Portzamparc

Sécurité

Site internet

Internet offre aujourd'hui un formidable **espace de liberté** et de services. Pour en profiter pleinement, il ne faut pas oublier que **fraude et piratage** peuvent également être d'actualité.

Sommaire

1. Bien connaître les risques pour mieux se protéger

1.1 Accès à votre compte

La **sécurité** de votre compte est primordiale pour nous, mais c'est ensemble que nous devons l'assurer. En effet, quelques **gestes simples** de votre part suffisent pour s'assurer que vous ne serez pas le maillon faible.

1.1.1 Mots de passe

Votre mot de passe est la porte d'entrée vers vos comptes Portzamparc. Il s'agit d'une information très sensible qui doit rester **secrète** !

Voici quelques conseils pour vous assurer un mot de passe efficace :

- **Lors de l'ouverture de votre compte**

- Lors de l'ouverture de votre compte Portzamparc, un mot de passe temporaire vous est délivré, il doit impérativement être modifié dès votre première connexion,

- par la suite, nous vous recommandons fortement de le changer le plus régulièrement possible, au maximum tous les six mois.

- **Règles de création du mot de passe**

- Il doit être composé d'au moins 6 caractères (nous vous recommandons néanmoins 8 caractères ou plus), à la fois avec des caractères alphabétiques minuscules et majuscules (aAbBcCdD…), numériques (0123456789) et des caractères spéciaux (!"#$%&'()*+-./ ;<=> ?@[]_{|}).

- Évitez les prénoms, dates de naissance, et de manière générale tout ce qui peut s'apparenter à des informations personnelles,

- Privilégiez un mot de passe dédié à votre compte Portzamparc, que vous n'utiliserez pas pour une autre application (réseau social, boîte de messagerie électronique…).

- **En cas de doute ?**

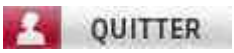
Si vous avez le moindre doute sur l'intégrité de votre mot de passe, changez-le immédiatement !

1.1.2 Déconnexion

Dès que vous n'utilisez plus les services de Portzamparc, il est indispensable de mettre fin à votre session en vous déconnectant, surtout si vous naviguez depuis un ordinateur public. Le risque est qu'un individu puisse retourner sur votre session sans avoir à connaître vos identifiants.

- **Déconnexion manuelle**

Ainsi, cliquez systématiquement sur le bouton « Quitter » avant de fermer votre navigateur :



Il sera alors impossible de se connecter à votre Espace Client sans saisir vos identifiants à nouveau.

- **Déconnexion automatique**

Pour votre sécurité, vous serez automatiquement déconnecté après 60 minutes d'inactivité sur votre compte. Il est donc normal dans cette situation qu'on vous demande à nouveau de vous authentifier afin de poursuivre votre navigation sur votre Espace Client.

1.1.3 Veille sur vos mouvements

À chaque connexion sur votre Espace Client, pensez à contrôler les derniers mouvements effectués sur l'ensemble de vos comptes afin de déterminer si vous en êtes à l'origine.

En cas de mouvement suspect, joignez immédiatement votre Conseiller Portzamparc pour l'informer de la situation.

1.1.4 Diffusion des infos

Vous êtes responsable de vos identifiants Portzamparc, notamment votre mot de passe qui doit rester **secret** en toutes circonstances !

- **Votre mot de passe ne concerne que vous !**

- Ne divulguez **jamais** votre mot de passe à personne.

- Un conseiller Portzamparc ne vous demandera jamais de lui communiquer votre mot de passe, que ce soit par mail ou par téléphone. Si tel était le cas, vous pourriez être victime d'une tentative de fraude : ne donnez surtout pas suite à cette demande et contactez sans tarder votre Conseiller Portzamparc pour l'en informer,

- De préférence, ne le gardez pas en mémoire dans votre navigateur internet si ce dernier vous le propose.

- **Une vigilance à tout moment**

Méfiez-vous des informations qui peuvent circuler sur internet ! La plupart des transferts se font en clair, c'est-à-dire qu'ils peuvent être interceptés par tous. Ainsi, ne communiquez jamais d'informations confidentielles par mail ou sur des réseaux sociaux.

Plus généralement, toute information personnelle peut être utilisée par un individu mal intentionné pour tenter de découvrir votre mot de passe. Prudence donc.

1.2 Protection de votre ordinateur

Votre ordinateur, c'est votre outil pour vous connecter à vos comptes Portzamparc. Et si l'outil n'est pas bon, la sécurité ne pourra pas être assurée. **Nos conseils** sont là pour vous guider dans l'obtention d'un **ordinateur sécurisé**

Gardez bien à l'esprit que votre niveau de sécurité est celui de votre maillon faible : un seul élément fragile peut faire tomber toute l'architecture.

1.2.1 Système d'exploitation

- **Le principe**

Comme tout logiciel, votre système d'exploitation est vulnérable : des failles de sécurité peuvent être découvertes par les créateurs ou des pirates informatiques, et leur exploitation peut permettre à ces derniers de prendre le contrôle de votre poste. Par conséquent, à chaque nouvelle menace identifiée, les développeurs apportent un patch de sécurité.

Il doit donc absolument être mis à jour pour assurer que tous les correctifs de sécurité soient implémentés sur votre ordinateur.

- **Et en pratique ?**

Pour mettre à jour votre système d'exploitation, les sites suivants pourront vous renseigner, en fonction de votre produit :

- Windows : **WindowsUpdate.com**
- Mac OS : **Apple Support**

Pour les possesseurs de système Linux, reportez-vous à l'aide en ligne de votre distribution.

- **À retenir :**

Nous vous conseillons très vivement de ne pas vous connecter à votre espace client Portzamparc avant d'avoir consciencieusement vérifié que votre système d'exploitation est à jour.

1.2.2. Anti-virus

- **Le principe**

Un anti-virus est un logiciel indispensable pour vous protéger des menaces qui vous guettent durant votre navigation sur internet. Il reconnaît, grâce à sa base de signatures, et stoppe les virus et vers (voir définition dans la partie « Dangers d'internet ») avant qu'ils ne puissent agir sur votre ordinateur, en le bloquant, prenant le contrôle de celui-ci ou détruisant vos fichiers.

Pour qu'il soit efficace, il faut que l'anti-virus puisse reconnaître la menace en mettant à jour sa « watchlist », ou base de signatures. Ainsi, mettre à jour son anti-virus est absolument indispensable sous peine d'avoir un logiciel inutile !

- **Et en pratique ?**

Dans un premier temps, vous procurer un anti-virus est fondamental : il existe des solutions payantes disponibles directement en téléchargement ou en magasin, mais aussi des solutions gratuites. À vous de

choisir celui qui vous convient le mieux !

Une fois votre anti-virus installé, il faut le configurer pour qu'il effectue les trois tâches suivantes :

- Analyser en permanence les programmes que vous exécutez,

- Effectuer périodiquement un scan de tous les fichiers de votre ordinateur afin de détecter les fichiers infectés et les détruire,

- Se mettre à jour automatiquement, avec la plus grande périodicité possible (nous recommandons une mise à jour journalière).

- **À retenir :**

Nous vous conseillons très vivement de ne pas vous connecter à votre espace client Portzamparc avant d'avoir consciencieusement vérifié que votre anti-virus est fonctionnel et mis à jour.

1.2.3 Pare-feu

- **Le principe**

Un pare-feu (firewall en anglais) est un logiciel qui vous permet de contrôler les échanges de données entre votre ordinateur et internet, vous protégeant de l'exécution d'opérations non souhaitées.

- **Et en pratique ?**

Il existe plusieurs solutions pour se procurer un pare-feu : celui de votre système d'exploitation (pensez à l'activer !), de votre fournisseur d'accès à internet (rendez-vous sur son site web pour plus d'informations) ou un autre de votre choix que vous pouvez télécharger et installer sur votre machine. Certains sont gratuits.

Tout comme l'anti-virus, le pare-feu a besoin d'être mis à jour pour rester efficace en détectant les nouvelles menaces découvertes. Ainsi, nous vous recommandons d'activer les mises à jour automatiques, qui se lanceront à chaque démarrage de votre ordinateur. Si c'est impossible, consultez le plus souvent possible le site de l'éditeur pour rester informé des mises à jour disponibles.

- **À retenir :**

Nous vous conseillons très vivement de ne pas vous connecter à votre espace client Portzamparc avant d'avoir consciencieusement vérifié que votre pare-feu est fonctionnel et mis à jour.

1.2.4 Navigateur internet

- **Le principe**

Le navigateur internet est le logiciel installé sur votre poste pour visualiser les pages des sites internet. Les plus utilisés sont actuellement : Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opéra. Certains sont installés de base avec votre système d'exploitation, mais vous pouvez installer un ou plusieurs autres selon votre préférence.

- **Et en pratique ?**

- En termes de sécurité, il n'y a pas de navigateur particulier à privilégier. Vous devez toutefois toujours veiller à ce qu'il soit mis à jour ! En effet, comme tout logiciel, des failles peuvent être exploitées par des individus malhonnêtes, et les conséquences sur votre ordinateur peuvent être terribles : vol de vos informations, prise de contrôle de votre poste, destruction de vos fichiers…

- De plus, les navigateurs à jour proposent des modules de sécurité qui peuvent vous protéger contre les sites qui présentent des risques de phishing ou d'infection par un virus.

- Les navigateurs conservent souvent dans leur cache ou dans un trousseau des données telles que votre historique de navigation, vos mots de passe, vos sessions ouvertes ou encore des cookies (de petits fichiers qui vous assurent une navigation plus rapide). Pensez à vider ce cache régulièrement car ils sont une mine d'informations sur votre navigation. Vous pourrez trouver la démarche à suivre dans l'aide de votre logiciel.

- **À retenir :**

Nous vous conseillons très vivement de ne pas vous connecter à votre espace client Portzamparc avant d'avoir consciencieusement vérifié que votre navigateur internet est à jour.

1.2.5 Wifi

- **Le principe**

Il existe deux façons de relier votre ordinateur à internet : par un câble Ethernet ou sans fil, c'est-à-dire par le réseau Wifi. Le principal inconvénient de ce dernier est qu'il fait transiter les informations par des ondes radios sur plusieurs centaines de mètres autour de votre équipement. Il faut se faire à l'idée qu'un réseau Wifi est par nature difficile à sécuriser et que les mesures suivantes vont vous prémunir contre les risques les plus répandus. Pour vous assurer une sécurité optimale de vos transferts de données, nous vous recommandons de privilégier les connexions à fils.

- **Et en pratique ?**

- Au niveau du routeur : pensez à changer rapidement le mot de passe qui vous a été donné par votre fournisseur d'accès. Ce sont souvent les mêmes sur les mêmes modèles. Il est donc très simple de s'y connecter et d'écouter vos transferts de données. De plus, modifiez le nom de votre réseau afin qu'on ne puisse pas vous identifier formellement et désactiver sa diffusion. Ainsi, les appareils qui se trouvent dans sa zone d'émission ne pourront pas le détecter.

- Au niveau de la transmission de données : cryptez votre connexion en utilisant le protocole WPA ou WPA2 (nous déconseillons le WEP qui n'est plus suffisamment sécurisé). Enfin, pour être sûr que seuls vos appareils pourront se connecter à votre réseau, activez l'authentification par adresse MAC (voir le Lexique pour la définition d'une adresse MAC).

Pour effectuer toutes ces opérations, consultez le manuel utilisateur de votre routeur.

- **À retenir :**

Nous vous conseillons très vivement de ne pas vous connecter à votre espace client Portzamparc avant d'avoir consciencieusement vérifié que votre réseau Wifi est pleinement sécurisé.

1.3 Danger sur Internet

Internet est à la fois un outil formidable et une source inépuisable de dangers pour vos données personnelles. Voici **une liste des risques** qui vous guettent et nos **recommandations** pour naviguer sereinement !

1.3.1 Phising

- **De quoi s'agit-il ?**

Le phishing, appelé filoutage en français ou encore hameçonnage en québécois, est une technique qui consiste à dérober des informations confidentielles en abusant de votre crédulité.

Le plus souvent, une tentative de phishing se présente sous la forme d'un mail que vous recevez de la part d'un expéditeur qui se fait passer pour Portzamparc , en reprenant sa charte graphique et ses logos, pour vous faire cliquer sur un lien contenu dans le message. Ce lien, au lieu de vous diriger vers le véritable site de Portzamparc, vous connecte à un site pirate et vous invite à fournir vos informations confidentielles, telles que vos mots de passe, numéros de compte, numéros de carte bleue etc… Les pirates récupèrent ainsi ces informations pour les utiliser de façon frauduleuse.

- **Comment s'en prémunir ?**

- Lorsque vous recevez un mail prétendument envoyé par Portzamparc qui vous invite, pour quelque raison que ce soit, à vous connecter sur son site, ne cliquez pas sur le lien inclus dans le message, mais rendez-vous plutôt sur le site en tapant l'adresse habituelle dans votre navigateur.

- Si la forme du mail vous semble anormale : des fautes d'orthographe, tournures de phrases insolites, caractères issus d'alphabets étrangers, problèmes d'images qui ne s'affichent pas, demande urgente de renseignements confidentiels, c'est que vous êtes face à une tentative de phishing. De façon générale, Portzamparc ne vous demandera jamais par mail ou par téléphone des informations confidentielles.

- Vérifiez toujours que vous êtes sur le véritable site de Portzamparc , en notant l'adresse exacte et la présence du cadenas de sécurité :

Attention ! La présence du cadenas n'implique pas avec certitude que vous êtes sur un site sécurisé ! L'emplacement de celui-ci est très important. En effet, sur l'image ci-dessus, il aurait suffi à un individu mal intentionné de remplacer l'image à gauche de l'adresse par celle d'un cadenas pour essayer de vous tromper. Or, sur Internet Explorer, le cadenas est à droite (entouré en rouge). Renseignez-vous sur les spécificités de votre navigateur internet, et notamment l'emplacement du cadenas.

- Utilisez les fonctions anti-phishing de votre navigateur : ce module parfois implémenté vous informe que le site sur lequel vous vous rendez a déjà été détecté comme un site contrefait. Si une telle alerte apparaît, quittez immédiatement la page que vous tentiez d'afficher.

- **Que faire si c'est trop tard ?**

- Si vous avez fourni vos codes d'accès (identifiant et mot de passe) à un site contrefait suite à une tentative de phishing, appelez immédiatement votre conseiller pour l'informer de la situation et voir avec lui la procédure à suivre. Si vous êtes dans l'incapacité de le faire, changez impérativement votre mot de passe sur votre espace client.

- Pensez à contrôler les derniers mouvements effectués sur l'ensemble de vos comptes afin de déterminer si vous en êtes à l'origine. En cas de mouvement suspect, joignez immédiatement votre Conseiller Portzamparc pour l'informer de la situation.

- **À retenir**

- Portzamparc ne vous demandera jamais par mail ou par téléphone des informations confidentielles.

- Si un mail vous demande de fournir vos codes d'accès, ne cliquez surtout pas sur le lien inclus dans le message, et supprimez-le.

1.3.2 Virus/Vers

- **De quoi s'agit-il ?**

Les virus et les vers sont plus généralement des malwares, ou logiciels malicieux en français. Les moyens d'infection de votre ordinateur sont très nombreux :

- Navigation sur des sites douteux,

- Connexion à internet avec un ordinateur dont les système d'exploitation, navigateur, anti-virus et pare-feu ne sont pas mis à jour régulièrement,

- Ouverture d'un programme infecté (notamment les .exe téléchargés sur internet),

- Connexion de périphériques amovibles infectés (clé USB, disquette, CD, DVD de données).

Une fois sur votre poste, les virus et les vers vont se mettre en fonctionnement de façon totalement invisible pour vous, parfois après une longue période d'inactivité. Leurs effets sont nombreux : prise de contrôle de votre ordinateur, vol de données confidentielles, envoi de mails non désirés (spams), chantage par la paralysie de votre système d'exploitation, destruction de tous vos fichiers, diffusion de messages publicitaires etc…

- **Comment s'en prémunir ?**

- Il n'existe malheureusement pas de protection absolue contre les virus et les vers, puisque ceux-ci évoluent en permanence. Ainsi, il est indispensable de posséder un anti-virus et un pare-feu à la fois fonctionnels et mis à jour le plus régulièrement possible. De plus, mettez à jour votre système d'exploitation et votre navigateur internet.

- De façon générale, ne vous rendez pas sur des sites qui ne vous inspirent pas confiance, n'ouvrez des pièces jointes de mail que si vous êtes sûr de leur expéditeur et de leur contenu. Si vous avez téléchargé un programme, scannez-le à l'aide de votre anti-virus avant de l'exécuter.

- Pensez à contrôler les derniers mouvements effectués sur l'ensemble de vos comptes afin de déterminer si vous en êtes à l'origine. En cas de mouvement suspect, joignez immédiatement votre Conseiller Portzamparc pour l'informer de la situation.

- **Que faire si c'est trop tard ?**

Si vous êtes victime de l'un des nombreux effets indésirables énoncés ci-dessus, vous êtes très certainement infecté par un virus informatique ou un ver. Dans ce cas,

- Ne vous rendez surtout pas sur votre espace client Portzamparc ! En effet, le logiciel malicieux pourrait vous dérober vos informations confidentielles et les transmettre à un individu mal intentionné.

- Si vous l'avez déjà fait, appelez immédiatement votre conseiller pour l'informer de la situation et voir avec lui la procédure à suivre.- Après avoir scanné votre ordinateur avec votre anti-virus et détruit le fichier infecté, vous pourrez changer de mot de passe.

- Surveillez très régulièrement les mouvements sur votre compte pour vérifier qu'aucune opération suspecte n'a été engagée. Si tel était le cas, contactez immédiatement votre conseiller Portzamparc.

- **À retenir**

- Ne naviguez sur internet que si vous possédez un système d'exploitation, un navigateur internet, un

anti-virus et un pare-feu à jour,

- Ne vous rendez pas sur des sites qui vous semblent suspects,

- Téléchargez des programmes ou des pièces jointes de mails uniquement si vous êtes certain de leur contenu. Dans le cas contraire, scannez-les avec votre anti-virus avant de les exécuter.

1.3.3 Spam

- **De quoi s'agit-il ?**

Les spams, ou pourriels en français, sont des messages électroniques non sollicités. Leurs buts sont variés :

- vanter les mérites d'un produit, souvent de luxe ou de cosmétique, et la plupart du temps contrefait,

- vous apporter de fausses informations (hoax en anglais) ou des histoires touchantes pour vous demander ensuite des financements ou de transférer le mail à tous vos contacts,

- vous diriger vers un site contrefait qui vous demande des informations confidentielles (voir phishing),

- vous faire télécharger une pièce jointe, infectée par un virus.

- **Comment s'en prémunir ?**

- La première des protections est de ne transmettre son adresse mail qu'à votre entourage et aux sites de confiance. En effet, c'est lorsque vous l'écrivez en clair sur un site (un forum ou une petite annonce par exemple) qu'elle peut se retrouver détectée par un robot dont le but est de créer les listes de diffusion de spams.

- Les services de boîte mails (outlook, gmail, hotmail…) incluent de plus en plus des protections très efficaces contre le spam. De plus, si vous recevez un message que vous n'avez pas sollicité, vous pouvez le spécifier et les prochains mails de cet expéditeur iront directement dans votre dossier « spams ».

- **Que faire si c'est trop tard ?**

- Les spams sont la plupart du temps très facilement identifiables : expéditeur inconnu, fautes d'orthographe ou langue anglaise, publicité pour un produit. Ainsi, lisez toujours l'objet de vos courriels avant de les ouvrir, et supprimez directement les spams. En effet, les ouvrir pourrait installer un virus sur votre ordinateur !

- La plupart du temps, il existe un lien en bas du mail pour « se désinscrire de la liste de diffusion » ou « se désabonner ». Si vous connaissez l'expéditeur du courriel, vous pouvez cliquer sur ce lien. Si ce n'est pas le cas, ne cliquez surtout pas ! En effet, ceci validerait définitivement l'existence de votre adresse de messagerie et vous recevriez encore plus de spams !

- **À retenir**

- N'écrivez pas votre adresse mail en clair sur un site auquel vous ne faîtes pas confiance,

- En cas de réception d'un spam dans votre boîte mail, supprimez-le sans l'ouvrir.

1.3.4 Spyware

- **De quoi s'agit-il ?**

Un spyware, ou logiciel espion, est un malware dont le but est de collecter et transmettre toutes vos informations confidentielles à des tiers, souvent des individus mal intentionnés qui ont l'intention de les utiliser à votre insu ou de les revendre. Il s'installe de façon invisible sur votre ordinateur, et peut rester en sommeil un certain temps avant d'agir contre vous. Vous verrez alors des fenêtres publicitaires s'ouvrir à votre insu sur votre écran d'ordinateur.

- **Comment s'en prémunir ?**

- Il n'existe malheureusement pas de protection absolue contre les spywares, puisque ceux-ci évoluent en permanence. Ainsi, il est indispensable de posséder un anti-virus et un pare-feu à la fois fonctionnels et mis à jour le plus régulièrement possible. De plus, mettez à jour votre système d'exploitation et votre navigateur internet.

- De façon générale, ne vous rendez pas sur des sites qui ne vous inspirent pas confiance, n'ouvrez des pièces jointes de mail que si vous êtes sûr de leur expéditeur et de leur contenu. Si vous avez téléchargé un programme, scannez-le à l'aide de votre anti-virus avant de l'exécuter.

- **Que faire si c'est trop tard ?**

Si vous êtes victime de l'un des effets indésirables énoncés ci-dessus, vous êtes très certainement infecté par un spyware. Dans ce cas,

- Ne vous rendez surtout pas sur votre espace client Portzamparc ! En effet, le logiciel malicieux pourrait vous dérober vos informations confidentielles et les transmettre à un individu mal intentionné.

- Si vous l'avez déjà fait, appelez immédiatement votre conseiller pour l'informer de la situation et voir avec lui la procédure à suivre.

- Après avoir scanné votre ordinateur avec votre anti-virus et détruit le fichier infecté, vous pourrez changer de mot de passe.

- Surveillez très régulièrement les mouvements sur votre compte pour vérifier qu'aucune opération suspecte n'a été engagée. Si tel était le cas, contactez immédiatement votre conseiller Portzamparc.

- **À retenir**

- Ne naviguez sur internet que si vous possédez un système d'exploitation, un navigateur internet, un anti-virus et un pare-feu à jour,

- Ne vous rendez pas sur des sites qui vous semblent suspects,

- Téléchargez des programmes ou des pièces jointes de mails uniquement si vous êtes certain de leur contenu. Dans le cas contraire, scannez-les avec votre anti-virus avant de les exécuter.

1.3.5 Cheval de Troie

- **De quoi s'agit-il ?**

Le cheval de Troie est un type de malware (comme les virus informatiques) qui s'attaque spécifiquement aux informations contenues dans votre ordinateur, en les détournant, les diffusant ou les détruisant.

- **Comment s'en prémunir ?**

- Il n'existe malheureusement pas de protection absolue contre les chevaux de Troie, puisque ceux-ci évoluent en permanence. Ainsi, il est indispensable de posséder un anti-virus et un pare-feu à la fois fonctionnels et mis à jour le plus régulièrement possible. De plus, mettez à jour votre système d'exploitation et votre navigateur internet.

- De façon générale, ne vous rendez pas sur des sites qui ne vous inspirent pas confiance, n'ouvrez des pièces jointes de mail que si vous êtes sûr de leur expéditeur et de leur contenu. Si vous avez téléchargé un programme, scannez-le à l'aide de votre anti-virus avant de l'exécuter.

- Pensez à contrôler les derniers mouvements effectués sur l'ensemble de vos comptes afin de déterminer si vous en êtes à l'origine. En cas de mouvement suspect, joignez immédiatement votre Conseiller Portzamparc pour l'informer de la situation.

- **Que faire si c'est trop tard ?**

Si vous êtes victime de l'un des effets indésirables énoncés ci-dessus, vous êtes très certainement infecté par un malware, qui peut être un cheval de Troie. Dans ce cas,

- Ne vous rendez surtout pas sur votre espace client Portzamparc ! En effet, le logiciel malicieux pourrait vous dérober vos informations confidentielles et les transmettre à un individu mal intentionné.

- Si vous l'avez déjà fait, appelez immédiatement votre conseiller pour l'informer de la situation et voir avec lui la procédure à suivre.

- Après avoir scanné votre ordinateur avec votre anti-virus et détruit le fichier infecté, vous pourrez changer de mot de passe.

- Surveillez très régulièrement les mouvements sur votre compte pour vérifier qu'aucune opération suspecte n'a été engagée. Si tel était le cas, contactez immédiatement votre conseiller Portzamparc.

- **À retenir**

- Ne naviguez sur internet que si vous possédez un système d'exploitation, un navigateur internet, un anti-virus et un pare-feu à jour,

- Ne vous rendez pas sur des sites qui vous semblent suspects,

- Téléchargez des programmes ou des pièces jointes de mails uniquement si vous êtes certain de leur contenu. Dans le cas contraire, scannez-les avec votre anti-virus avant de les exécuter.

1.3.6 Phaming (encore utile ?)

- **De quoi s'agit-il ?**

Le pharming est une technique de détournement de site : l'adresse que vous tapez dans votre navigateur est correcte mais vous êtes dirigé vers un site pirate. Ceci est rendu possible à l'aide de deux procédés :

- Le détournement des bases de données des fournisseurs d'accès à internet,

- L'installation d'un malware sur votre ordinateur.

Le but de cette attaque est identique à celui du phishing : vous dérober des informations confidentielles, que vous donnez à un site contrefait.

- **Comment s'en prémunir ?**

- Il n'existe malheureusement pas de protection absolue contre le pharming. Il est indispensable de posséder un anti-virus et un pare-feu à la fois fonctionnels et mis à jour le plus régulièrement possible. De plus, mettez à jour votre système d'exploitation et votre navigateur internet.

- Vérifiez toujours que vous êtes sur le véritable site de Portzamparc, en notant l'adresse exacte et la présence du cadenas de sécurité :

Attention ! La présence du cadenas n'implique pas avec certitude que vous êtes sur un site sécurisé ! L'emplacement de celui-ci est très important. En effet, sur l'image ci-dessus, il aurait suffi à un individu mal intentionné de remplacer l'image à gauche de l'adresse par celle d'un cadenas pour essayer de vous tromper. Or, sur Internet Explorer, le cadenas est à droite (entouré en rouge). Renseignez-vous sur les spécificités de votre navigateur internet, et notamment l'emplacement du cadenas.

- Utilisez les fonctions anti-phishing de votre navigateur : ce module parfois implémenté vous informe que le site sur lequel vous vous rendez a déjà été détecté comme un site contrefait. Si une telle alerte apparaît, quittez immédiatement la page que vous tentiez d'afficher.

- **Que faire si c'est trop tard ?**

- Si vous avez fourni vos codes d'accès (identifiant et mot de passe) à un site contrefait suite à une tentative de phishing, contactez immédiatement votre conseiller pour l'informer de la situation et voir avec lui la procédure à suivre.

- Pensez à contrôler les derniers mouvements effectués sur l'ensemble de vos comptes afin de déterminer si vous en êtes à l'origine. En cas de mouvement suspect, joignez immédiatement votre Conseiller Portzamparc pour l'informer de la situation.

- **À retenir**

- Vérifiez toujours que le site sur lequel vous êtes dirigé est le véritable site et non une contrefaçon à l'aide des indices décrits ci-dessus : présence d'un cadenas au bon emplacement, validité du certificat, aspect général si vous connaissez déjà le site,

- Mettez régulièrement à jour vos anti-virus et pare-feu, qui sauront vous protéger des malwares.

2. La sécurité, c'est l'affaire de chacun

2.1 Sécurité sur le site

Le site de Portzamparc a été conçu pour vous assurer un **niveau de sécurité optimal** lors de votre navigation. Parce que votre sécurité est notre priorité, découvrez nos services.

2.1.1 Authentification

- **Avant de vous identifier**

Ne vous rendez jamais sur le site de Portzamparc en suivant un lien sur internet ou dans un mail reçu, même prétendument de notre part. Tapez toujours dans la barre d'adresse : www.b-capital.fr. Nous vous recommandons d'ajouter notre site dans vos favoris/marques-page.

- **Pour vous connecter**

Cliquez toujours sur l'onglet MES COMPTES présent en haut à droite de la page, et ne tapez vos identifiants que si la page qui s'ouvre a l'aspect suivant :

Si ce n'est pas le cas, c'est que vous n'êtes certainement pas sur le véritable site de Portzamparc, mais possiblement sur une copie pirate créée pour vous dérober vos identifiants. Dans ce cas, n'entrez aucune information et contactez immédiatement votre conseiller Portzamparc pour l'informer de l'existence de cette page.

- **Limite de tentatives de connexion**

Par mesure de sécurité, si vous vous trompez 3 fois de suite dans votre mot de passe, l'accès à votre espace client sera totalement bloqué et vous devrez alors contacter impérativement votre conseiller Portzamparc pour suivre la procédure de déblocage. Cette protection permet d'éviter les attaques par « force brute », c'est-à-dire le test de toutes les combinaisons possibles de mots de passe pour trouver le bon.

- **Déconnexion automatique**

Pour votre sécurité, vous serez automatiquement déconnecté après 30 minutes d'inactivité sur votre compte. Il est donc normal dans cette situation qu'on vous demande à nouveau de vous authentifier afin de poursuivre votre navigation sur votre Espace Client. Toutefois, **préférez la déconnexion manuelle**.

2.1.2 Certificat/Chiffrement

- **Protocole de cryptage**

Afin de garantir une sécurité optimale, le site de Portzamparc utilise la technologie standard TLS (Transport Layer Security) en 128 bits, qui correspond au niveau de chiffrement le plus élevé autorisé en France. Ce protocole se traduit par l'apparition d'un S après le http dans la barre d'adresse, et à la présence d'un cadenas à côté de l'adresse du site.

Attention ! La présence du cadenas n'implique pas avec certitude que vous êtes sur un site sécurisé ! L'emplacement de celui-ci est très important. En effet, sur l'image ci-dessus, il aurait suffi à un individu mal intentionné de remplacer l'image à gauche de l'adresse par celle d'un cadenas pour essayer de vous tromper. Or, sur Internet Explorer, le cadenas est à droite (entouré en rouge). Renseignez-vous sur les spécificités de votre navigateur internet, et notamment l'emplacement du cadenas.

- **Certificat**

Pour que l'information hébergée sur un site puisse être protégée sous le protocole TLS, l'installation d'un certificat de sécurité est indispensable. Il s'agit d'un ensemble de documents électroniques émis par un organisme de certification. Il permet le cryptage des informations échangées entre le serveur et votre ordinateur.

2.2 Mobilité

Rien de tel pour la sécurité que ce que vous connaissez : votre ordinateur, votre réseau wifi domestique...
Mais si vous êtes sur un **ordinateur portable**, un **Smartphone** ou une **tablette**, sur un **réseau public**, la situation se corse !

2.2.1 Connectivité publique

Être en mobilité, cela signifie ne pas être connecté sur son réseau domestique, par câble ou wifi. Il existe trois moyens de se connecter à internet ou à d'autres appareils une fois que vous êtes en mobilité, c'est-à-dire dans la rue ou un hôtel par exemple.

Il faut être vigilant car vous ne connaissez pas les spécificités de chaque réseau, comme son niveau de protection ! Voici donc quelques conseils en fonction des situations.

- **Wifi public**

Contrairement à votre réseau domestique, un wifi public est disponible en tant que service dans des lieux de résidence par exemple (hôtel). Il faut être prudent car vous ne connaissez pas le niveau de sécurité de ces réseaux wifi, et s'ils sont bien cryptés. De plus, demandez toujours le nom du véritable réseau afin de ne pas se connecter à un autre Wifi pirate qui porterait le même nom, et volerait toutes vos données.

- **3G-3G+-4G**

Les réseaux 3G, 3G+ et 4G sont ceux fournis par les opérateurs télécoms. Ils sont disponibles si aucun réseau wifi accessible ne se situe à proximité de votre mobile et si votre forfait mobile vous le permet.

- **Bluetooth**

Si votre téléphone est équipé de fonctions Bluetooth, veillez à bien le désactiver lorsque vous ne vous en servez pas. Dans le cas contraire, un individu pourrait s'introduire dans votre support mobile sans que vous ne le sachiez ! Activez-le seulement lorsque vous souhaitez communiquer avec un autre mobile. La sécurité sur ces réseaux est très faible.

2.2.2 Sécurité physique

Vos supports mobiles sont…mobiles ! Prenez-en donc soin lorsque vous vous déplacez car vous pouvez les perdre ou vous les faire dérober, avec leur contenu.

S'il s'agit d'un ordinateur portable, n'hésitez pas à le sécuriser avec un câble et un cadenas afin qu'il ne soit pas volé, et verrouillez votre session dès que vous vous éloignez.

S'il s'agit d'une tablette ou d'un Smartphone, verrouillez bien votre support à l'aide d'un code confidentiel (évitez les codes trop triviaux tels que 0000) et en cas de vol, contactez immédiatement votre opérateur telecom pour qu'il bloque totalement l'accès à votre téléphone ou tablette.

Lexique

Certains termes de nos conseils vous semblent barbares ? Il est pourtant important que vous compreniez bien les notions qui y sont abordées.

Ainsi, voici un petit **lexique** qui pourra vous aider à y voir plus clair.

3G – 3G+ - 4G

Norme de réseau de téléphonie mobile à haut et très haut débit, permettant aux Smartphones de se connecter à internet.

Adresse MAC

Suite de chiffres unique au monde, propres à un terminal, qui permettent de l'identifier formellement. Il est codé sur 6 octets séparés par un trait d'union.

Anti-virus

Un anti-virus est un logiciel qui permet de détecter les malwares (les virus, mais aussi les vers, les chevaux de Troie, les spywares). Il se lance à chaque démarrage de votre ordinateur.

Des solutions gratuites et payantes existent, mais toutes ont un point commun : la nécessité d'être mise à jour très régulièrement, sous peine de rendre le logiciel inefficace et donc totalement inutile.

Bluetooth

Norme de réseau à courte distance permettant à deux terminaux mobiles de se connecter entre eux pour l'échange de données (fichiers, photos).

Certificat de sécurité

Un certificat de sécurité est un ensemble de documents électroniques émis par un organisme de certification, qui permet le chiffrement de l'information reçue et l'identification de l'origine de cette information.

Chiffrement

Le chiffrement est l'un des éléments du processus de codage et de décodage des messages qui assure la confidentialité des données. Le nom exact de ce processus est la cryptographie, qui consiste à transformer les données à l'aide de formules mathématiques pour les protéger.

Clé mobile / Clé mobile de session

Ce service envoie sur votre téléphone mobile un numéro d'authentification vous permettant de valider une transaction bancaire que vous venez de saisir.

Cookies

Un cookie est un fichier stocké sur votre disque dur. Il permet de vous reconnaître à chaque fois que vous revenez sur un site. Son but est de connaître vos préférences (par exemple les options que vous aurez cochées) pour vous éviter de les ressaisir.

Cheval de Troie

Un cheval de Troie est un type de virus. Il s'agit d'un programme machine qui se dissimule derrière un autre programme. Les chevaux de Troie sont souvent envoyés en pièce jointe d'e-mail. Il peut se présenter sous forme de jeu. Une fois ouvert, il peut endommager votre ordinateur, effacer des dossiers ou changer l'aspect de votre bureau. Il s'envoie lui-même automatiquement à d'autres personnes de votre carnet d'adresses pour se propager.

Mise à jour

Mettre à jour un logiciel permet d'obtenir sa version la plus récente. C'est une opération indispensable pour les systèmes d'exploitation, les pare-feu, les anti-virus et navigateurs internet pour une navigation sécurisée.

Navigateur internet

Un navigateur internet est un logiciel qui vous permet de vous rendre sur des sites web. Les plus connus sont Google Chrome, Internet Explorer, Mozilla Firefox ou encore Safari et Opéra. Il est impératif de les mettre à jour pour qu'ils soient efficaces contre la détection de sites frauduleux.

Pare-feu (ou firewall)

Le firewall est un système qui permet de protéger un réseau informatique connecté à Internet des attaques extérieures. Il est d'autant plus important d'en installer un sur les ordinateurs connectés à Internet en permanence puisque le risque d'actions frauduleuses est plus grand.

Pharming

Le pharming est une technique de détournement de site : l'adresse que vous tapez dans votre navigateur est correcte mais vous êtes dirigé vers un site pirate. Le but de cette attaque est identique à celui du phishing : vous dérober des informations confidentielles, que vous donnez à un site contrefait.

Phishing (ou filoutage, hameçonnage)

Le phishing est une fraude qui s'appuie sur le courrier électronique.

L'aspect premier du « phishing » prend généralement la forme d'un e-mail dans le corps duquel ou via un lien, vous sont demandés vos identifiants de connexion sous couvert de mise à jour de vos données bancaires. Cette supercherie vise à collecter les données nécessaires à accéder ensuite à vos comptes.

Protocole TLS

Le protocole TLS (Transport Layer Security) est un protocole d'échange d'informations permettant d'assurer l'authentification, la confidentialité et l'intégrité des données qui se transmettent sur Internet. Pour que l'information hébergée sur un site puisse être protégée sous le protocole TLS, l'installation d'un certificat de sécurité est indispensable.

Routeur

Élément intermédiaire dans un réseau informatique, il est indispensable pour connecter votre ordinateur à internet. Il se présente de plus en plus fréquemment sous la forme de « box ».

Smartphone (ou téléphone intelligent)

Téléphone dont les fonctionnalités permettent à son utilisateur d'accéder à internet, par les réseaux Wifi ou 3G, 3G+, 4G selon le forfait mobile souscrit.

Spam (ou pourriel)

Le spam est un message publicitaire non sollicité, envoyé par e-mail. Il peut générer l'ouverture instantanée de fenêtres Internet sur votre écran.

Spyware (ou logiciel espion)

Le Spyware est un logiciel installé à l'insu des utilisateurs qui lors de vos connexions peut récupérer certaines données comme vos habitudes de navigation.

Système d'exploitation

Il s’agit du logiciel, la plupart du temps déjà installé lors de votre achat du terminal, qui fait fonctionner votre ordinateur. Il s’agit la plupart du temps de Microsoft Windows, Apple Mac OS ou Linux. Tous doivent être mis à jour très régulièrement pour installer les patchs de sécurité.

Ver

Un ver est un programme autonome et parasite, capable de se reproduire par lui-même et dont le but est d'infecter le plus grand nombre de machines en se propageant via un réseau.

Virus

Un virus est un programme qui détruit certains fichiers indispensables ou sature les ressources de la machine.

Wifi

Le Wifi est une norme de réseau sans fil, à moyenne portée (quelques centaines de mètres autour de l’émetteur). Il peut être privé, donc crypté et sécurisé par un mot de passe, ou public.