La Banque en sécurité

Internet vous ouvre une fenêtre sur le monde mais il ouvre aussi votre ordinateur sur un monde où il n'y a pas que des gens honnêtes. La sécurité est un élément primordial pour bpost banque. Nous prenons toutes les mesures nécessaires afin de garantir une sécurité maximale tant au niveau du site internet que des transactions bancaires.

Cette sécurité maximale dépend d'une chaîne dont votre ordinateur constitue un des maillons. Vous devez également, en tant qu'utilisateur, contribuer à la solidité de cette chaîne de sécurité. C'est pourquoi il est important de respecter les règles de base afin de maintenir la sécurité à tous les échelons et d'éviter les risques et dangers qui nous menacent sur le net.

Mesures prises par bpost banque pour sécuriser son site

Pour bpost banque, la sécurité des opérations bancaires est prioritaire. Voici quelques mesures de sécurité adoptées:

- La connexion sécurisée (d'où le "https:" dans l'adresse) qui garantit la codification des flux d'informations entrants et sortants. Grâce à cela, les données qui circulent sont sécurisées.
- Avec PCbanking, vos données et vos transactions ne se trouvent pas sur votre ordinateur mais sur les serveurs de la banque, protégés par firewall et sécurisés au maximum. Des contrôles sont constamment effectués afin d'adapter la protection et la sécurité de manière flexible et rapide pour faire face aux nouvelles menaces.
- La signature électronique: l'association du lecteur de carte bpost banque et votre code PIN, fournit une signature électronique qui ne peut être utilisée qu'une fois. Après trois tentatives infructueuses, votre carte bancaire sera bloquée.

  PCbanking utilise 2 types de signatures :

  - **Signature M1** du lecteur de carte bancaire: sert uniquement à **vous identifier** lorsque vous commencez une session PCbanking.
  - **Signature M2** du lecteur de carte bancaire: sert à **signer vos opérations**.

  Attention

  bpost banque ne vous demandera jamais de vous identifier avec une signature M2 ou de signer une transaction avec une signature M1. Si vous êtes confronté à une telle demande, ne signez rien et contactez-nous immédiatement.

  Quand faut-il signer?

  Vous devez signer à chaque fois que vous nous donnez une instruction, de la même manière que vous devriez apposer votre signature manuscrite sur un document papier. Afin de faciliter l'utilisation de PCbanking, nous avons cependant prévu quelques exceptions à cette règle dans le cadre des virements.

  Quand dois-je signer un virement?

  En règle générale, vous devez signer tous les virements belges, européens et internationaux. Pour faciliter et accélérer vos paiements en PCbanking, nous avons prévu quelques dispenses. Vous ne devez pas signer un virement si le compte bénéficiaire est un compte belge qui est:

- déjà connu dans votre liste de bénéficiaires sauvegardés

  ou

- fait partie des comptes les plus utilisés en Belgique (par exemple les comptes des pouvoirs publics, des entreprises de télécommunications, fournisseurs d'énergie, compagnie d'assurances,...)

- **et**

- Vous ne dépassez pas la limite de 2.500 euros par jour ou 5.000 euros par semaine.

Les règles de base de l'internet en sécurité

La sécurité sur internet nous concerne tous. bpost banque vous explique donc les règles de base afin que chacun puisse continuer à utiliser le web en sécurité et de façon agréable, notamment pour ses opérations bancaires.

1. **Ne répondez JAMAIS à un mail soi-disant envoyé par bpost banque dans lequel on vous demanderait,** par exemple:
   - de communiquer votre numéro de carte de crédit;
   - de confirmer votre code secret personnel (PIN);
   - d'installer un programme contenant des possibilités supplémentaires pour PCbanking, etc.

   Même si un tel message devait présenter toutes les caractéristiques habituelles de bpost banque et vous inspirer confiance, n'y répondez en aucun cas. De tels messages prennent souvent votre sécurité pour prétexte : « nous faisons cela pour des raisons de sécurité, etc. ». N'y répondez tout simplement pas : bpost banque ne vous demandera jamais de communiquer des informations confidentielles via un canal non protégé. En cas de besoin, nous vous demandons ces informations dans un environnement confidentiel: en agence ou après une identification en bonne et due forme dans PCbanking.

2. **Vérifiez TOUJOURS si vous êtes bel et bien sur un véritable site de bpost banque.**
   Vous pouvez vérifier que vous vous trouvez sur un site de bpost banque au moyen du petit cadenas qui s'affiche dans la partie inférieure droite de votre navigateur (ex: Internet Explorer 6, Internet Explorer 7, Firefox). Si vous arrivez sur l'un de nos sites via un e-mail, cliquez sur ce cadenas et vérifiez que l'adresse se termine bien par .bpostbanque.be (https://www.bpostbanque.be …)..

3. **Installez un logiciel anti-virus et mettez-le régulièrement à jour**.
   Internet vous ouvre une fenêtre sur le monde mais il ouvre aussi votre ordinateur sur un monde où il n'y a pas que des gens honnêtes. Voilà pourquoi vous devez protéger votre ordinateur avec un bon anti-virus. Sans oublier bien entendu de le mettre à jour régulièrement. Les logiciels de sécurité mènent une lutte continuelle contre les gens mal intentionnés, ce qui explique leurs fréquentes mises à jour. Installez-les toujours sans délai.

   Vous avez reçu un mail suspect, vous demandant, par exemple, de communiquer ou de confirmer les numéros ou les codes de vos cartes de crédit bpost banque? Transmettez-le directement à security.alert@bpostbanque.be. Nos responsables de la sécurité le vérifieront tout de suite. Internet doit rester sûr et agréable!

Comment devenir un utilisateur vigilant?

Pour profiter d'internet en sécurité, suivez les règles de base ci-dessus, mais aussi.

- Bloquez les pirates à l'aide d'un pare-feu (firewall) qui régule les flux d'informations entrants et sortants.
- Protégez-vous des spywares (en plus de virus) grâce à un anti-spyware fiable et mettez-le régulièrement à jour. Certains anti-virus protègent également votre ordinateur des spywares. Vous pouvez consulter une liste non-exhaustive de ces programmes (gratuits ou payants) disponibles dans les magasins informatiques ou sur Internet.
- Effectuez régulièrement un scan complet de votre ordinateur à l'aide de l'anti-virus.
- Sécurisez votre connexion internet sans fil pour empêcher les voisins ou les personnes qui se trouvent à proximité de chez vous d'utiliser à votre insu votre connexion à haut débit. Changez les mots de passe fournis avec votre matériel, ainsi que le nom de votre réseau (SSID). Utilisez un système de cryptage des données WPA2 ou au minimum WEP. Demandez éventuellement l'aide d'un spécialiste avant de procéder à ces modifications.
- Installez toujours la version la plus récente du browser. Ceux-ci contiennent en général les dernières avancées techniques en matière de sécurité.
- Installez les mises à jour de sécurité de votre système d'exploitation.
- Pour plus d'informations sur la terminologie technique, consultez le lexique.

Les bonnes habitudes

- Ne pas communiquer le code secret de votre module de sécurité (votre numéro d'abonnement, le code PIN de votre carte de débit);
- Ne jamais inscrire son code PIN quelque part;
- PCbanking ou la carte bancaire restent personnels et ne peuvent pas être utilisés par plusieurs personnes;
- Clôturez votre session PCbanking de la bonne manière en cliquant d'abord sur le bouton « Se déconnecter » qui se trouve à gauche sur l'écran.

De manière générale :

- bpost banque ne vous demandera jamais d'informations confidentielles par mail. Si on essaye d'obtenir des informations personnelles via e-mail ou pop-up (phishing), n'y répondez pas mais prévenez notre Helpdesk au 022/012345.
- Méfiez-vous si vous êtes contacté par téléphone au sujet d'une fraude éventuelle liée à votre carte de crédit ou à votre compte. Une nouvelle technique de fraude, le vishing (voice-phishing) consiste à contacter les clients d'une banque par téléphone pour les informer d'une fraude et les inviter à rappeler un numéro communiqué en s'identifiant avec des données confidentielles (numéro, codes,...). Ne paniquez pas et ne donnez pas suite à ce genre d'appels. Contactez votre agence, phonebanking ou notre Helpdesk par les numéros que vous connaissez et jamais ceux reçus dans le message. En dehors des heures, et en cas de doute, vous pouvez faire bloquer votre carte bancaire via Card Stop (0,30euro/min).
- Si vous constatez un usage frauduleux (transactions, montants incorrectes, etc.) de votre PCbanking, informez bpost banque qui prendra les mesures nécessaires.
- Attention aux mails qui vous promettent des gains, dans lesquels on écrit que vous allez recevoir de l'argent sur votre compte ou que vous devez le conserver pour des inconnus. Il s'agit toujours de fraudes qui ont pour but de vider votre compte. Plus d'infos sur http://www.spamsquad.be/fr/home.html.
- Evitez les faux sites web. Pour accéder à un site sécurisé, ne cliquez jamais sur un lien reçu dans un e-mail. Ceux-ci peuvent vous menez ailleurs que là où vous pensez. Pour vous rendre sur un site où vous avez l'habitude d'aller, utilisez de préférence les liens présents dans vos favoris.

- Toujours être prudent lors de l'installation d'un nouveau programme. Il faut toujours être certain de ce que vous installez et de sa provenance. Soyez particulièrement attentif si vous partagez votre ordinateur avec vos enfants.
- N'utilisez jamais des ordinateurs publics (cybercafé) pour effectuez vos transactions bancaires. Vous ne savez pas si ces ordinateurs sont infectés par des virus ou autres programmes menaçant la sécurité de vos transactions.
- Méfiez-vous des pièces jointes au courrier électronique. Si vous n'êtes pas certains de l'origine, ne l'ouvrez pas.
- Ne répondez jamais à un SPAM et ne cliquez sur aucun hyperlien contenu dans le message car vous confirmeriez ainsi l'existence de votre boite aux lettres et recevrez ensuite beaucoup plus de messages indésirables. Effacez ces messages ou utilisez un filtre anti-spam. Soyez vigilant lorsque vous faites vos achats sur Internet.
- Ne communiquez pas le numéro de votre carte de crédit si vous ne souhaitez pas faire un achat. Certains sites demandent un numéro de carte de crédit soit disant pour vérifier que vous êtes majeurs mais utilisent ensuite votre carte pour effectuer des achats à votre insu.

En cas d'usage frauduleux de vos données

- Vous avez reçu un mail suspect? On vous demande de communiquer ou de confirmer les numéros de vos cartes bancaires de bpost banque ou vos codes PIN ? Contactez POSTINFO au 022/012345.
- En cas de perte, de vol ou à chaque risque d'usage frauduleux de votre carte bancaire, avertissez immédiatement: Card Stop (7 jours sur 7, 24 heures sur 24) au numéro 070/344.344 et POSTINFO au 022/012345 du lundi au vendredi de 8h à 19h et samedi de 9h à 12h ou dès que le service est accessible si la constatation des faits a lieu en dehors des heures de fonctionnement.
- Déclarez la perte ou le vol de votre carte bancaire dans les 24 heures aux services de police du lieu où la perte ou le vol ont eu lieu.

Lexique

- **Adware**: Logiciel qui contient une publicité."Ad" signifie "publicité" en anglais. Un Adware est un logiciel gratuit dans lequel est affichée une publicité. En règle générale un Adware n'est pas un logiciel espion (spyware) dans la mesure où l'utilisateur est prévenu que le logiciel affichera des publicités.

- **Antivirus**: Logiciel permettant de détecter et de supprimer les virus informatiques sur n'importe quel type de stockage (disque dur, disquette, CD-ROM, etc.). Pour être efficace ce type de logiciel demande des mises à jour très fréquentes au cours desquelles il mémorise les nouvelles formes de virus en circulation.

- **Browser**: Programme utilisé pour explorer le Web. Les deux principaux browsers du marché : Internet Explorer (Microsoft) et Netscape Navigator (Netscape).

- **Firewall**: Un firewall est un système (sous forme de logiciel ou d'appareil) qui interdit l'accès de trafic non autorisé depuis et vers votre ordinateur ou votre réseau. Tous les messages de et vers Internet passent par le firewall qui scanne chaque information. Le firewall bloque les informations qui ne répondent pas aux critères de sécurité.

- **Lecteur de carte**: Le lecteur de carte est un module de sécurité permettant d'effectuer ses opérations bancaires à la bpost banque. Pour utiliser ce lecteur,

vous avez besoin d'un numéro d'utilisateur, de la carte bancaire bpost banque et du code PIN secret de la carte.

- **Phishing**: Le phishing, contraction des termes fishing (pêche) et phreaking (fraude informatique) est un terme désignant l'obtention d'informations confidentielles (comme les mots de passe ou d'autres informations privées), en se faisant passer auprès des victimes pour une personne digne de confiance ayant un besoin légitime de l'information demandée. Il s'agit d'une forme très dangereuse de spam. Les messages informent souvent les destinataires que leur compte pose problème et leur demandent de fournir, sur un site Web, des renseignements sur leur compte et sur eux-mêmes.

- **Spam**: signifie « un mail indésirable » en anglais. Ces messages sont envoyés en masse et contiennent généralement de messages commerciaux (des médicaments, paris, participation à des loteries). Les spams ont généralement un contenu illégal, trompeur et/ou nocif. L'expéditeur dissimule généralement son identité.

- **Spyware**: il s'agit d'un logiciel qui se niche dans votre ordinateur, vous espionne pendant que vous surfez sur Internet et vole vos données d'utilisateur. Le spyware se dissimule souvent dans les applications freeware ou shareware que vous téléchargez sur Internet. Le spyware peut scanner les fichiers sur le disque dur, installer d'autres spyware, lire les cookies, modifier votre page de démarrage Internet, etc. Le spyware est aussi capable de lire vos données confidentielles et de les envoyer à des escrocs d'Internet. Ceux-ci utilisent vos données pour vous envoyer des e-publicités non sollicitées (spam) ou ils revendent vos données à d'autres.

- **SSID**: il s'agit du nom de votre réseau Wifi qui est diffusé et qui identifie votre point d'accès à tous les ordinateurs sans fil.

- **Virus**: un virus informatique est un programme qui s'installe contre votre gré et à votre insu sur votre ordinateur. Il peut se cacher dans un fichier (attachment) - quel qu'il soit - que vous avez pris sur Internet. Un virus informatique se fixe sur un autre programme, il l'écrase ou le remplace par un autre programme. Il peut endommager votre matériel, supprimer des programmes, ralentir la vitesse de votre machine, etc…

- **Vishing**: contraction des termes Voice (voix/vocal) et Phishing (voir ci-dessus). Un appel téléphonique, généralement préenregistré, vous informe de mouvements inhabituels sur votre carte ou sur votre compte, probablement liés à une tentative de fraude et vous invite à rappeler un numéro de téléphone où vous devrez vous identifier en donnant des informations confidentielles.

- **Wifi**: Wireless Network = réseau sans fil...

Liens intéressants

En savoir plus sur les mails indésirables (Spam):
http://www.spamsquad.be/frl/home.html

Informations sur les programmes indésirables et conseils pour les éviter:
http://www.ibpt.be

- **Anti-virus:**
  Gratuits: Avast, Antivir,...
  Payants: BitDefender, Kaspersky, McAfee, Norton Symantec, Panda,...

- **Firewalls:**
  Gratuits: Zone alarm,...
  Payants: Norton,...

- **Programmes anti-spywares:**
  Gratuits: Adaware, Spybot,...
  Payants: Kaspersky,...

- Il existe également des **packages complets** anti-virus, firewalls, anti-spywares payants: BitDefender, McAfee, Norton Symantec,...