Chez SFL Gestion de patrimoine nous sommes conscients de l'importance de protéger l'information que vous échangez avec nous par Internet contre le piratage informatique.

Nous vous prions de prendre quelques instants pour lire la description des mesures que nous avons prises pour assurer la sécurité de vos renseignements transmis en direct et pour apprendre comment vous pouvez vous protéger sur Internet

Naviguez en toute sécurité

SFL Gestion de patrimoine est conscients de l'importance de protéger l'information que vous échangez avec nous par Internet contre le piratage informatique.

La sécurité et la confidentialité sont prioritaires pour nous. C'est pourquoi nous avons consacré beaucoup d'efforts à faire en sorte que l'information que vous nous transmettez demeure strictement confidentielle. Tous nos employés sont tenus de respecter les normes élevées définies dans notre avis de confidentialité que nous vous invitons à consulter.

Nous vous prions également de prendre quelques instants pour lire la description des mesures que nous avons prises pour assurer la sécurité de vos renseignements transmis en direct.

Naviguez dans notre site en toute confiance

Qu'est-ce qu'une section sécurisée ?

Dans les sections sécurisées de notre site, l'on emploie la technologie des protocoles SSL. Lorsque des renseignements confidentiels tels que votre nom, adresse ou mot de passe sont envoyés par l'entremise d'Internet, les protocoles SSL permettent de protéger la confidentialité des données en transit et de vérifier que les données n'ont été modifiées d'aucune façon durant la transmission. Parce qu'elles sont chiffrées par ces protocoles, les informations sont donc illisibles en transit entre votre navigateur web et notre site. Notre site comporte également des passerelles de sécurité. Ainsi, les données échangées par Internet passent par une série de points de contrôle de sûreté lorsqu'elles arrivent à nos systèmes internes ou qu'elles en partent. Ceci permet de prévenir tout accès non autorisé à nos systèmes informatiques.

Afin de bénéficier de la sécurité offerte par les protocoles SSL, vous devez disposer d'un navigateur Web permettant un niveau de chiffrement de 128 bits, comme les versions 4.01 et supérieures (pour les utilisateurs de PC) et 4.5 et supérieures (pour les utilisateurs de MAC) de Microsoft Internet Explorer. Veuillez noter que dans le cas du Bureau virtuel des représentants (Site Webi), les applications MAC ne sont pas supportées.

Témoins (cookies)

Les témoins sont des blocs de texte qu'un site insère dans un fichier sur le disque dur de votre ordinateur. Bien qu'un code dans le fichier de témoins permette au site de vous identifier en tant qu'utilisateur particulier, il ne vous « reconnaît » pas au moyen de votre nom ni de votre adresse. Vous ne compromettez donc pas votre confidentialité et votre sécurité lorsque vous acceptez un témoin de notre site.

Sauvegarde de renseignements personnels et façons de vous protéger

Notre site vous donne la possibilité de sauvegarder des données. Cela signifie que vous pouvez interrompre votre navigation quand vous le désirez et la reprendre plus tard à partir du même endroit. Pour que vous puissiez tirer parti de cet avantage tout en protégeant votre confidentialité et votre sécurité, nous vous invitons à prendre quelques précautions élémentaires.

Sauvegarde de renseignements personnels

Vous êtes la seule personne à connaître le mot de passe vous permettant d'accéder à votre dossier personnel chez SFL Gestion de patrimoine. Vous ne devez le communiquer à quiconque et vous devez le changer fréquemment.

Ce mot de passe doit idéalement compter de 8 à 10 caractères et contenir au moins un chiffre et une lettre.

Si vous n'arrivez toujours pas à vous rappeler de votre mot de passe, communiquez avec nous. Nous réinitialiserons votre dossier personnel et vous devrez alors inscrire un nouveau mot de passe.

Après 5 essais non fructueux d'entrée dans le système à l'aide d'un mot de passe erroné, le système bloque automatiquement l'accès à votre dossier personnel. Pour le réactiver, communiquez avec l'un de employés ou associés SFL Gestion de patrimoine.

Sortie du système

Lorsque vous terminez une session dans votre dossier personnel, quittez le système afin de vous assurer que nul ne peut accéder à votre dossier. De même, si vous vous éloignez de votre ordinateur et surtout si la limite de temps qui vous est accordée n'a pas été atteinte, quittez le système. Pour ce faire, vous n'avez qu'à fermer votre navigateur.

Si vous oubliez de quitter, le système met automatiquement fin à votre session après une certaine période d'inactivité.

Votre mot de passe : la clé de votre sécurité

Le choix d'un mot de passe ne doit pas être pris à la légère. Un mot de passe trop évident peut facilement être deviné par un imposteur. En suivant quelques règles simples, vous choisirez des mots de passe qui garantiront votre confidentialité et votre sécurité.

Choisissez toujours des mots de passe qui comprennent au moins des lettres et des chiffres. L'inclusion de caractères spéciaux (p. ex. : @, ?,) les rend encore plus sécuritaires. Choisissez un mot de passe différent chaque fois que vous vous inscrivez à un service différent.

Lorsque vous modifiez votre mot de passe, évitez de le changer pour un de ceux que vous avez utilisés récemment.

Ne choisissez pas des mots de passe qui sont évidents. Évitez de choisir vos mots de passe à partir d'éléments comme les suivants :

- noms,
- surnoms,
- noms des enfants,
- fêtes, anniversaires,
- renseignements familiaux personnels,
- numéros de téléphone,
- biens,
- intérêts,
- mots du dictionnaire,
- mots du dictionnaire épelés à l'envers,
- noms de villes et de rues,
- noms d'équipes de sport et d'attractions locales,
- numéros de plaque d'immatriculation.

Un imposteur disposant d'outils à la fine pointe de la technologie est en mesure de rassembler un ensemble substantiel de données à partir de dictionnaires, de listes d'envoi et de sites web de réseaux sociaux et de s'en servir pour tenter de découvrir votre mot de passe.

Pour choisir des mots de passe sécuritaires, vous pouvez utiliser différentes techniques telles que

- modification de l'orthographe à partir de la phonétique (p. ex. : « chat » devient « shat »);
- substitution de lettres à des chiffres ou caractères spéciaux et utilisation alternée de lettres majuscules et minuscules (p. ex. : « monpiano » devient « M0nP1@n0 »);
- utilisation d'acronymes, y compris ceux de votre propre cru (« Tout vient à point à qui sait attendre » devient « TVAPAQSA »);
- utilisation de noms communs transformés par le déplacement d'une lettre ou par l'emploi de rangées différentes sur le clavier (p.ex.: « claude » devient « clbuee » si l'on déplace la 3e et la 5e lettre d'une position vers la droite; « qwerty » devient « qsefth » si l'on choisit la 2e, la 4e et la 5e lettre d'une rangée plus bas sur le clavier).

Gestion efficace de votre mot de passe

- Utilisez un nouveau mot de passe chaque fois que vous vous inscrivez à un nouveau service.
- Ne donnez pas votre mot de passe à quiconque.

- Ne conservez pas des mots de passe dans votre ordinateur.
- Changez régulièrement votre mot de passe.
- Si vous mettez votre mot de passe par écrit, assurez-vous de le placer en lieu sûr.

Certificat de page sécurisée

Au cours de vos sessions dans les parties sécurisées de notre site, vous pouvez vérifier, au moyen de l'affichage du certificat de page sécurisée, que vous faites vraiment affaire avec Desjardins Sécurité financière, et non avec un tiers malintentionné :

Microsoft Internet Explorer (utilisateurs de PC) :

- Sélectionnez « Propriétés » dans le menu « Fichier » et cliquez sur « Certificats ».

Si vous utilisez un ordinateur MAC ou un navigateur Web autre que Internet Explorer, veuillez consulter la rubrique d'aide de votre navigateur Web pour savoir comment accéder à l'affichage du certificat de page sécurisée.

Niveau de chiffrement et paramètres de sécurité de votre navigateur

Les options de sécurité de votre navigateur constituent une autre façon d'assurer votre protection. Les navigateurs vous offrent la possibilité de recevoir un message d'alerte ou un avertissement si l'une des situations suivantes se produit ou est sur le point de se produire :

Réception d'une identité invalide à l'égard du site auquel vous vous apprêtez à transmettre des données;

Envoi d'une transmission par l'entremise d'une connexion « ouverte » ou non sécurisée.

Signaux de sécurité du navigateur

Il existe deux façons qui permettent à votre navigateur de vous aviser de la présence dans une page Web de mesures de sécurité relatives à la transmission de données :

- L'URL qui identifie la page commence toujours par « https:// » plutôt que par la séquence « http:// » habituelle.
- Un symbole de sécurité indique que les transactions s'effectuent selon un mode qui accepte les transmissions sécurisées : Une icône « cadenas fermé » est affichée dans le coin inférieur droit de l'écran de votre navigateur Microsoft Internet Explorer. (utilisateurs de PC)

Vous pouvez vérifier le niveau de chiffrement de votre navigateur de la manière suivante :

- Microsoft Internet Explorer version 4.01 ou supérieure :
  - Sélectionnez « À propos de Internet Explorer » dans le menu « ? » afin d'afficher la puissance de chiffrement (aussi appelé « cryptage ») offerte par votre navigateur. (utilisateur de PC)

- Sélectionnez « Aide de Internet Explorer » dans le menu « Aide », puis « Sécurité » afin d'afficher la puissance de chiffrement offert par votre navigateur ou encore, consultez l'information affichée en bas à gauche dans la barre d'état.

Fraude par hameçonnage

L'hameçonnage est un stratagème utilisé par les fraudeurs qui consiste à envoyer massivement des courriels ou des textos semblant provenir d'une institution financière ou d'une entreprise connue.

Ces courriels ou textos sont utilisés par des personnes mal intentionnées pour voler vos informations personnelles ou installer un logiciel malveillant sur votre ordinateur, en vous incitant à cliquer sur des liens ou à ouvrir des fichiers joints.

Les impacts potentiels de ce type d'attaque peuvent s'avérer importants tels que la perte de vos données, l'accès non autorisé ou le vol de vos informations confidentielles ensuite utilisées pour commettre des fraudes.

La vigilance et la reconnaissance des courriels d'hameçonnage permettent de vous protéger de ces impacts. Un courriel d'hameçonnage se présente sous plusieurs formes, mais sa caractéristique principale est qu'il est non sollicité.

1 simple geste à adopter pour éviter de vous faire hameçonner

Avant de cliquer, vous validez l'information en :

1. Vérifiant si le courriel ou texto est attendu et sollicité
2. Portant attention aux différentes situations qui tentent de vous faire réagir :
   Urgence : L'objectif est de vous inciter à poser une action rapide et irréfléchie en misant sur le sentiment d'urgence et la conséquence engendrée.
   Profit : L'objectif est de vous faire croire que vous avez obtenu un gain ou un avantage, sans y avoir souscrit. Les fraudeurs misent sur l'appât du gain pour vous pousser à divulguer vos renseignements personnels.
   Problème : L'objectif est de vous informer qu'un problème est survenu dans votre compte. Cette situation vous oblige à divulguer vos renseignements personnels pour résoudre le problème.
3. Vérifiant si l'adresse courriel de l'expéditeur vous semble connue et légitime (notamment après l'arobas (@) : est-ce une adresse d'entreprise ou personnelle?)
4. Déplaçant votre curseur sur le lien hypertexte (sans cliquer sur le lien) pour vérifier que l'adresse du lien semble légitime et correspond à l'entreprise de l'expéditeur (attention aux adresses similaires).
5. Jugeant de la pertinence et de la vraisemblance du courriel. Soyez suspicieux! (ex. : avez-vous vraiment participé à un concours? attendez-vous un colis? est-ce la procédure habituelle? est-ce « trop beau pour être vrai »?, etc.).
6. Ne fournissant jamais d'information confidentielle permettant de vous authentifier via un courriel (ex. : NAS carte de crédit, date de naissance, mot de passe, etc.).

7. Évitant la curiosité et la distraction par des identités visuelles ou logos connus (qui peuvent être facilement copiés et prendre l'apparence d'un courriel ou site Web authentique).

Bref soyez vigilant!

Vous croyez avoir vécu une tentative d'hameçonnage?

Rapportez la situation au 1 866 335-0338 ou par courriel à protection@desjardins.com.

Sollicitation téléphonique

Le 30 septembre 2008, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a lancé la Liste nationale des numéros de télécommunication exclus (LNNTE). Les consommateurs canadiens qui désirent réduire le nombre d'appels et de télécopies de télémarketing qu'ils reçoivent peuvent ainsi s'inscrire sur cette liste.

Si vous êtes un citoyen américain, prenez note que l'entreprise n'effectue aucune sollicitation téléphonique aux États-Unis.

Nous avons tout mis en œuvre pour satisfaire aux exigences du CRTC. Comme par le passé, nous devons entre autres tenir notre propre liste interne de non-sollicitation afin de respecter le choix de nos clients.

Voici les réponses aux questions les plus fréquemment posées concernant :

- la liste nationale des numéros de télécommunication exclus
- la liste interne de non-sollicitation de Desjardins Sécurité financière