INTRODUCTION

L'activité bancaire consiste dans la plus part des cas au développement des produits et services qu'elle proposera aux clients. Traditionnellement ces produits et services étaient proposés aux clients de banque dans l'une des agences ou guichet de celle-ci.

L'avènement des nouvelles technologies à impacter de nombreux secteurs et parmi les secteurs les plus influencés par celles-ci le secteur bancaire apparait comme le secteur le plus affecté par cette révolution technologique

En effet le secteur bancaire est un domaine basé sur les informations qui à leur tour s'appuient fortement sur les NTIC. Toutefois les NTIC ne sont pas seulement cruciales dans l'analyse des informations, mais elles permettent aussi aux banques de différencier leur offre de services par rapport aux concurrents.

Alors, dans une époque ou les médias (ordinateurs, médias, téléviseurs…) et les moyens de transmission (télécommunication, câble, électronique…) se complètent et se chevauchent, l'agence bancaire n'est plus considérée aujourd'hui comme le lieu de passage obligé du client.

D'où le développement durant les dix dernières années du concept des services financiers électroniques, communément appelé « e-banking ». Le terme e-banking, (Inter) net Banking, Web Banking ou encore Online Banking désigne l'utilisation de l'Internet par une institution financière en vue d'offrir à ses clients une gamme de services bancaires plus ou moins larges, allant de la simple vitrine commerciale à la gestion à distance de transactions financières.

Ce concept est entré dans les mœurs de plusieurs institutions financières pour le traitement de leurs opérations courantes, dans la mesure où de plus en plus il répond aux attentes des clients dont les besoins et les exigences ont évolué avec le développement fulgurant des NTIC. Notons toutefois que l'adoption de toute innovation dans une organisation n'est pas chose évidente. Surtout dans la banque ou la notion de sécurité est l'élément essentiel pour assurer à la clientèle la confidentialité des transactions et par conséquent la confiance de ces derniers.

L'objectif de cet exposé consiste dans un premier temps en l'analyse du fonctionnement et des avantages apportés par l'e-banking non seulement du côté des clients mais aussi de celui de la banque. L'e-banking s'effectuant la plus part du temps via Internet, il sera question dans un

second temps de brosser les menaces qu'exposent particulièrement l'e-banking avant de déboucher sur les solutions à ces menaces.

I. FONCTIONNEMENT ET AVANTAGES DE L'E-BANKING

L'e-banking fait partie d'un ensemble que constitue la banque en ligne. Celle-ci se décline en : PC banking (ce système nécessite un programme spécial fourni par la banque qui, une fois installé, s'avère en général très simple pour une personne un tant soit peu familiarisée avec l'informatique. Les données sont transmises par un modem) ; le Net banking ou e-banking ; le Phone banking. Pour utiliser ce service, il suffit de posséder un téléphone à touches et de signer un contrat particulier auprès d'une institution bancaire. Le client appelle via un numéro de téléphone donné et tombe sur un récepteur vocal qui lui explique la marche à suivre. Ce service comprend également deux niveaux : un serveur vocal accessible 24h/24 et 7jours/7 au moyen duquel le client peut consulter ses comptes et effectuer ses transactions bancaires, une centrale d'appel téléphonique ouverte sur des plages horaires plus larges que celle des agences et permettant d'être directement en ligne avec un conseiller de la banque qui peut soit donner un conseil, soit répondre à une question ou exécuter certaines opérations ; le Mobile banking.

A. Le fonctionnement technique

Une fois que tous les supports sont prêts (ordinateur et modem entre autres), l'utilisateur peut installer le logiciel qui est fourni avec la documentation (cas des pays européens). Ce logiciel installe une icône sur le poste de travail (Windows). Cette icône permet d'accéder directement à ce service. Ce procédé évite bien des problèmes de piratage. La connexion indirecte par Internet est possible. Il suffit de se rendre sur le site de son partenaire financier (cas particulier du Cameroun), mais on s'expose d'avantage à des piratages.

Lors d'une connexion, les renseignements suivants sont demandés cas d'Afriland First Bank:

- N° d'abonné du client/ N° d'identification
- Mot de passe

Ces informations sont indispensables pour se connecter à son ou à ses comptes. A partir de ce moment vous pouvez effectuer toutes les opérations permises par votre banque via Internet.

B. Les avantages

- Possibilité d'effectuer des opérations bancaires en temps réel : le client peut effectuer rapidement et aisément toutes ses opérations bancaires (règlements de factures, avances sur commande, ordres de bourse) et ses comptes sont immédiatement impactés.
- Réalisation des opérations bancaires dans les meilleures conditions (pas de file d'attente, pas de bruit, pas de stress) et selon un processus apparemment sécurisé.
- Mise à la disposition de la clientèle de produits et services disponibles dans la banque traditionnelle (consultation de solde, consultation et édition d'extraits de compte, effectuer tous les types de virements, ouverture de compte) à l'exception du dépôt et du retrait d'argent liquide et des transferts d'argent à l'international.
- Disponibilité de l'information: le client a la possibilité d'avoir accès à ses informations financières 24h sur 24.

La banque électronique présente des avantages énormes pour la banque (pénétration de nouveaux marchés et élargissement du rayon d'action) et pour le consommateur en offrant des opérations simplifiées mais elle pose aussi de nombreux problèmes.

II. MENACES

Les techniques des fraudeurs sont simples pour pouvoir accéder aux comptes bancaires. Avant l'avènement d'Internet, accéder à des informations personnelles nécessitait une présence physique (pour aller voir dans le portefeuille de la victime). Aujourd'hui ce n'est plus le cas les hackers rivalisent d'ingéniosité pour soutirer aux internautes des informations confidentielles ; dans le cas du e-banking nous avons recensé : le phishing, le pharming, le man in the middle.

A. Le phishing

Les attaques de phishing sont les plus connues. Elles désignent toute tentative par téléphone, courrier électronique, messagerie instantanée ou fax, de se procurer des informations personnelles dans l'intention de voler l'identité, la propriété intellectuelle, et finalement, des ressources financières. La plupart de ces tentatives se font sous couvert d'un objectif légitime, c'est-à-dire qu'elles paraissent valides, mais sont en fait le fruit d'une entreprise criminelle.

Une attaque électronique de phishing comprend généralement deux éléments : un message électronique à l'aspect authentique et une page Web frauduleuse.

B. Le pharming

Le **pharming** est une technique de piratage informatique exploitant des vulnérabilités DNS (Domain Name System) pour récupérer les données d'une victime. Ce type d'hameçonnage (*phishing*) permet de voler des informations après avoir attiré la victime sur un site web maquillé même si le nom de domaine est correctement saisi. L'objectif du pharming est le même que celui du phishing : induire l'internaute en erreur et l'amener sur un site contrefait. Cependant, au lieu de solliciter directement des informations personnelles ou professionnelles, le pharming consiste à pirater des URL légitimes et les rediriger, via le serveur du nom de domaine, vers des adresses IP frauduleuses qui usurpent les adresses d'origine.

C. L'attaque man-in-the middle

Man-in-the middle signifie l'homme du milieu. Cette attaque fait intervenir trois protagonistes : le client, le serveur et l'attaquant. Le but de l'attaquent est de se faire passer pour le client auprès du serveur et de se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, accès système, etc.)

La plupart du temps l'attaquant utilise des techniques de détournement de flux pour rediriger les flux des clients et du serveur vers lui.

Par ailleurs, à coté des ces attaques ciblant le domaine bancaire, on trouve des infections informatiques comme les chevaux de Troie et de nombreux malwares destinés à voler des informations des utilisateurs de réseaux sociaux (Myspace, Facebook…) ou de jeux en ligne (poker, casino, World of Warcraft…)

D. La négligence des clients

Dans la plupart des cas les systèmes informatiques des banques sont hautement sécurisés. Les failles utilisées sont principalement humaines : la naïveté de la personne qui navigue sur Internet et sa méconnaissance des règles minimales de sécurité à appliquer à son PC.

III. Les solutions : la sensibilisation du client et l'authentification forte

A. La sensibilisation du client

La question est de savoir si le client doit simplement subir l'escalade entre les banques et les hackers ou alors s'il doit avoir un rôle actif ? Le client doit avoir un rôle actif. L'utilisateur doit respecter des règles minimales de sécurité : les unes sont relatives aux mesures de base liées à la sécurité informatique et les autres aux mesures spécifiques liées à la sécurité de l'e-banking.

1. Les règles de base de la sécurité informatique

A la base de toute manipulation informatique sécurisée, ces règles sont à respecter impérativement :

- **Les mots de passe**

Les mots de passe sont les clés d'accès aux informations et aux comptes des clients en ligne. Le défi consiste donc à les choisir de manière à ce qu'ils soient aisément mémorisables tout en étant difficiles à deviner par autrui.

- **L'antivirus**

Permet de préserver l'ordinateur des virus et des vers. Installer un antivirus et le maintenir à jour est un indispensable de la sécurité sur Internet.

- **Le firewall**

Il doit être bien configurer pour permettre non seulement de bloquer les attaques ou connexions suspectes pouvant provenir de virus, vers ou chevaux de Troie, mais aussi d'éviter la fuite de vos informations personnelles et confidentielles.

- **L'anti-spyware**

Son installation permettra de balayer régulièrement l'ordinateur afin de repérer les logiciels malicieux qui pourraient s'y trouver.

2. Les règles spécifiques à la sécurité e-banking

Avant toute connexion aux services en ligne, il est essentiel de lire et d'appliquer les bons réflexes :

- **Les e-mails**

Deux mesures sont à prendre : apprendre à détecter les e-mails frauduleux et ne pas utiliser des liens contenus dans un email pour accéder à un site mais plutôt saisir directement l'adresse de celui-ci.

- **Les pages Web sécurisées**

Lorsque le client utilise des services de paiement ou d'opérations bancaires en ligne, il doit toujours assurer que les pages sont sécurisées. Pour cela, des indices permettent facilement de le vérifier :

– affichage de la clé 

– ou du verrou 

- **Les connexions douteuses**

Le client ayant remarqué un fait anormal et pensant avoir un problème de sécurité avec sa session, peut bloquer son compte e-banking si sa banque propose ce service.

B. Le renforcement de la sécurité

1. L'authentification forte

L'ouverture de services en ligne doit s'accompagner d'un dispositif de sécurité permettant à la banque d'éviter les actes frauduleux en s'assurant de l'identité du donneur d'ordre (le client).

Les mesures d'authentification ont été renforcées, ainsi on est passé de l'authentification statique à une authentification dynamique ; de l'utilisation d'un seul facteur d'authentification (le mot de passe) à deux facteurs (mot de passe et TAN carte). Mais il y a toujours moyen d'aller plus loin, en demandant une authentification à chaque transaction (one time password)

Les banques peuvent aussi atteindre un niveau de sécurité élevé en remplaçant les simples mots de passe par une autre procédure d'authentification forte. Il s'agit de la biométrie. Elle permet l'identification ou l'authentification d'une personne sur la base de données reconnaissables et vérifiables qui lui sont propres (empreintes digitales…).

On peut considérer que l'authentification forte est une des fondations essentielles pour garantir :

- ✓ L'autorisation ou contrôle d'accès (qui peut avoir accès)
- ✓ La confidentialité (qui peut le voir)
- ✓ L'intégrité (qui peut le modifier)
- ✓ La traçabilité (qui l'a fait)

2. **Cryptage des données**

C'est un procédé de transformation d'une information intelligible en une information inintelligible par l'utilisation d'algorithme. Son but est de garantir la confidentialité en cachant l'information à toute personne qui n'est pas censée en avoir connaissance. De cette façon les données sont transmises de façon sécurisée par un système de cryptage.

CONCLUSION

La banque, en plus des divers canaux qu'elle utilisait pour la distribution de ses produits et services a intégré les nouvelles technologies de l'information et de la communication pour les transactions à distance avec ses clients. Cette nouvelle façon d'être en relation avec les clients à certes des avantages pour les clients : rapidité et exécution des opérations dans de meilleures conditions et pour la banque en termes de pénétration de nouveaux marché mais a aussi généré de nouveaux problèmes en termes de sécurité. Le but de ce type de transactions étant des mouvements de fonds, il a suscité l'intérêt d'intelligences malveillantes. Par l'utilisation des techniques dont l'objectif est de dérober les informations confidentielles des clients, elles peuvent ainsi détourner les ressources de la clientèle. A ces problèmes, les banques et les clients chacun à leur niveau ont essayé de trouver des mesures pour préserver la qualité de leur relation.

WEBOGRAPHIE

www.wikipedia.org

www.bicec.com

www.cambiste.info

www.journaldunet.com