vous le souhaitez, avec la carte de crédit de MasterCard ou de Visa que vous possédez et bénéficier immédiatement de tous les avantages. Vous n'avez pas besoin de logiciel supplémentaire

Enregistrement rapide : votre enregistrement est une condition indispensable. Dans ce cadre, vous indiquez votre mot de passe personnel et un message de sécurité que vous aurez choisi vous-même. Vous pouvez soit vous enregistrer sur le site Internet de la SaarLB à l'adresse www. Saarlb.de soit directement après du commerçant en ligne certifié. Si, à l'avenir, vous faites des achats dans des boutiques en ligne certifiées, les paiements ne seront plus effectués qu'avec votre mot de passe. Enregistrez-vous dès que vous y serez invité pour la première fois pour pouvoir continuer à faire des achats avec votre carte de crédit.

Achat sûr en ligne.
Code 3D-Secure

Comment fonctionne le paiement sur internet avec le Code 3D-Secure ?

1. Faites vos achats en ligne, comme d'habitude, choisissez vos articles et lancez ensuite l'opération de paiement.

2. Si vous entrez les données de votre carte chez un commerçant certifié, une fenêtre s'ouvre automatiquement avec le champ d'entrée Code 3D-Secure.

3. Votre message de sécurité personnel s'affiche. S'il est correct, vous savez que la SaarLB, et personne d'autre, demande votre mot de passe. Introduisez simplement votre mot de passe et cliquez sur « Confirmer ».

4. Vous êtes alors identifié comme détenteur légal de la carte et votre paiement est effectué comme d'habitude.

Enregistrez-vous simplement et bénéficiez immédiatement d'une protection intégrale.

Vous seul connaissez votre mot de passe – ainsi, personne d'autre ne peut utiliser abusivement votre carte de crédit pour faire des achats en ligne.

Enregistrez-vous dès à présent pour le S-ID-Check. Une fois inscrit, vous profitez d'une procédure particulièrement sûre et pouvez à l'avenir également effectuer vos paiements en ligne avec rapidité et simplicité.

www.s-id-check.de

Vigilance lorsque vous utilisez la carte de crédit

Qu’en est-il du « cryptogramme »?

Le Card Validation Code (CVC) ou Card Verification Value (CVV) est une caractéristique de sécurité sur les cartes de crédit : le cryptogramme. Le cryptogramme complique l’utilisation de données volées relatives à la carte de crédit, car il est possible de constater si une carte de crédit existe réellement. Le format usuel actuellement est

CVC2 et/ou CVV2. Il s’agit d’une combinaison de chiffres qui est imprimée sur la carte de crédit en plus du numéro de la carte de crédit. Elle n’est pas gravée. De ce fait, le cryptogramme n’est pas lisible par machine. Sur la MasterCard (CVC2) et la Visa (CVV2), les cryptogrammes se composent toujours de trois chiffres et se trouvent au verso de la carte.

À quoi dois-je veiller lorsque j’utilise ma carte de crédit ?

Protégez votre carte de tout endommagement

- Ne mettez pas votre carte sans protection dans votre poche.
- Ne conservez pas votre carte avec des objets pointus ou tranchants.
- N’exposez pas votre carte à des températures élevées (p. ex. dans une voiture garée en plein soleil).
- Utilisez un étui rigide pour votre carte.

Soyez vigilant

- Ne quittez pas votre carte des yeux lorsque vous faites des achats, prenez du carburant, à l’hôtel ou au restaurant. Si ceci s’avère nécessaire, insistez pour accompagner le personnel.
- Contrôlez exactement le montant de la facture avant de payer – à l’étranger, contrôlez également toujours la devise de règlement.
- Assurez-vous que personne ne peut vous observer lorsque vous entrez le code PIN.

Conseils en cas d’urgence

Évitez les champs magnétiques

Les champs magnétiques peuvent endommager la piste magnétique qui se trouve au verso de la carte. La fonction de la carte est éventuellement altérée. Tenez la carte éloignée de mobiles, de postes de télévision, d’enceintes, de fermetures magnétiques sur des sacs, de porte-monnaie, de tablettes rabattables dans les trains et de surfaces de sécurisation des marchandises sur les comptoirs.

Protégez votre mot de passe

- N’écrivez pas votre mot de passe sur une feuille de papier et ne l’enregistrez pas.
- N’inscrivez pas le mot de passe sur votre carte.
- Veillez à ce que personne ne voit l’entrée de votre mot de passe, par exemple dans un lieu public.
- Faites preuve de méfiance lorsque l’on 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 carte de crédit

En cas de doute, veuillez bloquer immédiatement votre accès à la banque en ligne ou votre carte de crédit en cas de perte, de vol ou de suspicion d’abus : dans les deux cas, adressez-vous directement à la SaarLB ou composez le numéro d’urgence de blocage (pour les coordonnées, voir ci-dessous). Le numéro d’urgence de blocage est également joignable depuis l’étranger. Veuillez vous informer avant de voyager si le code du pays est éventuellement différent (www.sperr-notruf.de).

Vos correspondants en cas d’urgence

À qui puis-je m’adresser ?

SaarLB-Online-Banking-Hotline
(du lundi au vendredi de 8h30 à 12h30 et de 13h30 à 16h00)
+49 681 383-3300

PLUSCARD-Karteninhaber-Service
(tous les jours, 24 heures sur 24)
+49 681 93764599

Zentrale Sperr-Hotline für Konto und Karten (numéro central de blocage de comptes et cartes)
(tous les jours, 24 heures sur 24, également depuis l’étranger)
+49 116 116

Les prix sont ceux convenus avec votre opérateur pour le réseau fixe et le réseau de téléphonie mobile. Pour les appels effectués à partir de réseaux allemands de téléphonie mobile, le prix s’élève au plus à 0,42 euro/min.