Vous effectuez vos opérations via Web Banking ?
Nous vous invitons à observer quelques conseils de sécurité

Vérifier que le site est sécurisé

1. **Toujours se connecter au Web Banking à partir d'un ordinateur et d'une connexion internet connus**. Eviter les ordinateurs publics (ex. : cafés, hôtels), les connexions Wifi ou filaires publiques.
   Certains programmes ou virus sont susceptibles d'être installés sur les ordinateurs publics de même que certaines redirections de connexions wifi.

2. **Installer un anti-virus viable** (ex. Kapersky, ESET, McAfee) et s'assurer la mise à jour quotidienne.
   Certains anti-virus proposent une fonction spécialement dédiée aux connexions vers les sites bancaires.

3. **Utiliser un système d'exploitation « officiel »**
   Ne pas utiliser de une version piratée de Windows piraté ou d'O.S jailbreaké.

4. **Maintenir à jour le système d'exploitation.**
   Windows permet une mise à jour automatique de son système.

5. Vérifier l'adresse URL est bien celle du Web Banking et qu'elle débute toujours par **HTTPS**.

Quelques bonnes pratiques de sécurité

6. **Vérifier régulièrement l'historique des virements**.
   Signaler immédiatement à la banque un virement dont le destinataire est inconnu.

7. Sur l'application "Web Banking" pour iPhone et smartphones Android, **mettre en place une alerte** pour les virements ou dépenses par carte de crédit dépassant un certain montant et lorsque le solde du compte courant est inférieur à un certain montant.

8. Privilégier **l'identification renforcée** en vous connectant avec le Token.

9. Utiliser un code secret unique pour vous connecter au Web Banking.
   D'une manière générale ne partager jamais le même mot de passe sur plusieurs sites Internet.

10. Ne jamais communiquer **aucun code secret** par mail, téléphone ou tout autre formulaire.
    La banque ne vous demandera jamais de code secret (ni de codes LuxTrust ou Card Code) et ne vous enverra pas de lien vers le Web Banking dans un e-mail.

11. **Quitter le Web Banking en cliquant sur « Déconnexion »** et non pas la croix de la fenêtre du navigateur.

12. Saisir l'adresse du site dans votre navigateur ou utiliser un « favori ». Ne pas cliquer sur les liens hypertextes proposés dans un e-mail.

Que faire ?

13. En cas de perte ou de vol de votre téléphone, tablette ou ordinateur, contacter immédiatement le support Web Banking et modifier tous vos mots de passe au plus vite (messagerie, etc.)

14. Nous communiquer tout comportement suspect (de l'application ou par exemple par un mail reçu).

BGL BNP Paribas Direct
Tél. (+352) 42 42-2000 du lundi au vendredi de 8h à 18h
E-mail : info@bgl.lu

,