SBM

Services bancaires en ligne de la SBM: conseils de sécurité

La SBM s'est engagée à mettre à votre disposition la plateforme la plus sécurisée possible pour accéder à nos services en ligne. Ainsi avons-nous élaboré et mis en place plusieurs mesures pour sécuriser l'accès à vos comptes bancaires.

Les conseils de sécurité que nous vous donnons ci-dessous vous aideront à protéger vos données personnelles et les fonds figurant à vos comptes bancaires. Ils peuvent être exécutés de manière très simple. Nous vous recommandons fortement de les suivre de manière à éviter toute mauvaise surprise.

1. **Accédez correctement aux services bancaires en ligne de la SBM.**

   Pour accéder correctement à nos services en ligne, veuillez vous connecter à l'adresse suivante http://www.sbmonline.com et cliquer sur le lien « Services en ligne » qui apparaîtra sur la page d'accueil. Pour des raisons de sécurité, nous vous suggérons de toujours utiliser des navigateurs internet que nous recommandons. Microsoft Internet Explorer (versions 7.0 et plus) ou Netscape Navigator (version 6.2.x) pour systèmes d'exploitation Microsoft Windows vous garantiront une expérience en ligne optimale.

2. **Vérifiez les indications de sécurité suivantes:**

   - Assurez-vous que vous êtes bien sur le site web sécurisé des services en ligne de la SBM en vérifiant que l'adresse URL commence par "https" au lieu de "http";
   - Vérifiez que l'icône en forme de cadenas fermé apparaît bien en bas de page, à droite;
   - Bougez votre curseur sur cette icône pour vér ifier si la ment ion "SSL secure (128 bit)" apparaît;
   - Vérifiez le certificat du site web en cliquant à deux reprises sur l'icône et assurez-vous que les détails suivants apparaissent:
     - "Issued to ibmg.sbmgroup.mu"
     - "Issued by www.verisign.com"

     Et que la date de validité n'a pas expiré ("valid from …to …")

3. **Précautions à observer**

3.1 Protéger votre mot de passé

   - NE JAMAIS révéler à QUICONQUE votre nom d'utilisateur (« user id») et mot de passe.
   - Choisissez un mot de passe dont vous pourrez facilement vous rappeler et qui sera difficile à deviner, par exemple Partym@1;
   - Utilisez une combinaison de lettres (majuscules et petites lettres), chiffres et symboles typographiques (@, !, ~,etc) quand vous choisissez un mot de passe;

- Ne pas utiliser des mots du dictionnaire ou des informations liées à la famille en choisissant un mot de passe car ils sont faciles à déchiffrer ou à deviner;
- Votre mot de passe doit être unique et servir exclusivement à vous donner accès à SBMNet. Veuillez à ne pas utiliser le même mot de passe pour accéder à un autre site internet, quel qu'il soit;
- Changez votre mot de passe régulièrement;
- Ne jamais choisir les options "Auto Complete" (remplir automatiquement) ou "Remember My Password" (se rappeler de mon mot de passe);
- Changez votre mot de passe IMMEDIATEMENT si vous sentez qu'il ne vous offre pas suffisamment de sécurité;
- Une fois que vous aurez accédé au site, le système SBMNet ne vous demandera PAS d'entrer à nouveau votre mot de passe. Au cas où on vous le demanderait à travers une fenêtre qui apparaîtrait à l'écran, veuillez ignorer cette requête et fermez la fenêtre;
- Détruisez toute correspondance de la SBM contenant votre nom d'utilisateur (« User ID ») ou les details de votre mot de passe.

3.2 Accès à SBMNET dans les endroits publics (cybercafés et accès publics Wi-Fi)

- Evitez de vous connecter à SBMNet à partir d'ordinateurs en réseau ou disponibles au public;
- Ne jamais changer des détails sensibles comme votre nom d'utilisateur ou « PIN » ou mot de passe dans un lieu public;
- Prenez garde aux personnes se tenant près de vous quand vous entrez votre mot de passe ou nom d'utilisateur ou « PIN ».

3.3 Pour clore votre session en ligne

- Suivez les procédures "Sign Out" pour clore votre session au lieu de simplement fermer la fenêtre;
- Effacez régulièrement les fichiers temporaires et « cookies » après avoir surfé sur internet.

3.4 Sécurisez votre ordinateur personnel.

- Assurez-vous qu'aucune autre personne n'ait accès à votre ordinateur personnel;
- Utilisez un anti-virus fiable et mettez-le à jour régulièrement;
- Configurez votre ordinateur personnel de manière à recevoir les avis de mise à jour pour votre système d'exploitation;
- Gardez à jour votre système d'exploitation, navigateur, et logiciel e-mail avec les dernières versions et modifications de sécurité;
- Utilisez un pare-feu et un système de détection adéquat pour bloquer ou détecter les attaques ou programmes malveillants sur vos systèmes;
- Ne pas installer des logiciels gratuits téléchargés via l'internet ou obtenus de sources non fiables.

3.5 Précautions pour les e-mails

- Méfiez-vous des e-mails vous demandant votre code « PIN » ou mot de passe. La SBM n'envoie jamais des e-mails pour demander des mots de passe ou codes « PIN »;
- Ne jamais cliquer sur les liens se trouvant dans des e-mails ou sur des sites tiers pour avoir accès à SBMNet;
- Utilisez des filtres de « spam » sur votre ordinateur personnel afin de vous protéger des « spams ».

3.6 Autres mesures de sécurité

- Ne pas surfer sur d'autres sites web en même temps quand vous effectuez des transactions bancaires par internet.
- Ne pas laissez votre ordinateur personnel sans surveillance quand vous effectuez des transactions bancaires par internet.

3.7 Suivez votre compte SBMNet régulièrement

- A chaque nouvelle visite, vérifiez les informations disponibles concernant la date et l'heure de votre précédente visite;
- Consultez régulièrement vos relevés de compte afin d'éviter toute fraude;
- Contactez la SBM immédiatement en cas d'irrégularité.

Pour plus de renseignements, veuillez nous téléphoner sur le **0202266606** ou rendez vous dans la succursale SBM la plus proche de votre domicile ou envoyez-nous un courriel à l'adresse **hotlinemada@sbmgroup.mu**.