Sécurité

Le développement de nouveaux services en ligne facilite la vie quotidienne. Il est aujourd'hui possible d'effectuer aisément de nombreuses opérations. De plus, BCP Net est accessible via votre iPhone, iPad ou Smartphone Android. Néanmoins cela suppose un certain nombre de mesures à minima pour l'utilisation d'Internet sur un poste fixe ou nomade, dans de bonnes conditions de sécurité.

Lors de la conception de son site web, une des principales préoccupations de la Banque BCP a été la sécurité de l'information. À ce titre, nous avons opté pour des solutions d'authentification fortes. La Banque BCP a regroupé plusieurs informations dans les pages dédiées à la Sécurité. Nous avons volontairement pris les conseils mis à disposition par CASES Luxembourg – le Portail de la sécurité de l'information de l'État Luxembourgeois et vous conseillons de le consulter attentivement. Nous les avons organisés par rubriques pour une consultation rapide à tout instant. N'hésitez pas à les consulter avant toute transaction sur votre site transactionnel mis à disposition par votre Banque.

Facteurs d'une authentification

Authentification par quelque chose que vous savez : il s'agit généralement d'une authentification par mot de passe ou par code pin.
Un mot de passe peut facilement être copié à l'insu de l'utilisateur légitime. L'on peut se faire voler son mot de passe par exemple lors d'une attaque de type 'codes malicieux' ou 'phishing' ; en les sauvegardant sur un site web non sécurisé par SSL ; ou encore par le simple fait que quelqu'un regarde par-dessus votre épaule et note votre mot de passe lorsque vous l'inscrivez ('shoulder surfing').

Authentification par quelque chose que vous possédez : cette manière d'authentification se réalise généralement grâce à une clé permettant un accès physique à l'ordinateur.
Le niveau de sécurité de cette manière d'identification dépend de la facilité à faire des copies de l'outil concerné. Il est impossible de faire une copie d'une carte 'LuxTrust'. Les avantages d'un tel système d'authentification sont :

– la certitude d'avoir une carte non-reproductible ;
– trois essai erronés mènent au blocage de la carte ;
– lors d'une perte, la carte peut être révoquée et ne fonctionnera plus, même si le voleur est en possession du code PIN.

Ainsi, ne pas laisser inséré le 'signing stick' dans l'ordinateur si celui-ci n'est pas utilisé.
Authentification par quelque chose que vous êtes **:** il s'agit ici de l'authentification par empreinte digitale, ou encore la reconnaissance par la disposition de vos veines dans votre main ou l'image de votre rétine.

Les mots de passe

Il faut connaître le mot de passe pour pouvoir accéder aux ressources.
Le mot de passe est le plus souvent le seul garant de la sécurité d'un système et se doit d'être choisi avec le plus grand soin en respectant quelques critères simples.

Le courrier électronique

Le courrier électronique est un moyen de communication des plus appréciés.

Bien qu'il soit très utile et pratique, son utilisation et sa large diffusion à travers le globe en fait le médium de propagation de fichiers malveillants : vers, virus, chevaux de Troie, logiciels espion, canulars, spam, phishing, etc.

Vers, Virus, Chevaux de Troie
Faites attention aux malwares, c'est-à-dire aux programmes de type virus, vers, ou chevaux de Troie développés dans le but de nuire au fonctionnement normal d'un système et de porter atteinte à ses utilisateurs.

Spam
Le terme de « spam » est communément utilisé pour caractériser un courrier électronique non sollicité envoyé à une multitude de destinataires.
Ces courriers ne coûtent pratiquement rien à l'expéditeur, par contre, ils peuvent coûter très cher aux destinataires.

Hoax
Hoax signifie canular et correspond à de fausses nouvelles ou informations dont le but est d'être rapidement diffusées.
Les motivations sont différentes selon l'individu à l'origine de ces messages mais généralement le but est de parasiter la bande passante en multipliant les victimes.

Social engineering
Ingénierie sociale est une technique de piratage consistant à profiter de la crédulité d'un utilisateur afin de lui soutirer des informations confidentielles attenantes à un système d'information cible.

Protection des données
Il est recommandé d'éviter de disséminer des données personnelles, cela concerne spécialement le remplissage de formulaires sur le web.

Configuration du navigateur
Attention aux contenus dynamiques des pages Web. Ceux-ci peuvent représenter un danger pour la sécurité de vos informations.

Configuration du système
Configurez correctement votre ordinateur pour pouvoir en assurer la sécurité.

15 RÈGLES DE SÉCURITÉ POUR LES UTILISATEURS D'INTERNET

PROTEGEZ VOTRE ORDINATEUR

1. Installez un antivirus et faites une mise à jour régulière. Ne pas faire de mise à jour équivaut à ne pas avoir d'antivirus.
2. Utilisez un pare-feu (firewall) comme filtre pour le trafic internet de/vers votre ordinateur.
3. Soyez attentif aux mises à jour fournies par les éditeurs crédibles de logiciels et installez-les suivant les instructions.

PROTEGEZ VOTRE INFORMATION

4. Vérifier la provenance des logiciels via leurs certificats.
5. Éviter d'ouvrir les courriers électronique ou fichier dont le contenu semble anormal.
6. Se déconnecter systématiquement des sessions grâce aux liens proposés.
7. Utiliser la messagerie sécurisée BCP Net pour tout contact avec Banque BCP.
8. Reconnaître le site légitime de la Banque (cadenas navigateur, barre verte et certificat de la Banque).
9. N'accédez pas aux sites contenant d'informations personnelles, confidentielles ou sensibles, ou qui permettent d'effectuer des transactions bancaires, par des liaisons (links). Ecrivez toujours l'adresse du site directement sur la barre.
10. Ne donnez jamais d'informations confidentielles ou personnelles par mail, même si sollicitées par des sources apparemment fiables.
11. Ne donnez jamais d'informations personnelles ou confidentielles sans confirmer la fiabilité du site. Vérifiez que l'adresse du site commence par "https://" ("s" pour sécurité) suivie du nom du site, et que la page possède un cadenas sur la barre inférieure du navigateur (browser).
12. N'ouvrez pas les messages électroniques sans être sûr de l'identité de l'expéditeur et du contenu. Si vous doutez de l'origine du message, effacez-le immédiatement sans l'ouvrir.

NE VOUS LAISSEZ PAS TROMPER
13. Soyez toujours attentif aux demandes d'informations personnelles ou confidentielles pouvant être utilisées à votre insu (ex. : mot de passe, numéro d'identification, carte d'identité, numéro de compte …).

UTILISEZ VOS CODES D'ACCÈS AVEC SOIN
14. Facile à mémoriser mais difficile à deviner. N'utilisez pas de codes d'identification ou mots de passe faciles à identifier (par ex. : 111111 ; 123456 ; password).
15. Un bon mot de passe se compose au minimum de 10 signes. Il est recommandé d'utiliser un mélange de chiffres, de lettres majuscules et minuscules, ainsi que des signes de ponctuation. Mémorisez-les et ne les communiquez à personne.

10 RÈGLES DE CONDUITE POUR LES UTILISATEURS DE SMARTPHONES

- Faites des backups réguliers
- Chiffrez les données sensibles
- Utilisez des services cloud chiffrés et un mot de passe solide.
- Protégez le smartphone par un verrouillage de l'écran.
- Activez un programme de suivi pour la protection contre le vol
- Évitez des applications qui nécessitent un accès injustifié à des données privées et ne pas télécharger d'application hors des plateformes officielles
- N'envoyez pas d'informations sensibles sur un réseau WiFi public ou faiblement sécurisé
- Désactivez la connexion automatique WiFi.
- N'ouvrez pas sans réfléchir les fichiers qui vous sont envoyés, même s'ils proviennent d'un expéditeur connu.
- Ne vous laissez pas avoir par l'ingénierie sociale