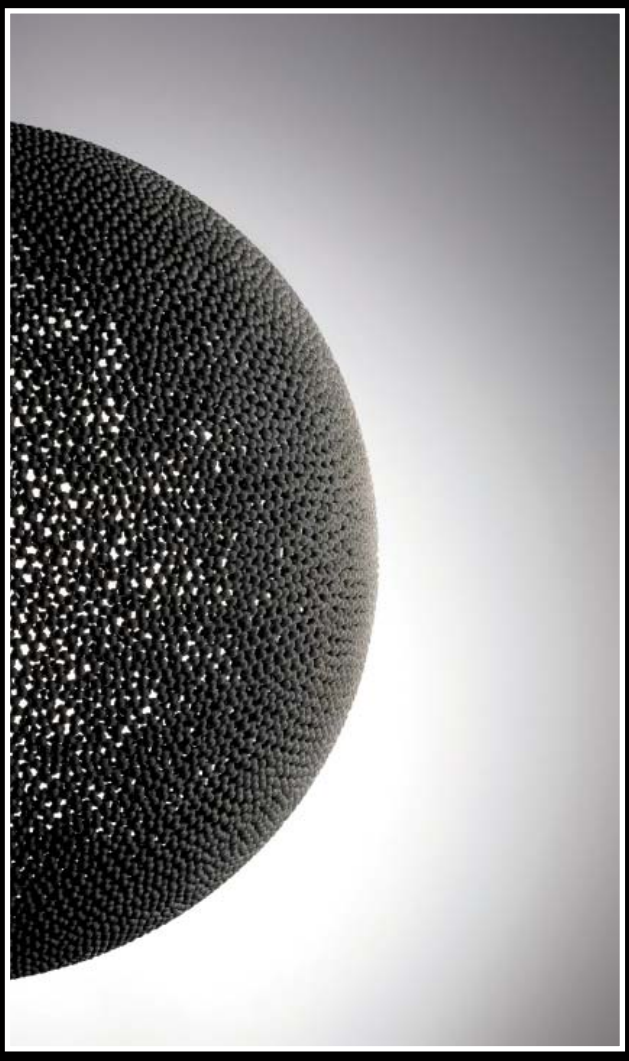
BANQUE NEUFLIZE OBC

LES BONNES PRATIQUES INTERNET ET MESSAGERIE



Neuflize OBC
ABN AMRO


VIRUS SPAM PHISH

Les risques informatiques aujourd'hui

L'environnement de la cybercriminalité est toujours en forte progression et continue à se professionnaliser. De ce fait, les tentatives de fraudes deviennent de plus en plus sophistiquées et ciblées. Aujourd'hui, les fraudeurs utilisent ou tentent d'utiliser divers moyens pour perpétrer leurs attaques : depuis un site Internet, par la messagerie depuis votre propre PC, ou même par téléphone.

Panorama des menaces existantes

> CE GUIDE A VOCATION À VOUS DONNER QUELQUES CONSEILS PRATIQUES DE SÉCURITÉ QUI, SANS ÊTRE EXHAUSTIFS, PERMETTENT DE SE PRÉMUNIR ET DE LIMITER LES RISQUES.

LES VIRUS

Un virus informatique est un programme malveillant qui détruit ou modifie certains fichiers indispensables au fonctionnement de l'ordinateur.
Certaines variantes, dénommées « spyware »[1], peuvent intercepter les caractères saisis au clavier, ce qui peut compromettre l'accès par internet à vos comptes bancaires, sites de vente en ligne et surtout les mots de passe d'accès. D'autres types de virus permettent également à un pirate de prendre le contrôle de l'ordinateur infecté et d'y effectuer toutes les opérations comme s'il était devant l'ordinateur.

LE « SPAM »

Ce terme désigne tout courrier électronique non sollicité. Ces courriers cachent souvent des pièges et tentatives d'actes frauduleux à travers des offres proposant des réductions, bénéfices et gains en tous genres. Lorsque vous avez reçu un spam, détruisez-le tout simplement. Ne jamais répondre à un spam pour se désinscrire, car cela confirmerait à l'émetteur que l'adresse est valide et vous seriez alors de plus en plus sollicité.

LE « PHISHING »

C'est une pratique malveillante actuellement en très forte augmentation, qui est destinée à collecter des codes d'accès à des sites bancaires ou de ventes en ligne. Les fraudeurs se font passer pour une entreprise ou une banque. Ils vous envoient un e-mail ou un SMS vous conduisant vers un faux site Internet dont le design est souvent très proche, afin de vous inciter à saisir vos codes d'accès. Dans le passé ces mails étaient souvent rédigés en français approximatif, mais la qualité du contenu progresse très fortement.

LE « SOCIAL ENGINEERING »

C'est un appel téléphonique que vous recevez, se prétendant par exemple de la Banque, vous demandant de lui communiquer des informations relatives à votre compte, code d'accès ou tout type d'informations similaires…

1) Un logiciel espion (en anglais spyware) est un logiciel malveillant dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur ne puisse s'en rendre compte.

Conseils pratiques

SÉCURISATION DE VOTRE ORDINATEUR PERSONNEL

Les principes décrits ci-dessous sont importants pour maintenir un niveau de sécurité correct au regard des menaces les plus couramment rencontrées, sans toutefois pouvoir garantir un niveau de sécurité absolu.

Les 4 règles d'or

1. Un logiciel anti-virus qui doit être mis à jour tous les jours. Il est préférable de prendre un logiciel reconnu sur le marché.
2. Un logiciel « firewall »[2] qui peut être activé une fois pour toutes, lors de la configuration initiale de l'ordinateur.
3. Un logiciel « anti-spyware »[3] qui vous protège en complément contre la plupart des logiciels espions.
4. Un filtre anti-spam qui permettra de réduire au minimum les e-mails non sollicités. Cet outil est souvent proposé, en option, par votre fournisseur d'accès.

- Définir un mot de passe au démarrage lors de la connexion de l'ordinateur.
- Mettre à jour régulièrement le système d'exploitation, ceci peut être paramétré automatiquement dans la configuration du système qui est en général proposé lors de l'installation initiale de l'ordinateur. Il est également important d'appliquer les mises à jour sans tarder lorsque le système d'exploitation les signale.
- En cas de revente de l'ordinateur, il est très important de supprimer soigneusement l'ensemble des données contenues dans celui-ci.
- Faire régulièrement une sauvegarde de vos données sur un ou deux disques externes à stocker en un lieu différent de l'ordinateur.
- Ne jamais connecter une clé USB qui a été « trouvée », c'est une nouvelle tendance pour infecter les ordinateurs avec des virus.
- Le site : http://www.securite-informatique.gouv.fr donne des conseils complémentaires qui sont régulièrement actualisés.

2) Un pare-feu ou firewall (en anglais) est un logiciel permettant de surveiller les connexions sur un ordinateur et d'éviter les intrusions
3) Un logiciel anti spyware est un logiciel complémentaire à l'antivirus, spécialisé dans la détection de cette menace.

CONFIGURATION DE L'ACCÈS À INTERNET :

A domicile, lors de la mise en œuvre du boîtier de connexion ADSL à Internet, il est important de se renseigner auprès de votre fournisseur d'accès pour qu'une configuration sécurisée soit mise en œuvre.
Tous les fournisseurs d'accès expliquent comment procéder à cette configuration sécurisée qui n'est en général pas proposée lors de l'installation.
A défaut, votre accès Internet pourrait être utilisé de manière malveillante et vous seriez tenu pour responsable de cette utilisation. L'intrusion est la plupart du temps invisible et il serait très difficile de la déceler.

NAVIGATION SUR INTERNET

Mots de passe :

De manière générale, il est très important de ne pas utiliser de mots de passe faciles à deviner, et surtout d'avoir des mots de passe **différents** suivant les sites sur lesquels vous vous connectez.

UTILISATION DES POINTS D'ACCÈS WIFI PUBLICS

Nous vous **déconseillons** d'utiliser les accès Wifi publics gratuits ou payants, par exemple depuis un cybercafé, une gare ou un aéroport, pour la connexion aux sites de banque ou de vente en ligne.

Ces points d'accès peuvent être mal paramétrés et notamment conserver les codes d'accès ainsi que l'historique des sites sur lesquels vous venez de vous connecter. Une personne passant derrière vous pourrait accéder à ces mêmes sites avec vos identifiants.

UN EXEMPLE DE RÈGLES DE DÉFINITION DE MOTS DE PASSE

Par exemple : un mot de passe facile à retenir mais difficile à deviner. Les règles de base à suivre:

- Au moins **8** caractères ;
- Mélanger les chiffres, majuscules, minuscules et caractères spéciaux ou lettres accentuées ;
- Pas de mots du dictionnaire (français ou étranger), nom de famille, etc ;
- Utiliser un mot de passe différent selon les sites.

En complément, nous recommandons de ne jamais stocker vos mots de passe dans le navigateur Internet et de s'astreindre à les ressaisir lors de l'accès aux sites.

Les 5 règles d'or

1. Envoyez vos messages uniquement à des personnes dont vous avez connaissance : amis, famille, fournisseurs...

2. Sur la réception de mail, vérifiez que le correspondant est bien une personne connue et que l'intitulé du mail reçu est habituel de la part de votre correspondant.

3. Sur un mail non sollicité, soyez très prudent sur l'utilisation des liens inclus dans ce mail ou sur les pièces jointes. En cas de doute n'ouvrez pas le mail et détruisez le tout simplement.

4. Ne communiquez jamais par mail de coordonnées bancaires, carte bancaire...

5. De la même manière n'envoyez pas de demandes d'ordre de bourse ou de virements par mail. Internet ne garantit aucunement le délai d'acheminement et les mails peuvent être facilement falsifiés ou interceptés.

MESSAGERIE PERSONNELLE

Il est important de respecter quelques règles simples au quotidien pour réduire le risque de recevoir un e-mail susceptible de vous induire en erreur.

La sécurité de votre messagerie personnelle (orange, gmail, yahoo...) devient de plus en plus critique, car c'est via cette messagerie que seront renvoyés les mots de passe oubliés sur les sites de ventes en ligne.

La compromission de cette messagerie peut conduire à l'utilisation abusive de vos identifiants pour des achats, ou à l'accès à vos informations privées (correspondance avec votre banquier ou vos proches par exemple…).

L'accès à votre messagerie personnelle doit être correctement protégé, notamment par un **mot de passe spécifique** et non trivial, et qui ne doit jamais être communiqué.

REMARQUE IMPORTANTE :

ASSOCIÉES AU COMPTE DE MESSAGERIE, IL Y A FRÉQUEMMENT UNE OU PLUSIEURS « QUESTIONS DE SÉCURITÉ ». CES QUESTIONS SONT SOUVENT UTILISÉES POUR POUVOIR RÉINITIALISER L' ACCÈS À CETTE MESSAGERIE.

IL FAUT ÉVITER D'UTILISER DES INFORMATIONS RELATIVES À NOS PROCHES OU TRIVIALES ET QUI PEUVENT AVOIR ÉTÉ PUBLIÉES SUR LES RÉSEAUX SOCIAUX, CE QUI FACILITE GRANDEMENT LE TRAVAIL DES FRAUDEURS.

Sites bancaires ou de ventes en ligne

Il est recommandé de saisir manuellement le nom des sites de banque en ligne ou d'achats à distance, puis de les mémoriser dans les favoris. Cela permet de se prémunir du phénomène de « Phishing », par lequel un pirate vous envoie un mail qui vous incite à cliquer sur un lien pointant vers un site très ressemblant en reprenant le design du site visé.

Pour tout paiement en ligne ou transaction sur un site bancaire, il est très important de vérifier systématiquement les 3 règles suivantes :

Les 3 règles d'or

1. Vérifiez la présence du cadenas dans le navigateur confirmant que la session est sécurisée.
2. Vérifiez que votre session est bien sécurisée en « https » qui doit être affiché avant le nom du site.
3. Une fois les transactions terminées, déconnectez-vous du site, avant de fermer le navigateur.

SERVICE PAYWEBCARD

Nous recommandons l'utilisation des numéros de cartes bancaires temporaires qui sont mis en œuvre avec le service Paywebcard que la Banque met à votre disposition. Il permet de sécuriser le règlement d'achats à distance auprès de commerçants ou prestataires de services, par carte bancaire par le biais d'internet au moyen de la fourniture d'un ou de plusieurs e-numéros. Un numéro vous est attribué pour une utilisation unique, ce qui évite toute réutilisation ultérieure et tout risque de détournement si le numéro est conservé sur le site marchand, ce qui arrive parfois, sans même que vous en soyez informé.

SERVICE 3D SECURE

Appelés « Verified by Visa » et « MasterCard SecureCode », ces programmes mondiaux ont été développés afin d'authentifier le titulaire de la carte bancaire lors d'un paiement en ligne.

A chaque paiement effectué sur un site internet affilié 3D Secure, la procédure d'autorisation financière classique est couplée à une authentification du titulaire de la carte bancaire avant validation de l'opération. Lorsque la transaction est effectuée sur un site marchand non affilié, le paiement s'effectue sans cette phase d'authentification.

Pour les titulaires d'une carte bancaire Neuflize OBC, l'identifiant personnel permettant cette authentification est un code dynamique, à usage unique, envoyé par SMS ou message vocal vers le numéro de téléphone indiqué préalablement.

Ci-dessous l'exemple de notre site correctement sécurisé.
Les paramètres sont encadrés en rouge.

En complément, assurez-vous que le certificat du site est valide. Dans le cas de notre site de banque en ligne, en cliquant sur le bandeau du cadenas (indiquant Banque Neuflize OBC), on obtient le message suivant (il peut varier en fonction du navigateur utilisé) :

Nous vous recommandons également de ne pas utiliser de manière simultanée les autres onglets de votre navigateur et d'éviter d'utiliser les options de frappe prédictives des sites dans l'explorateur.

On commence à rencontrer des sites frauduleux qui « changent » la page masquée alors que vous êtes sur un autre onglet du navigateur et qui lors du retour sur cet onglet vous redemande le mot de passe alors que vous étiez déjà connecté.

Dans ce cas de figure, il faut absolument revérifier avec attention le nom complet du site avant toute chose !

A l'opposé, il ne faut surtout pas se connecter à un site, si le message suivant s'affiche :

Réseaux sociaux

> IL FAUT ETRE CIRCONSPECT LORS DES PRISES DE CONTACT PAR DES PERSONNES INCONNUES.

Ces nouveaux outils sont en phase de très forte expansion, ils peuvent être utilisés à titre professionnel (Linkedin, Viadéo…) ou personnel (Facebook, Twitter, Google+…).

De manière générale, il faut être très prudent sur les informations que vous publiez sur ces sites, car de nombreux détails personnels anodins peuvent permettre à une personne mal intentionnée de compiler la multitude d'informations diffusées, et de retrouver finalement des informations très complètes. Un exemple assez courant est d'annoncer son départ en vacances à ses contacts, ce qui peut être une information utile pour des personnes mal intentionnées et connaissant l'adresse de résidence.

Il faut être conscient qu'il est très difficile d'effacer ce qui a été écrit sur les réseaux sociaux et qu'il est impossible de savoir à qui les informations diffusées ont été transmises.
Lors de la création des comptes, il faut activer les options de confidentialité disponibles pour limiter l'accès des informations à ses correspondants habituels et reconnus.

TÉLÉPHONES **PORTABLES**

Si vous recevez un appel téléphonique, émanant prétendument de la Banque, vous demandant de lui communiquer des informations relatives à votre compte, code d'accès[5], ou tout type d'informations approchantes, n'y répondez pas. Notez le numéro le cas échéant s'il apparaît et prenez immédiatement contact avec votre banquier.

Au-delà des aspects usuels de communication, nous vous recommandons la plus grande prudence lors de la réception de SMS d'origine inconnue, demandant de rappeler des numéros, qui sont le plus souvent surtaxés. Le phénomène est tout à fait comparable aux aspects de « spam » que nous rencontrons dans les mails.

Lors de l'activation de la fonction « bluetooth », le plus souvent pour connecter une oreillette, il est important de définir un code d'accès ou de configurer un mode « masqué », car sinon il devient relativement simple d'accéder à vos contacts téléphoniques depuis un autre téléphone.

L'évolution technologique aidant, les téléphones mobiles deviennent des smartphones disposant de fonctionnalités d'un ordinateur à part entière, avec notamment la capacité à naviguer sur Internet et donc l'ensemble des risques déjà décrits auparavant. Les mêmes principes de vigilance sont à appliquer.

5) En particulier, la Banque ne vous appellera jamais pour effectuer des tests sur votre carte d'accès à son site de banque en ligne. Conservez donc secret les codes qui s'affichent sur le lecteur.

LIMITES DE
RESPONSABILITÉS

Cette brochure est destinée à vous informer sur les risques liés à l'utilisation de l'internet, à vous aider à mieux vous protéger contre la fraude, le vol ou le détournement de vos données personnelles et à lutter contre les virus informatiques ou contre les tentatives d'intrusion dans vos moyens de communication.

Cependant, en raison de l'évolution permanente des techniques de piratage et des modes de diffusion de vos données personnelles, les informations et les conseils formulés dans ce document ne peuvent prétendre vous garantir une sécurité absolue, la Banque Neuflize OBC ne pouvant être tenue responsable de quelque manière que ce soit à cet égard.

SA à directoire et conseil de surveillance au capital
de 383 507 453 euros.
Siège social : 3 avenue Hoche- 75008 Paris
552 003 261 RCS Paris - numéro ORIAS : 07025 717
Agréée en tant qu'établissement de crédit par le
CECEI, 31 rue Croix des Petits Champs - 75001 PARIS
Téléphone : + 33 (1) 56 21 70 00
Carte professionnelle « Transactions sur immeubles et fonds
de commerce » n° T14364 ; engagement de non détention
de fonds, absence de garantie financière.

www.neuflizeobc.fr

Conception et réalisation : Corinne Bourassine - février 2012