

Le clavier virtuel et l'accessibilité bancaire en Belgique : Anticipation.

1. Contexte.

Les nouvelles technologies et Internet en particulier favorisent plus largement l'accès des personnes handicapées à de nombreux services, comme les services bancaires, grâce au développement de la banque en ligne.

Cependant, ces avancées technologiques que sont les sites internet et plus précisément les sites internet des banques sont encore semées d'embûches pour les personnes handicapées.

Pour des raisons de plus grande sécurité, certaines banques américaines, canadiennes, françaises et autres évoluent vers l'utilisation d'un clavier virtuel pour la saisie du code d'accès aux services en ligne.

Anticipons l'arrivée de ce type de technologie de notre pays et les conséquences pour les personnes handicapées.

2. Qu'est-ce qu'un clavier virtuel ?

Les banques qui évoluent vers ce système, l'estiment très simple et dans les faits il n'est pas très compliqué pour une personne valide. Au lieu de saisir le code secret sur le clavier, il faut cliquer sur une grille qui apparaît sur l'écran et dont les numéros sont placés aléatoirement – ce côté au hasard permettant un renforcement de la sécurité, puisqu'à chaque connexion, l'emplacement change (à chaque nouvel accès, les chiffres du clavier virtuel changent de cases pour plus de sécurité). De plus, d'une fois à l'autre,

certaines systèmes déplacent le clavier sur l'écran : il n'est donc plus systématiquement au même endroit. La saisie du code secret se fait donc systématiquement et exclusivement à partir de la souris. Il est impératif de préciser que l'utilisateur doit cliquer sur les chiffres du code dans le bon ordre, sinon cela ne fonctionne pas.

3. Le clavier virtuel et les personnes handicapées.

Considéré comme un outil permettant une meilleure intégration des personnes handicapées dans la société, internet permet d'accéder, aujourd'hui à des services publics ou privés de chez soi, ce qui résout les problèmes de mobilité et d'accès aux lieux de ces services.

Les banques ont introduit des services de consultation et de gestion des comptes bancaires par ce média. Ceci a permis à leurs clients porteurs de handicap d'accéder de manière plus autonome aux opérations bancaires telles que la consultation du solde de leur compte, la réalisation de virements, d'opérations boursières etc...

Dans les pays où « beaucoup plus » de pirates informatiques sévissent dans les banques, les utilisateurs handicapés sont aujourd'hui confrontés à la mise en place de claviers virtuels et autres dispositifs pour renforcer la sécurité, et donc perdent l'autonomie qu'ils avaient - là - gagnée.

Le choix d'une "plus grande sécurité", se révèle être un nouveau moyen d'exclusion des personnes handicapées de services bancaires en ligne.

Le cas français.

Depuis quelques années, les banques françaises introduisent de nouveaux systèmes d'identification afin de renforcer la sécurité et d'éviter le piratage des comptes bancaires de leurs clients par des logiciels espions qu'ils appellent Keyloggers¹ qui écoutent la frappe du clavier.

En mettant en place les claviers virtuels pour les opérations bancaires à domiciles, les banques souhaitent ainsi éviter que des machines se

1 Un enregistreur de frappe ou keylogger peut être assimilé à un matériel ou à un logiciel espion qui a la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux. Par exemple, certains enregistreurs de frappe analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie.

connectent aux comptes de leurs clients en simulant et/ou en capturant la saisie au clavier de leur mot de passe.

Ce système évite certes les problèmes liés à la saisie d'un mot de passe au clavier. Mais il a plus d'un inconvénient.

Problème de sécurité au niveau du mot de passe : les claviers virtuels sont uniquement composés des chiffres allant de 0 à 9. En conséquence, le mot de passe est plus facile à reconstituer que s'il était formé de chiffres, de lettres et autres signes tels que \$, €, *, ou -.

Problème d'accessibilité : la plupart de ces "claviers virtuels" sont inaccessibles aux internautes qui ne peuvent utiliser la souris : soit parce qu'ils sont aveugles ou malvoyants et qu'ils ne voient pas ou difficilement le pointeur ; soit qu'ils ont un handicap moteur et ne peuvent pas se servir d'une souris.

Problème de lisibilité : certains claviers virtuels utilisent des chiffres qui sont peu lisibles pour des personnes devant grossir la taille des caractères. Il leur est également difficile de positionner le pointeur de leur souris correctement sur le chiffre approprié. S'ils sélectionnent un chiffre par erreur, ils auront du mal à corriger ce chiffre. Ils doivent cliquer sur "corriger" puis re cliquer sur le chiffre souhaité.

Alors que l'Europe, dans E-Inclusion 2010 souhaite que les personnes handicapées et les personnes âgées prennent part à la société, alors que la France a voté la loi de février 2005 sur l'égalité des chances pour les personnes handicapées, le renforcement de la sécurité des banques au détriment de l'accessibilité de leurs services est un pas en arrière dans une meilleure intégration des personnes handicapées dans la société de l'information.

Argumentaires des banques pour l'utilisation du clavier virtuel.

Face aux reproches de leurs clients handicapés qui éprouvaient des difficultés à utiliser le clavier virtuel, certaines banques françaises ont développé un argumentaire.

En faisant le tour de quelques grandes banques en ligne (BNP, Crédit-Agricole, Société Générale) et en cherchant sur leurs systèmes d'aide à la recherche des justifications au clavier virtuel, on peut trouver les arguments suivants :

- **BNP :** Ce nouveau système d'identification a pour but de renforcer la sécurité d'accès à la gestion des comptes.

- **Crédit Agricole** : Ce nouveau mode de saisie du code personnel à la souris a été mis en place pour une meilleure sécurité d'accès aux comptes en ligne. L'utilisation de la souris préserve donc la confidentialité du code personnel. Le clavier virtuel est utilisable, grâce à l'ajout d'un logiciel spécifique, par les personnes mal voyantes.
- **Société Générale** : Certains virus (appelés « Chevaux de Troie ») sont des programmes installés sur l'ordinateur à l'insu du propriétaire. Ces virus peuvent enregistrer les saisies faites à partir du clavier. Les données ainsi collectées sont ensuite transmises aux « pirates » qui vont récupérer des informations confidentielles, pour ensuite les utiliser frauduleusement. Le clavier virtuel est un moyen efficace de lutter contre ce type de virus. Le Clavier virtuel sert à saisir le code secret tandis que l'identifiant (numéro de compte) est tapé sur le pavé numérique.

Contres arguments

D'une manière générale, il n'est pas sécurisant de saisir le numéro du compte au clavier virtuel d'une part, et le code à la souris (donc déplacement des mains, rupture de concentration, utilisation de 2 périphériques différents pour la même opération...). *Jongler entre clavier et souris est désagréable* pour passer de l'un à l'autre. Le code d'accès est numérique, le code secret aussi ; tout saisir au clavier numérique est donc ce qu'il peut y avoir de plus serein. A l'exception de Société Générale, on saisit (au clavier) son code d'accès, on valide (à la souris) dans les autres banques, on saisit (toujours à la souris) le code secret – cette première étape de validation rend les choses plus fluides.

Autre reproche à opposer au système : si le clavier virtuel protège des Key Loggers, il *ne protège pas des coups d'oeils indiscrets*. Autant il est facile de cacher sa main pour saisir son code au clavier (et donc se protéger de ses collègues de bureaux, voisins de cyber café...), autant cela devient illusoire sur un clavier virtuel qui occupe une belle surface à l'écran.

Les dernières de key loggers générations ne se contentent pas d'écouter les frappes du clavier, mais effectuent des *captures écrans à chaque clic de souris*. Le clavier virtuel est donc capturé, quoi qu'il advienne.

Conclusions.

Pour lutter contre les keyloggers et autres nuisances du Net, il est indispensable que les banques renforcent leurs sécurités. Par contre, l'utilisation des claviers virtuels ne paraît pas être la solution idéale car, d'une part, elle enlève la partie d'autonomie que les personnes handicapées avaient acquise dans les transactions bancaires via internet, et d'autre part, ces claviers ne sont pas efficaces contre tous les keyloggers (notamment ceux qui capturent l'écran).

Bien que certaines banques proposent des programmes adaptés aux personnes malvoyantes et aveugles, la saisie d'un mot de passe à l'aide d'un clavier virtuel demande de la précision qui n'est pas toujours possible à un utilisateur ayant des difficultés pour positionner la souris sur un endroit déterminé de l'écran. Si la saisie au clavier s'avère impossible par le biais de ce nouveau système d'identification, ces internautes se voient exclus de l'accès à leur banque en ligne. Ils sont de nouveau dépendants d'une tierce personne qui effectuera les actions de saisie de leur mot de passe avec la souris pour eux.

De plus, les claviers virtuels s'étalant sur les écrans créent de nouveaux dangers comme le coup d'œil du voisin.

Cette technique (clavier virtuel) bien que plus sécurisée que la saisie directe au clavier, n'est cependant pas une solution hautement sécurisée comme peuvent l'être les authentifications fortes par cartes à puce. L'avantage de cette dernière solution dans la quelle le client n'a pas à envoyer un mot de passe fixe sur Internet, est qu'elle n'est pas vulnérable à des attaques de type "phishing"².

En Belgique, un système de protection repose sur une petite *calculette* (indépendante de l'ordinateur) qui génère un code valable une fois pour une connexion ponctuelle. C'est ce nouveau code ou certains chiffres de ce nouveau code qu'il faut entrer dans l'ordinateur pour effectuer ses opérations bancaires.

Si l'adoption du "clavier virtuel" semble gagner du terrain et devenir une technologie à la mode dans beaucoup de banques françaises, une autre technologie permettant de renforcer la sécurité commence à être utilisée par certaines banques. Il s'agit de la génération d'un "code sécurité" unique, qui est fourni par la Banque à chaque fois que l'utilisateur se connecte aux services en ligne de la banque. L'utilisateur obtient ce code sécurité unique par un SMS qui lui est envoyé sur son téléphone portable. Il doit donc être en possession d'un téléphone portable et être en mesure de lire ces messages « texte ». Si tel n'est pas le cas, la banque propose à l'utilisateur de régler sa transaction par téléphone à un numéro surtaxé, ce qui n'est pas forcément plus sécurisé. De même, ces nouveaux procédés, comme les claviers virtuels ne sont pas ce qu'il y a de mieux pour les personnes handicapées (il faut

² L'hameçonnage, appelé en anglais phishing, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une H usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : H mot de passe, numéro de H carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'H ingénierie sociale. L'hameçonnage peut se faire par H courrier électronique, par des H sites Web falsifiés ou autres moyens électroniques.

pouvoir lire un SMS, ce n'est pas le cas de tout le monde, le numéro sur téléphone fixe est surtaxé !!).

En Belgique, ces nouvelles technologies, ne nous ont pas encore « rejoints ». Il est urgent que les associations de personnes handicapées, comme l'Association Socialiste de la Personne Handicapée, se mobilisent pour empêcher que ces nouvelles exclusions s'aggravent. Tant que des solutions alternatives accessibles ne se développent pas en masse, les banques doivent proposer, aux personnes qui le souhaitent, d'accéder à leurs comptes dans les mêmes conditions qu'avant l'introduction des nouveaux systèmes de sécurité comme les claviers virtuels..

Sources :

- Discours de Madame Marie Anne Montchamp – Secrétaire d'Etat aux personnes handicapées ;Colloque « Politiques et législations en faveur de l'accessibilité numérique en Europe » Cité des Sciences et de l'Industrie, 31/01/2005.
- www.richardcarlier.com/clavier-virtuel-et-accessibilite-bancaire.php
- www.europa.eu/rapid/pressReleasesAction.
- BNP :
<https://www.secure.bnpparibas.net/controller?redir=5&stamp=1124959106455&type=homeconnex>
- Société Générale :
http://par.societegenerale.fr/EIP/resources/production/clavier_virtuel/clavier_virtuel_securite/
- Axa Banque : <https://www.axabanque.fr/Contenu/securite3.htm>

Responsable analyse : Rébéka MUTOMBO
Coordinatrice-animatrice

Responsable ASPH : Gisèle MARLIERE
Secrétaire nationale

Date : 9 juillet 2007