Santander Consumer Bank

La banque en ligne en toute sécurité

L'union fait la force

Table des matières

La sécurité en ligne : une responsabilité partagée

Ces dernières années, les entreprises, organisations et services publics ont basculé en masse vers les applications numériques. Une évolution clairement perceptible dans le secteur bancaire également. Les banques en ligne, mais aussi les banques traditionnelles, recourent de plus en plus à des applications en ligne et hautement sécurisées.

L'attention constante envers la sécurité informatique et son perfectionnement sont un gage de sérénité pour les transactions bancaires via Internet. Cela dit, la sécurité en ligne est une responsabilité partagée : votre banque fournit un environnement sûr mais vous aussi, en tant que client, pouvez faire beaucoup de choses dans cette optique. Cet e-book vous explique comment nous pouvons veiller ensemble à la sécurité des services bancaires en ligne. Nous vous y montrons les mesures prises par Santander Consumer Bank, ainsi que les risques dont vous devez être conscient.

Santander Consumer Bank : un environnement en ligne sécurisé

Le Web offre d'innombrables possibilités et opportunités, que nous sommes heureux de pouvoir utiliser en tant que banque en ligne. Mais ces opportunités s'accompagnent d'une responsabilité sociale. Santander Consumer Bank met donc tout en œuvre pour offrir un environnement bancaire en ligne sûr aux particuliers et aux entreprises.

La sécurité en ligne est ancrée dans l'ADN de notre groupe

Ensemble, nous sommes plus forts contre les cybercriminels. Cela s'applique non seulement à nos clients, mais aussi à nos opérations internes. La fraude en ligne ne s'arrête pas aux frontières nationales. Voilà pourquoi nous œuvrons en tant que groupe international à l'optimisation de la cybersécurité.

Chez Santander Consumer Bank, nous voulons sensibiliser les gens à la sécurité en ligne. De sorte qu'Internet devienne un lieu où chacun peut effectuer des opérations bancaires en toute sécurité. Cette prise de conscience commence avec nos propres collaborateurs. En tant que groupe, nous investissons constamment dans de nouvelles formations (ateliers, tests de phishing, piratages en direct, etc.) pour notre personnel afin qu'il puisse reconnaître rapidement les cybermenaces et les signaler aux autorités compétentes.

Vous avez des questions sur les transactions bancaires en ligne ? Ou des doutes concernant la fiabilité d'un message envoyé en notre nom ? Les collaborateurs de notre service clientèle sont disponibles tous les jours ouvrables de 9h00 à 18h00 pour répondre à vos questions par téléphone, e-mail ou chat.

Nos procédures de sécurité en ligne

Santander Consumer Bank ne prend non plus aucun risque en matière de sécurité IT. Nous avons développé diverses procédures de sécurité spécifiques afin de ne pas laisser la moindre chance aux cybercriminels.

Contrôle sécurisé de l'identité et des données de contact

Lors de l'ouverture d'un compte d'épargne en ligne, nous créons un lien entre l'identité du client et ses coordonnées. Nous utilisons à cette fin l'application sécurisée itsme®, la carte d'identité électronique ou une copie de votre carte d'identité. Ces procédures de sécurité sont également utilisées pour la modification de données.

Code personnel d'accès au compte d'épargne

Après avoir ouvert un compte d'épargne, vous recevez de notre part un e-mail contenant votre numéro de compte, votre nom d'utilisateur et votre code d'accès. Afin d'éviter que ce code d'accès ne tombe entre de mauvaises mains (par exemple parce que votre adresse e-mail a été piratée), nous travaillons avec des codes temporaires.

> Santander Consumer Bank ne prend aucun risque en matière de sécurité IT.

Le code que vous recevez par e-mail doit être modifié lorsque vous vous connectez pour la première fois à notre plateforme en ligne. Cette opération n'est possible qu'avec une clé d'accès que nous envoyons au numéro de téléphone que vous avez communiqué lors de l'ouverture du compte. Comme ce numéro de téléphone ne peut être modifié qu'au moyen d'une procédure strictement sécurisée, vous ne courez aucun risque.

Transferts uniquement vers votre propre compte

Lors de l'ouverture d'un nouveau compte d'épargne en ligne, nous vous demanderons de spécifier un compte de référence, c'est-à-dire un compte à vue ouvert à votre nom auprès d'une autre banque belge. Si vous voulez retirer de l'argent de votre compte d'épargne chez Santander Consumer Bank, vous ne pouvez le faire qu'en transférant de l'argent vers ce compte de référence.

Si vous modifiez le compte de référence en ligne, nous vous demanderons de transférer d'abord un montant de ce compte vers le compte d'épargne en ligne auprès de notre banque. Cela nous permettra de vérifier à nouveau l'identité.

Code SMS unique pour chaque transaction

Vous pouvez aisément vous connecter à notre plateforme en ligne via votre nom d'utilisateur et votre code personnel. Mais si vous souhaitez transférer de l'argent vers votre compte de référence ou modifier vos données personnelles, vous aurez également besoin d'un code SMS unique. Ce code sera envoyé au numéro mobile que vous avez communiqué lors de l'ouverture du compte.

Comment assurer votre propre sécurité en ligne ?

La sécurité des transactions bancaires en ligne dépend non seulement des solutions de sécurité des banques mais aussi du comportement des utilisateurs. Les cybercriminels sont de plus en plus astucieux… alors restez vigilant et vous pourrez réduire les risques. Nous avons résumé quelques conseils à votre intention.

Choisissez judicieusement vos mots de passe

Nous n'avons sans doute plus besoin de préciser que votre mot de passe ne doit pas inclure votre nom de famille et votre date de naissance, et qu'il vaut mieux ne pas utiliser le même mot de passe partout.
Mais saviez-vous également qu'il est plus sûr de choisir des mots de passe longs au lieu d'une combinaison complexe de lettres, chiffres et symboles ? À titre d'exemple, il faut une éternité pour craquer le mot de passe « pouletchienchatlapinoiseau », alors que « Ng3h7!a/ » peut être déchiffré en 3 jours à peine.

L'heure est venue de changer de mot de passe ? Alors l'option du haut est plus sûre.

Attention au phishing…

Certains cybercriminels tentent de tromper les gens via de faux e-mails afin de leur soutirer des informations ou de l'argent. Ils se font souvent passer pour des organisations dignes de confiance, telles que des banques, des agences gouvernementales ou des fournisseurs d'accès à Internet. Mais comment distinguer ces faux e-mails des vrais ?

- Examinez attentivement **l'adresse e-mail de l'expéditeur.** Les adresses électroniques sont difficiles à contrefaire, de sorte que les escrocs utilisent souvent des adresses génériques telles que @gmail.com ou @mail.com. Parfois, il y a aussi des fautes d'orthographe dans les adresses, par exemple satnander au lieu de Santander.

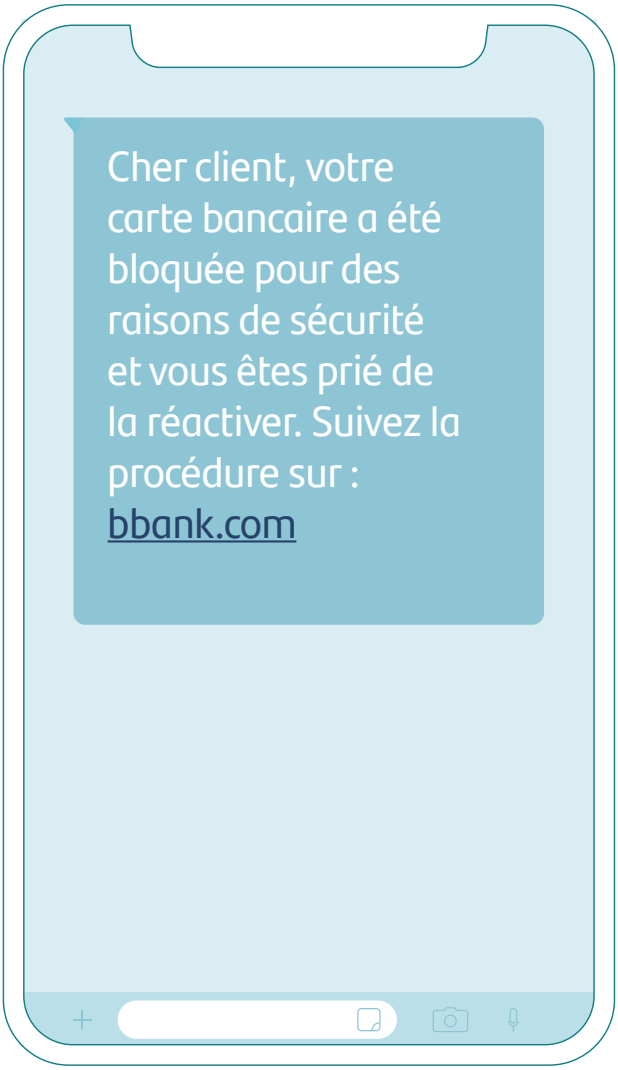
Quelques conseils

- Les e-mails de phishing comportent souvent un **ultimatum** ou une sorte de **menace**. Si vous ne payez pas, votre compte sera prétendument fermé ou vous devrez payer une amende.
- Les organisations fiables ne demanderont jamais des **informations confidentielles** par e-mail. Alors si vous recevez un e-mail inattendu vous demandant des coordonnées bancaires, des mots de passe, des adresses, des numéros de registre national, etc., soyez sur vos gardes.
- Les e-mails de phishing comportent parfois aussi une **pièce jointe**. Il s'agit généralement d'un logiciel permettant aux criminels de voler des données voire de l'argent sur les ordinateurs ou appareils mobiles de leurs victimes. N'ouvrez rien et supprimez immédiatement l'e-mail.
- Vérifiez les **fautes d'orthographe et de grammaire**, non seulement dans l'adresse e-mail mais aussi dans le reste du texte. Les cybercriminels envoient de faux e-mails dans le monde entier sans parler la langue du pays.

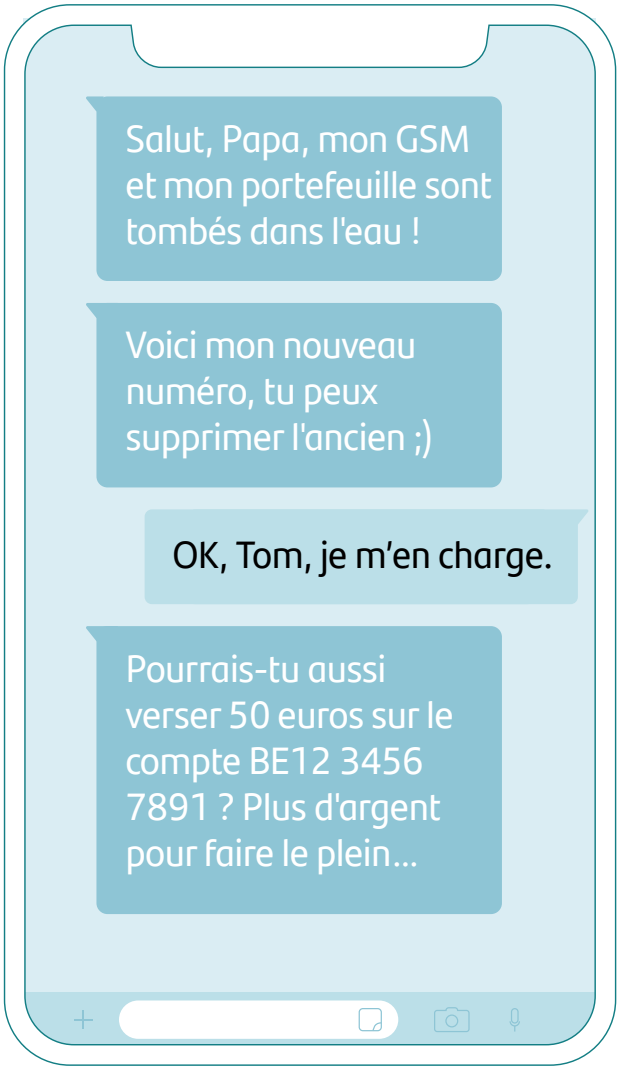
Ce message semble provenir du service de colis cpost, mais son adresse e-mail se termine par @mail.com. Les fautes d'orthographe peuvent également vous donner la puce à l'oreille.

Cet e-mail fait référence à une facture impayée, sans donner davantage d'informations. Il vous pose également un ultimatum : payez maintenant ou votre compte sera fermé. Ne vous laissez pas intimider et restez vigilant.

Quelques conseils



Les banques ne vous demanderont jamais par SMS de leur transmettre des informations confidentielles en ligne. Vous avez reçu un tel message ? Prenez contact avec votre banque avant de cliquer sur le lien.



Quel que soit votre degré d'inquiétude en tant que parent, ce message devrait tirer la sonnette d'alarme. Le fils n'utilise son prénom nulle part, demande que l'on supprime son ancien numéro et réclame directement un versement sur un nouveau numéro de compte.

... et au smishing

Le phishing ne se limite toutefois pas aux e-mails. Les SMS et les messages instantanés, comme WhatsApp, sont également utilisés pour voler des informations ou de l'argent. Là encore, les cybercriminels se font passer pour des banques, des entreprises ou des autorités.

Ils peuvent aussi prétendre être de la famille. Alors ne donnez jamais d'informations confidentielles par le biais de messages et méfiez-vous si un proche vous contacte avec un nouveau numéro et vous demande immédiatement de supprimer l'ancien numéro ou de lui verser de l'argent.

Conseil supplémentaire : les cybercriminels n'utilisent jamais le prénom de la personne dont ils usurpent l'identité. Restez vigilant si vous recevez un tel message.

Réfléchissez avant de vous connecter

Les connexions Internet non sécurisées sont le terrain de jeu des cybercriminels. Ils peuvent, en effet, s'introduire plus facilement dans votre ordinateur, tablette ou smartphone via un réseau non protégé. Aujourd'hui, de nombreux établissements horeca vous permettent de surfer gratuitement sur le réseau WiFi mis à la disposition des clients. Pratique, mais il s'agit souvent de réseaux non sécurisés. Mieux vaut ne pas en faire usage et utiliser votre abonnement de données mobiles pour surfer.

De même, vérifiez toujours attentivement l'URL lorsque vous surfez sur un site Web ou effectuez des achats en ligne. Les pages sécurisées se reconnaissent au cadenas devant leur adresse. La première partie de l'URL est également importante : les adresses qui commencent par « https:// » sont sécurisées. Celles qui commencent par « http:// » ne le sont pas.

À première vue, cette boutique en ligne n'a rien de particulier. Vérifiez néanmoins l'URL avant d'y saisir vos données. Elle vous indiquera en effet qu'il s'agit d'une connexion non sécurisée.

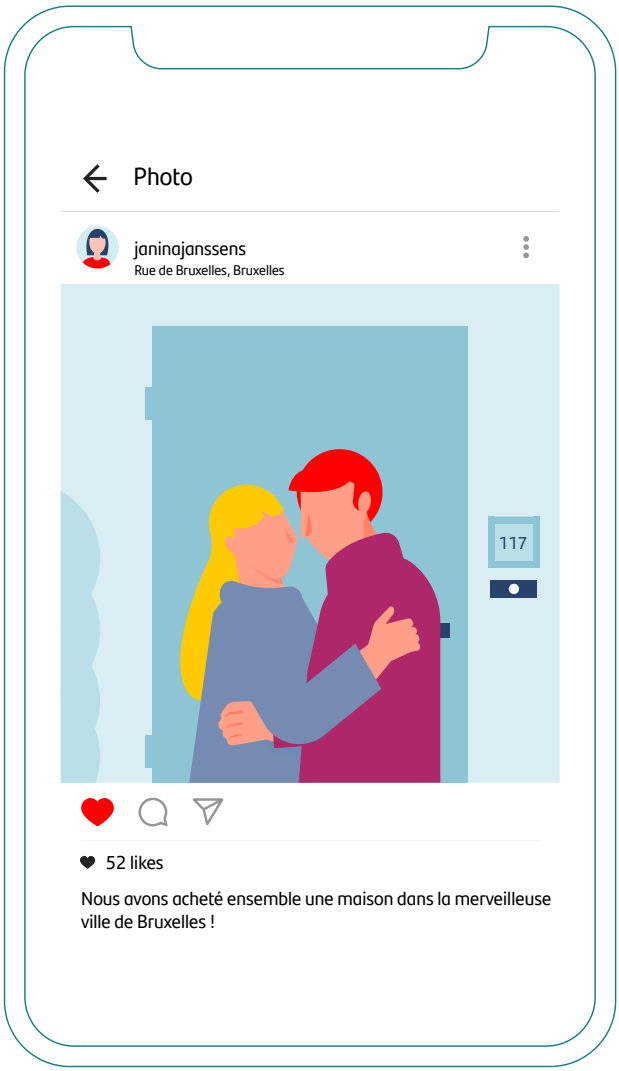
Le fait de travailler dans un café peut apporter un changement agréable, mais gardez à l'esprit que le réseau gratuit n'est pas sécurisé. Créez un hotspot personnel avec votre smartphone et utilisez vos données mobiles pour surfer.

Faites attention à ce que vous partagez

Les réseaux sociaux tels que Facebook, Instagram et TikTok vous permettent de partager d'agréables moments avec votre famille, vos amis et vos connaissances. Mais faites attention lorsque vous publiez des photos ou des vidéos en ligne. Ce qui est un détail pour vous peut constituer une information intéressante pour une personne mal intentionnée.

Vous êtes fier de montrer votre nouvelle maison à vos followers ? Très bien, mais assurez-vous que le nom de la rue et le numéro de la maison ne figurent pas sur la photo, et supprimez-y les éventuelles données de localisation. Vous partagez une photo de votre lieu de travail ? Vérifiez d'abord s'il n'y a pas d'informations sensibles sur votre écran.

Un moment de travail en toute décontraction dans un bar branché ? Belle photo mais assurez-vous qu'on ne voit pas votre carte bancaire. Et que les infos sur votre écran ne sont pas lisibles.



Vous nagez peut-être dans le bonheur... mais partagez cette photo de votre nouvelle demeure et tout le monde connaîtra votre adresse exacte - y compris les personnes mal intentionnées.

Faites appel à la technologie

Il existe de nombreuses applications permettant de protéger votre ordinateur portable, votre tablette ou votre smartphone contre les attaques extérieures. Les spywares, malwares ou liens dangereux sont ainsi bloqués avant même que vous ne les ouvriez ou ne cliquiez dessus. Pratique… mais il est important de maintenir à jour ces logiciels et le système d'exploitation de votre appareil. Ainsi, vous bénéficierez toujours de la dernière solution de sécurité.

Mieux vaut ne pas ignorer la notification indiquant que votre smartphone doit être mis à jour. Les mises à jour renforcent la sécurité et vous protègent mieux, vous et votre appareil, contre les cyberattaques.

Vous avez vu quelque chose de suspect ? Signalez-le !

Vous avez reçu un e-mail étrange, un appel téléphonique suspect ou un message bizarre ? Ou vous êtes malheureusement tombés dans le piège de cybercriminels ? Signalez l'incident aux autorités compétentes. Cela peut parfois sembler une goutte d'eau dans l'océan, mais ici aussi, « l'union fait la force ».

À qui pouvez-vous vous adresser ?

Signaler un phishing ou un smishing

Vous pensez avoir reçu un e-mail frauduleux ou un faux message ? Vous pouvez le transférer à suspect@safeonweb.be. Ensuite, mieux vaut effacer l'e-mail ou le message.

Cette adresse e-mail est gérée par le Centre pour la Cybersécurité Belgique (CCB). Les messages, liens ou pièces jointes suspects sont vérifiés et éventuellement bloqués, afin qu'ils ne fassent pas d'autres victimes.

Victime de la cybercriminalité ?

Quiconque a été victime d'une cyberattaque a tout intérêt à la signaler. N'ayez surtout pas honte de faire une déclaration, car tout le monde peut tomber dans le piège d'escrocs.

- Le point de contact central vous permet de signaler tout cas de fraude ou de tromperie : https://meldpunt.belgie.be/meldpunt/fr/bienvenue. Après avoir complété un questionnaire, vous serez conseillé quant aux démarches à entreprendre.
- Vous pouvez aussi prendre contact directement avec la police. Le site Web Safe on Web vous indique la meilleure façon de procéder.
- Vous avez été victime d'une fraude financière liée à vos opérations bancaires ou à vos investissements ? Vous pouvez aussi contacter directement la FSMA, l'Autorité des services et marchés financiers.

Nos collaborateurs sont à votre disposition tous les jours ouvrables de 8 h 30 à 18 h par téléphone ou par e-mail. | 02/588 96 26 | www.santanderconsumerbank.be