SOCIETE GENERALE
CALEDONIENNE DE BANQUE

RECOMMANDATIONS DE SECURITE - Internet Bancaire

Bonnes pratiques

La sécurité informatique désigne un ensemble de techniques et de bonnes pratiques pour protéger vos ordinateurs et vos intérêts dans l'usage des moyens informatique, tel que le service de banque en ligne Société Générale. Si les techniques et les bonnes pratiques sont élaborées par des spécialistes en sécurité informatique, vous devez connaitre et mettre en œuvre les plus simples.

- **Protéger son mot de passe**

Le mot de passe est une protection importante pour réaliser des transactions en ligne en toute sécurité. Néanmoins, pour assurer une protection optimale, le mot de passe doit respecter les bonnes pratiques listées ci-dessous.

  - Choix du mot de passe : le mot de passe de 6 chiffres est destiné à être saisi dans le clavier virtuel. Choisir un mot de passe « fort » protège des tentatives d'usurpation, ce mot de passe ne doit pas être trivial (répétition de chiffres ou suites de chiffres) et ne doit pas être facilement devinable par un tiers (date d'anniversaire).
  - Utilisation du mot de passe : n'entrez votre code que sur le clavier virtuel de l'espace d'accès sécurisé à votre banque en ligne à l'adresse suivante : https://www.sgcb.nc

Ne communiquez jamais votre mot de passe à qui que ce soit.
Nous vous rappelons que Société Générale ne vous réclamera jamais votre mot de passe.

- **Clore la session en fin de consultation :**

L'authentification sur le service de banque en ligne initie une session de consultation de votre espace client. La session permet de naviguer entre les pages et d'effectuer certaines opérations sans devoir vous authentifiez de nouveau. Bien que pratique, cette fonctionnalité peut permettre à un utilisateur de votre ordinateur de naviguer et d'effectuer certaines opérations à votre insu sur votre espace client.

Il est impératif de clore votre session en fin de consultation via le bouton de « déconnexion », fermer la page ou le navigateur est insuffisant.
Nous vous rappelons que toute opération effectuée à votre nom par le biais de votre session ne pourra être répudiée.

- **Désactiver la fonction de saisie semi-automatique du navigateur :**

La plupart des navigateurs internet proposent d'enregistrer les identifiants et les mots de passe utilisés dans les formulaires d'authentification, y compris votre identifiant de connexion au service de banque en ligne. La fonctionnalité de saisie semi-automatique de l'identifiant permet d'accéder ultérieurement à votre espace client sans avoir à entrer votre identifiant de nouveau. Bien que pratique, la saisie semi-automatique de l'identifiant peut aider un utilisateur de votre ordinateur à ouvrir à votre insu une session de consultation de votre espace client.

Il est impératif de désactiver la fonctionnalité d'auto-complétion du navigateur.
Nous vous rappelons que toute opération effectuée à votre nom par le biais de votre session ne pourra être répudiée.

- **Sécuriser son ordinateur :**

Avant de naviguer sur Internet, vous devez protéger votre ordinateur d'éventuelles attaques malveillantes. Pour cela vous devez suivre les instructions suivantes :

- Mettre à jour son système d'exploitation et ses logiciels : maintenir à jour son système d'exploitation et ses logiciels* est primordial pour se prémunir d'attaques malveillantes. En effet, combler les failles de sécurité connues rend inopérantes les techniques d'attaque les plus courantes.
- Installer un antivirus : un antivirus, même gratuit, doit être installé sur votre ordinateur. Ce logiciel vous protège en identifiant et en bloquant les applications malveillantes installées sur votre ordinateur. De plus, un antivirus vérifie la fiabilité des fichiers que vous téléchargez sur Internet ou que vous recevez par e-mail. Veillez également à maintenir votre solution antivirale à jour.

** en priorité sont à mettre à jour les logiciels accédant à Internet (navigateur, messagerie, …) et les logiciels a forte notoriété (pack Office, suite Adobe, Java, …)*

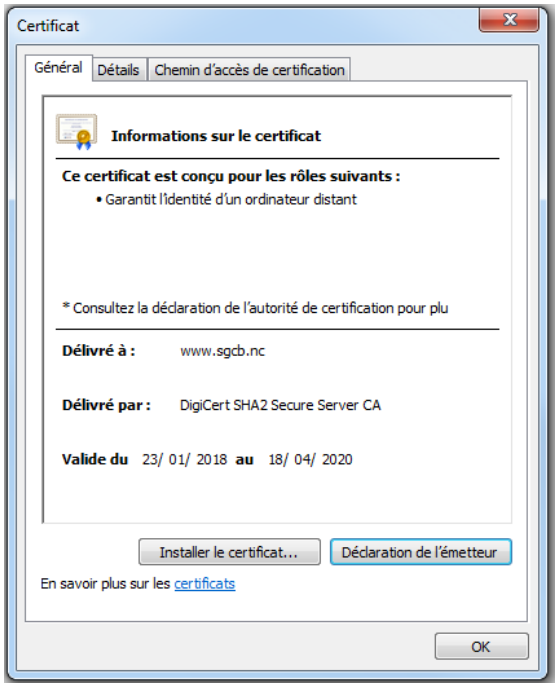
- **Vérifier la fiabilité du site consulté :**

Que vous consultiez un site bancaire ou un site de e-commerce, il est important de s'assurer que l'on se trouve sur un site officiel et sécurisé avant d'effectuer une opération d'authentification ou une opération bancaire. Veuillez à suivre ces instructions pour vous assurer de la fiabilité du site que vous consultez :

- Vérifier l'URL du site dans la barre d'adresse : une URL est l'identifiant unique de la page Internet que vous consultez et qui est visible dans la barre d'adresse de votre navigateur. Vérifiez attentivement cette adresse vous permettra d'identifier un site frauduleux car son adresse présentera obligatoirement des différences avec un site officiel (ex. www.particulier.sg.fr au lieu de www.particuliers.societegenerale.fr).

- Vérifier le préfixe de l'adresse : un site Internet officiel de prestation bancaire ou commerciale, utilise des protocoles de communications sécurisées avec ses clients. Assurez-vous de naviguer sur un site sécurisant vos communications, le préfixe « https » doit précéder l'URL du site (au lieu « http »).

L'adresse complète de l'espace sécurisé de Société Générale est :
https://www.sgcb.nc



- Vérifier le certificat de sécurité :

Le certificat est utilisé pour assurer l'appartenance du site au groupe Société Générale. Votre navigateur Internet permet d'afficher le certificat de sécurité utilisé par la page que vous consultez. Le certificat doit avoir la forme suivante :

- **Protections spécifiques aux Smartphones :**

L'utilisation croissante des Smartphones et le développement croissant des services bancaires sur cette plate-forme introduisent de nouveaux risques pour votre sécurité. L'amalgame entre le téléphone portable et le Smartphone est fréquent, cependant le Smartphone est, ni plus ni moins, un ordinateur avec lequel il est possible de téléphoner. Les mesures de sécurité valables pour un ordinateur (énoncées précédemment) le sont donc pour un Smartphone.

Cependant, des protections spécifiques sont à appliquer au Smartphone :
Protégez le téléphone avec un mot de passe (non trivial) et automatiser le verrouillage de l'écran en cas d'inactivité

- Veillez à appliquer l'intégralité des mises à jour proposées par l'éditeur de votre système
- Ne téléchargez que des applications sur des dépôts d'applications officiels (ex. Apple Store, Google Play Store), au risque d'introduire des applications malveillantes sur votre Smartphone
- Ne déverrouillez sous aucun prétexte le système d'exploitation du Smartphone (ex. jailbreak, rooting), cette pratique augmente votre exposition aux risques
- Ne stockez aucunes données confidentielles si elles ne sont pas chiffrées
- Installez une application antivirus que vous maintiendrez à jour

Nous vous rappelons qu'il est indispensable d'user des mêmes précautions sur un Smartphone que sur un ordinateur lorsque vous naviguez sur Internet

- **Téléchargez l'application dédiée Sogesmart**

Mesures de sécurité

Conscient des risques de sécurité dus à la sensibilité d'un service de banque en ligne, Société Générale met en œuvre toutes les mesures de sécurité à l'état de l'art afin de vous assurer un niveau de sécurité optimal.

- **Mécanismes et procédures d'authentification :**

L'authentification est un élément clé de la sécurité du service de banque en ligne. Cette procédure, qui vous donne accès à la consultation et à la gestion de vos comptes, permet aux systèmes informatiques Société Générale de vous identifier formellement.

Les éléments permettant de vous authentifier sont votre identifiant et votre mot de passe. L'identifiant est unique et vous est fourni à la souscription aux services en ligne. Un mot de passe par défaut vous est attribué à la souscription aux services en ligne et un formulaire de changement de mot de passe vous est soumis lors de votre première connexion.

Cas d'authentification par clavier virtuel

Le nouveau mot de passe que vous aurez choisi sera modifiable à tout moment à l'adresse suivante : https://www.sgcb.nc. Le couple identifiant, mot de passe vous permet d'accéder à la consultation et à la gestion de vos comptes grâce à un système innovant mis en place par Société Générale. Le clavier virtuel renforce la sécurité de votre mot de passe en rendant sa récupération par un individu malveillant plus complexe.

Ne communiquez jamais votre mot de passe à qui que ce soit.
Nous vous rappelons que Société Générale ne vous réclamera jamais votre mot de passe

Cas d'authentification et de validations par SGPass

La sécurité de votre mot de passe est assurée par un système innovant Société Générale. Grâce à la calculatrice SGPass, un nouveau mot de passe est généré à chaque authentification. Le couple identifiant, mot de passe vous permet d'accéder à la consultation et à la gestion de vos comptes.

En addition, la validation de certaines opérations bancaires peut nécessiter une nouvelle authentification pour assurer votre identité, votre consentement et l'intégrité de la transaction.
La calculatrice génère le mot de passe à usage unique (One-Time Password) à entrer sur le site pour valider l'opération bancaire.

Voici un exemple de calculatrice OTP (différents modèles existent) :

- **Chiffrement des communications :**

Le service de banque en ligne Société Générale s'appuie sur le protocole de communication chiffrée. L'activation du chiffrement permet de renforcer la communication HTTP que l'on dénomme désormais HTTPS (S : Secure/Sécurisé). Le protocole HTTPS assure que l'ensemble des informations échangées sur le site sont confidentielles et intègres.

N'hésitez pas à vérifier que vous consultez un site sécurisé :

- Le préfixe « https » précède l'adresse du site que vous consultez
- Selon le navigateur que vous utilisez, un logo de cadenas s'affiche dans la barre d'état

Cas d' « Extended Validation Certificate » (EV)

- Selon le navigateur que vous utilisez, la barre d'adresse devient verte et affiche un logo de certification (qui ressemble à un cadenas la plupart du temps, ex : 

)

L'adresse complète de l'espace sécurisé de Société Générale est : https://www.sgcb.nc

- **Procédure de déconnexion automatique :**

Pour votre sécurité, après cinq minutes d'inactivité sur le service, vous serez automatiquement déconnecté. Ainsi, personne ne pourra utiliser le site à votre place si vous vous êtes absentez sans vous être préalablement déconnecté. Pour vous reconnecter, vous devez à nouveau saisir votre couple identifiant, mot de passe.

Il est impératif de clore votre session en fin de consultation via le bouton de « déconnexion ».
Nous vous rappelons que toute opération effectuée à votre nom (par le biais de la session) ne pourra être répudiée par Société Générale

- **Traçabilité et archivage :**

A des fins de sécurité uniquement, l'activité de votre site bancaire est tracée et archivée (durée limitée réglementairement), 24h/24 et 7j/7, ceci, dans le respect de la réglementation bancaire en vigueur et en conformité avec les lois sur l'informatique et la liberté individuelle (pas d'accès ou de collecte des données personnelles client pour ce traitement).

Toute anomalie fait l'objet d'une analyse approfondie ainsi que des procédures ad hoc pour assurer la fiabilité et la continuité du service à tout instant