



CASES articles

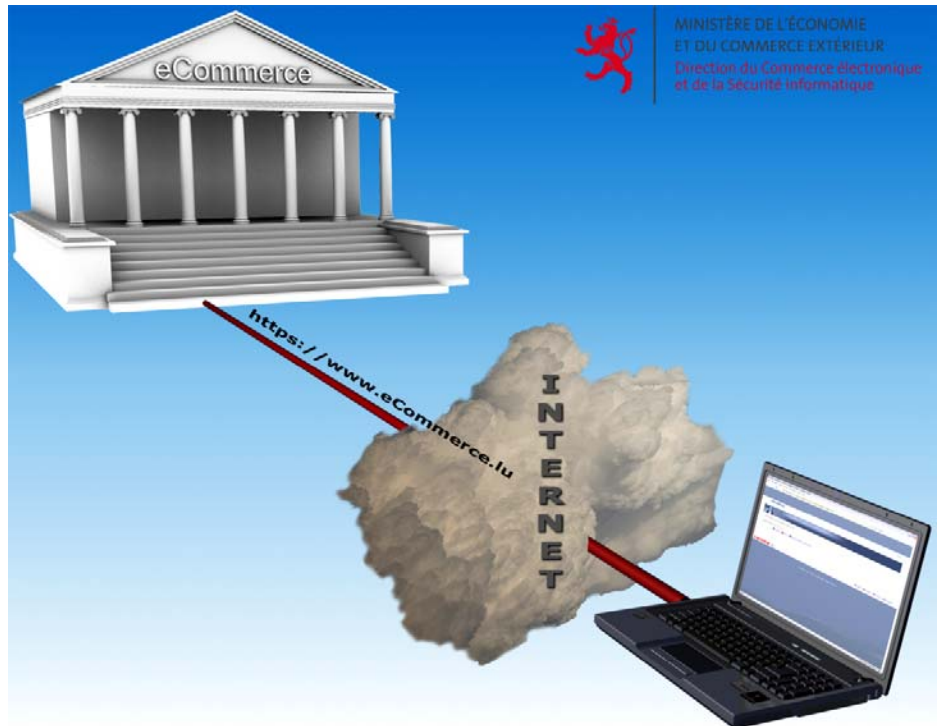
Le comportement inapproprié des utilisateurs génère des risques en matière de sécurité

Le commerce électronique plus sûr grâce à un comportement adéquat des utilisateurs

Pour plus de sécurité, adoptez les réflexes CASES !

La mise en œuvre de réflexes de sécurité permet de minimiser les risques d'attaque

Lors d'un sondage réalisé en avril 2008 dans le centre-ville de Londres auprès de plus de 500 personnes, 21 % des sondés ont échangé sans hésiter leur mot de passe contre une tablette de chocolat. Ce test camouflé en sondage a été réalisé par l'organisateur du Salon de la sécurité informatique Infosecurity Europe. À l'issue du test, les personnes questionnées se sont dites surprises que les sondeurs, à l'allure si soignée, aient pu, en fait, être des cybercriminels. La méconnaissance des formes d'attaque, des points faibles et des préjudices possibles, conduit à un comportement inadéquat des utilisateurs et donc exploité par les cybercriminels. Le comportement inadéquat ou imprudent des utilisateurs, ainsi qu'une certaine inexpérience du sujet, génèrent des risques en matière de sécurité. Ces comportements à risques peuvent également fragiliser des applications de commerce électronique bien protégées. Il est donc indispensable pour chaque utilisateur d'apprendre et d'appliquer nombre de réflexes de sécurité. Tout comme sur la route : le comportement adéquat des usagers minimise les risques pour chacun.



Qui n'a encore jamais déposé la clé de la maison sous un pot de fleurs à proximité de la porte ? Qui n'a jamais remis – au vu de tous – son portefeuille bien rempli dans sa poche à la sortie de la banque ? Ces attitudes, tout comme le fait de laisser son sac à main sur le siège de la voiture, facilitent grandement le travail des voleurs. Ces exemples peuvent être transposés à l'Internet et à ses applications. Qui n'a encore jamais communiqué son mot de passe ou oublié de fermer correctement une application Internet en cliquant sur le bouton adéquat ? Qui, lors de l'utilisation d'un ordinateur étranger, va penser à vérifier que le logiciel anti-virus est bien à jour ? Les cybercriminels exploitent ces négli-

gences des utilisateurs à leurs fins. Un comportement inadéquat des usagers augmente donc le risque pour ceux-ci de devenir victimes des pirates, notamment lors de l'utilisation d'applications d'e-commerce.

Risque = vulnérabilités x menaces x conséquences

Le risque peut être décrit par une équation simple : il résulte de la multiplication des paramètres « *vulnérabilités* », « *menaces* » et « *conséquences* ».

Le terme « *vulnérabilités* » décrit les failles de sécurité, de nature humaine ou technique, pouvant être exploitées

par des criminels. Les « *menaces* » sont par exemple les cybercriminels ou leurs outils. Les préjudices subis sont les « *conséquences* ». Il peut s'agir de préjudices financiers, d'atteintes à la réputation ou de pertes de temps. Dès lors que l'un des trois paramètres est égal à zéro, le risque est égal à zéro.

L'Internet est constitué de plus de 600 millions d'ordinateurs. Ce même chiffre laisse deviner que les criminels y sont également actifs. L'utilisateur n'a bien sûr aucune influence sur ces individus, le paramètre « *menaces* » échappe donc complètement à son contrôle. Il faut également partir du principe que chaque internaute peut subir des préjudices, ces derniers pouvant revêtir les formes les plus diverses, comme décrit ci-dessus. L'utilisateur n'est pas toujours en mesure d'influencer suffisamment sur le paramètre « *conséquences* ». Une sauvegarde permet toutefois par exemple de limiter les dégâts. Reste à analyser le paramètre « *vulnérabilités* » et à déterminer si celui-ci peut être influencé directement par l'utilisateur. Les usagers d'Internet peuvent minimiser ce paramètre et ainsi les points d'attaque potentiels, en adoptant un comportement adéquat. Plus le nombre de points faibles diminue et plus le risque de devenir la victime d'une attaque baisse.

Il n'est sans doute pas possible de les éliminer tous ; un certain risque résiduel ne peut donc être exclu. Les utilisateurs devraient toujours rester vigilants sur le net, même lorsqu'ils appliquent des réflexes de protection. Un portefeuille dissimulé dans une poche peut toujours être subtilisé par un pickpocket...

Un comportement d'utilisateur inadéquat peut générer des vulnérabilités

Un comportement inadéquat peut entraîner des préjudices. Une personne ayant retiré de l'argent à sa banque et qui compte les billets au vu de tous sur une place publique court plus de risques d'être dévalisée, alors

même que la banque est sécurisée. Sur l'Internet, de nombreux comportements sont négligents et ouvrent la voie aux attaques menées par les cybercriminels. Bon nombre d'usagers emploient par exemple un même mot de passe pour toutes leurs applications, celui-ci étant de surcroît bien souvent facile à deviner. Les mots de passe sont d'ailleurs volontiers communiqués à d'autres personnes, ou même notés sur l'ordinateur. Les systèmes d'exploitation et les programmes ne sont que très rarement ou jamais mis à jour. Malgré une utilisation quotidienne de l'Internet, de nombreux usagers ne trouvent pas le temps d'acquiescer les bases de la bonne utilisation de leurs logiciels antivirus ou de leur pare-feu. Beaucoup d'entre eux omettent de s'informer suffisamment au sujet des attaques potentielles, comme les logiciels d'espionnage, les chevaux de Troie, les vers ou encore le « *social engineering* ». Ils ne sont ainsi en mesure ni de les détecter, ni d'en appréhender les éventuelles conséquences. De nombreux utilisateurs, comme les familles par exemple, ont recours à un seul et même ordinateur. Alors que le premier membre de la famille l'utilise par exemple pour jouer, le second télécharge des films et de la musique sur Internet et le troisième effectue des virements bancaires. Bluetooth et Internet restent branchés pendant ce temps, même si l'utilisateur n'en a pas besoin. Les données personnelles sont transmises via l'Internet avec beaucoup de crédulité : des offres un peu trop alléchantes – qui s'avèrent souvent être des pièges de cybercriminels – sont parfois considérées comme de bonnes affaires.

La liste des comportements dommageables est longue. Il est néanmoins possible d'utiliser l'Internet et ses applications tout en limitant les risques de tomber dans des pièges.

Comportement d'utilisateur adéquat

« Adopter un comportement adéquat permet de réduire les risques de devenir la victime des cybercriminels.

Les réflexes de sécurité sur l'Internet, notamment dans le cadre de l'e-commerce, peuvent être acquis et appliqués. Ces réflexes sont comparables à l'utilisation de la ceinture de sécurité dans une voiture. Les « *règles d'or* » constituent la base des réflexes de sécurité à adopter sur l'Internet ; d'autres réflexes de protection relatifs à l'ordinateur, aux applications d'e-commerce, au navigateur et aux mots de passe viennent s'y ajouter. Tous ces réflexes sont faciles à acquiescer », explique Raymond Faber, responsable de la Direction du commerce électronique et de la sécurité informatique du Ministère de l'Économie et du Commerce extérieur luxembourgeois.

Réflexes de sécurité : les règles d'or

La mise en œuvre des « *règles d'or* » de la sécurité informatique ne nécessite aucune connaissance informatique particulière. Cinq règles importantes en matière de comportement des utilisateurs doivent être mentionnées.

La première de ces règles concerne les mots de passe : les utilisateurs devraient choisir des mots de passe assez longs, qui devraient de plus être difficiles à deviner et être constitués de lettres, de chiffres et de caractères spéciaux. Il convient d'utiliser un mot de passe différent pour chaque application et d'en changer souvent. Les mots de passe ne doivent jamais être notés ou sauvegardés.

Les mots de passe sont précieux et les cybercriminels tentent par tous les moyens de les obtenir. Les pirates essaient par exemple de voler les mots de passe des utilisateurs en faisant usage d'e-mails frauduleux. Il est donc recommandé d'être particulièrement vigilant et méfiant en présence de tels e-mails. Tout comme s'il s'agissait de sa carte d'identité, l'utilisateur ne doit jamais communiquer ses données d'accès à des tiers, pas même à son meilleur ami, ses collègues de travail ou son supérieur.

Les programmes de mise à jour destinés à remédier aux failles détectées

dans les logiciels constituent la deuxième règle d'or. Ces programmes, appelés patches, doivent être installés régulièrement par l'utilisateur. Le procédé peut être comparé à une voiture présentant un dysfonctionnement au niveau des freins et qui est réparée suite à une campagne de rappel.

L'utilisateur doit doter son ordinateur d'un logiciel anti-virus – c'est la troisième règle d'or. Celui-ci doit être actualisé régulièrement, de préférence quotidiennement, afin de pouvoir détecter les malwares les plus récents. À cet effet, en parallèle avec ses produits payants, l'industrie met également des produits gratuits à la disposition des utilisateurs privés.

L'ordinateur de l'utilisateur doit également disposer d'un pare-feu correctement configuré. L'application de cette quatrième règle permet à l'utilisateur d'empêcher les transferts de données non souhaités.

La cinquième règle d'or prévoit la vérification régulière de l'ordinateur à l'aide d'un logiciel anti-spyware. Des produits gratuits sont également proposés aux utilisateurs privés à cet effet.

Réflexes de sécurité : e-commerce

Les réflexes de sécurité spécifiques suivants devraient également être adoptés par l'utilisateur lorsqu'il utilise des applications e-commerce : l'ordinateur utilisé pour ces applications devrait être réservé à cette seule fin et employé le moins possible pour d'autres utilisations. De plus, cet ordinateur ne devrait être doté que des logiciels strictement nécessaires. Avant toute installation, il convient de vérifier que les logiciels ainsi que leurs supports proviennent de sources fiables. Une vigilance toute particulière est de rigueur lorsqu'il s'agit de CD gravés, de sticks mémoire ou d'offres très alléchantes sur l'Internet. L'utilisateur devrait également veiller à restreindre l'accès à cet ordinateur à un nombre limité de personnes. Sur les ordinateurs utilisés par plusieurs personnes, il convient de créer un

compte utilisateur spécifique pour les applications d'e-commerce. Sous Windows, ceci est possible en cliquant sur [Démarrer] [Panneau de configuration] [Comptes d'utilisateurs]. Un clavier et une souris Bluetooth ne devraient être utilisés qu'en association avec un chiffrement adéquat.

Réflexes de sécurité : e-banking

Les applications d'e-banking nécessitent également l'application de certains réflexes de sécurité supplémentaires. Les utilisateurs devraient fixer un montant maximum dans le cadre des applications d'e-banking, à l'instar des cartes de crédit. Dans la mesure du possible, il convient également de restreindre le nombre de pays vers lesquels des virements sont autorisés. Seuls les pays vers lesquels des virements sont effectués régulièrement devraient être autorisés. L'utilisateur devrait en outre toujours s'assurer que les pages web correspondantes sont sécurisées (voir Conseils de sécurité). Si un événement inhabituel se produit au cours d'une session d'e-banking, il est recommandé d'en aviser la banque. Chaque session doit être clôturée à l'aide du bouton de déconnexion (« logout »). Négliger ce réflexe équivaut à laisser la porte de la maison grande ouverte en s'absentant. L'utilisateur devrait également se familiariser avec les fonctions e-banking proposées par sa banque. Il est parfois possible de bloquer son propre compte e-banking, ce qui peut être comparé au blocage d'une carte de crédit ayant été perdue. L'utilisateur devrait également veiller à ne pas être observé lorsqu'il effectue des opérations de banque en ligne. Les endroits publics, tels que les aéroports ou les cybercafés, devraient alors être évités. L'utilisation d'un ordinateur étranger, y compris celui du poste de travail, présente un risque plus important. L'utilisateur ne peut en effet jamais être sûr du contenu de la machine ou des personnes l'ayant utilisée précédemment.

Conseils de sécurité :

Les utilisateurs peuvent évaluer leurs connaissances et leurs réflexes en matière de sécurité en passant le permis commerce électronique sur le portail de sécurité CASES : <https://epass.cases.lu>.

Ils peuvent également vérifier s'ils sont en mesure d'identifier des e-mails frauduleux : http://www.cases.public.lu/fr/pratique/solutions/phishing_test/.

Le portail de sécurité www.cases.lu propose des informations détaillées relatives à la sécurité des pages Internet. Un guide illustré permettant de vérifier la sécurisation d'une page Internet est disponible dans le dossier HTTPS.

Définition : ingénierie sociale ou « social engineering »

Le facteur humain est au centre des techniques de social engineering : les cybercriminels établissent des relations de confiance avec les utilisateurs. Une simple conversation est souvent suffisante. Ces relations sont ensuite exploitées afin d'obtenir des informations et d'en tirer profit.

Définition : navigateur

Le navigateur permet de consulter des pages web sur l'Internet.

Définition : plug-in

Un plug-in est un programme autonome apportant des fonctionnalités complémentaires à un autre logiciel auquel il est rattaché.

Définition : add-on

Un add-on est un module optionnel pouvant compléter un logiciel ou un matériel. Il ne s'agit pas d'un programme autonome.

Réflexes de sécurité : navigateur

Le navigateur permet de consulter des pages web sur Internet. L'adoption d'un comportement adapté permet ici encore d'éviter certaines failles de sécurité. L'utilisateur devrait par exemple mettre à jour régulièrement son navigateur. Les failles de sécurité du logiciel sont ainsi corrigées. De plus, de nouvelles fonctionnalités de protection sont à la disposition de l'utilisateur. Les contenus enregistrés par le navigateur devraient être effacés après chaque session d'e-commerce (voir Conseils de sécurité). Les programmes complémentaires tels que les plug-ins ou les add-ons devraient être évités, ceci afin de

réduire les failles de sécurité qu'ils pourraient comporter. En outre, les utilisateurs ne devraient pas utiliser une version d'évaluation de leur navigateur.

Les utilisateurs peuvent se protéger activement des attaques des cybercriminels. L'application de réflexes de sécurité réduit considérablement le risque qu'un pirate puisse accéder aux applications d'e-commerce de l'utilisateur.

Le portail de sécurité www.cases.lu propose des informations détaillées relatives à la sécurité des pages Internet. Un guide illustré permettant de vérifier la sécurisation d'une page

Internet est disponible dans le dossier HTTPS.

À l'aide de deux exemples, voici comment effacer les contenus enregistrés dans la mémoire intermédiaire du navigateur :

dans le navigateur Internet Explorer, ces contenus peuvent être effacés en cliquant sur [Outils] dans la barre des menus, puis sur [Options Internet], et dans l'onglet [Général] sous *Historique de navigation*; dans le navigateur Mozilla Firefox, ces contenus sont effacés en cliquant sur [Outils] dans la barre des menus, puis sur [Options], onglet [Vie privée] sous *Vie privée* [Paramètres].

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu