Informations importantes concernant la protection de votre NIP et mot de passe unique

Nous avons mis en œuvre des mesures afin de protéger vos informations de compte. Toutefois, afin de garantir que votre sécurité en ligne, l'accès au compte et les informations y afférentes ne sont pas compromises, nous vous recommandons d'adopter les directives de sécurité eService suivantes.

1. Avant de saisir votre WebUserID et NIP, vous devez toujours vous assurer que le site Web que vous consultez est bien celui de Schroders. Vous pouvez le faire en vérifiant l'URL qui s'affiche dans votre navigateur ainsi que le nom de la banque sur son certificat numérique. Cette précaution permet de garantir que vous ne divulguez pas votre code d'accès eService et votre NIP à un site web autre que celui de Schroders.
2. Conseils importants relatifs à la protection de votre NIP, votre mot de passe et vos informations de compte:
   (a) Le NIP doit comporter au minimum 6 chiffres ou 6 caractères alphanumériques.
   (b) Le NIP ne doit pas être basé sur le WebUserID, le numéro de téléphone personnel, l'anniversaire ou toute autre information personnelle pouvant être devinée.
   (c) Les NIP sont confidentiels et ne doivent pas être divulgués à qui que ce soit.
   (d) Les NIP doivent être mémorisés et ne doivent pas être enregistrés où que ce soit.
   (e) Les NIP doivent être changés régulièrement. En cas de suspicion, quelle qu'elle soit, que le NIP est compromis ou mis en danger, changez-le immédiatement et avertissez-en Schroders.
   (f) N'utilisez pas le même NIP pour différents sites web, applications ou services, particulièrement lorsqu'ils se rapportent à différentes entités.
   (g) Ne conservez pas votre WebUserID, NIP et/ou token de sécurité ensemble.
   (h) Ne sélectionnez pas l'option du navigateur pour sauvegarder ou retenir le nom d'utilisateur et le mot de passe.
   (i) Vérifiez que l'adresse du site web de la banque change de « http:// » à « https:// » et qu'une icône de sécurité en forme de regard ou de clé apparaît lorsque l'authentification et le cryptage sont attendus.
   (j) Ne permettez à personne de conserver, d'utiliser ou de jouer avec votre token de sécurité.
   (k) Ne révélez à personne le mot de passe unique généré par le token de sécurité.
   (l) Ne divulguez pas le numéro de série de votre token de sécurité à qui que ce soit.
   (m) Vérifiez fréquemment le solde et les transactions de votre compte bancaire et signalez toute divergence.
3. Installez un logiciel anti-virus, un anti-spyware et un pare-feu sur vos ordinateurs personnels.
4. Mettez régulièrement à jour les systèmes d'exploitation, les produits anti-virus et pare-feux avec des patches de sécurité ou de nouvelles versions.

5. Désactivez le partage de fichiers et d’imprimantes sur vos ordinateurs, en particulier lorsque vous avez un accès Internet via des modems câble, connexions à large bande ou configurations similaires.
6. Envisagez l’utilisation de la technologie de cryptage afin de protéger des données hautement sensibles.
7. Videz le cache du navigateur après la session en ligne.
8. Déconnectez-vous de la session en ligne.
9. N’installez pas de logiciels ou ne lancez pas de programmes d’origine inconnue.
10. Supprimez les e-mails indésirables ou en chaîne car ils peuvent contenir un code malveillant.
11. N’ouvrez pas les pièces jointes d’e-mails de personnes que vous ne connaissez pas.
12. Ne divulguez pas d’informations personnelles, financières ou sur votre carte de crédit à des sites web peu connus ou suspects.
13. Ne vous servez pas d’un ordinateur ou d’un appareil non digne de confiance pour utiliser eServices de Schroders.
14. Ne vous servez pas d’ordinateurs publics ou d’internet cafés pour utiliser eServices de Schroders.

Les informations susmentionnées sur les précautions de sécurité et les bonnes pratiques ne doivent pas être considérées comme exhaustives ou statiques.

N’hésitez pas à nous contacter pour toute question ou si vous avez besoin d’aide.