Meilleures pratiques pour la SÃ©curitÃ© des services bancaires en ligne
Internet
PostÃ© par : JulieM
PubliÃ©e le : 20/2/2012 11:30:00

Lorsquâ□□on aborde la question de **la sÃ©curitÃ© des services bancaires** en ligne, on se trouve confrontÃ© Ã **deux prÃ©jugÃ©s assez rÃ©pandus**, qui retiennent les institutions financiÃ¨res dâ□□offrir Ã leurs clients les meilleurs services possibles.

Câ□□est, du moins, lâ□□opinion dâ□□ **Hilding Arrehead**, Directeur monde des services aux professionnels chez ActivIdentity, que partage sa maison mÃ¨re, HID Global, leader reconnu sur le marchÃ© des solutions dâ□□identification sÃ©curisÃ©e.

Comme lâ□□explique **M. Arrehead** : Â« *Jâ□□ai eu le plaisir de collaborer avec des banques du monde entier, afin de les accompagner dans la conception et la mise en place de solutions de sÃ©curitÃ© dÃ©diÃ©es Ã leurs systÃ¨mes en ligne. Ainsi, mes collÃ¨gues et moi-mÃªme avons appris un certain nombre de choses sur les moyens Ã dÃ©ployer pour proposer des solutions Ã la fois sÃ©curisÃ©es et conviviales du point de vue de lâ□□utilisateur.*

Pour commencer, il faut savoir quâ□□une expÃ©rience utilisateur offrant un confort moindre lors de la connexion ne pose aucun souci, du moment que les clients se sentent en sÃ©curitÃ© et quâ□□ils ont accÃ¨s Ã un maximum de services bancaires en ligne (voire, de prÃ©fÃ©rence, Ã lâ□□ensemble des services proposÃ©s). Â»

Alors, comment utiliser les technologies de pointe actuellement disponibles pour concevoir un systÃ¨me bancaire en ligne bÃ©nÃ©ficiant dâ□□une sÃ©curitÃ© renforcÃ©e, tout en garantissant un vrai confort dâ□□utilisation et un accÃ¨s aussi large que possible Ã tous les services que vous souhaitez proposer ?

Voici les suggestions de M. Arrehead :

1. Laissez Ã vos clients le soin de choisir leur mÃ©thode dâ□□authentification lorsquâ□□ils se connectent, en fonction de lâ□□utilisation quâ□□ils entendent faire de votre service.

2. Donnez-leur la possibilitÃ© de configurer leurs propres niveaux de sÃ©curitÃ©.

3. Permettez-leur de dÃ©cider eux-mÃªmes depuis quel type de terminal ils se connectent.

4. IntÃ©grez votre systÃ¨me bancaire en ligne et sa sÃ©curitÃ© Ã vos autres activitÃ©s, afin de renvoyer Ã vos clients une image cohÃ©rente de votre approche en termes de sÃ©curitÃ©.

5. Autorisez-les Ã utiliser les mÃªmes identifiants pour leur banque en ligne que pour lâ□□accÃ¨s Ã dâ□□autres services bancaires.

6. Offrez-leur un accompagnement de qualitÃ© et suivant le mode qui leur convient : via une rubrique FAQ sur votre site Web, Ã travers une fonction de chat en ligne, par tÃ©lÃ©phone, par e-mail, en proposant des rendez-vous en face-Ã -face ou encore par courrier.

En matiÃ¨re de banque en ligne, lâ□□un des prÃ©jugÃ©s les plus courants consiste Ã penser que la problÃ©matique de la sÃ©curitÃ© peut tout simplement Ãªtre rÃ©solue, grÃ¢ce Ã une authentification dans les rÃ¨gles lors de lâ□□accÃ¨s au compte.

Â« *Ce nâ□□est pas de cette faÃ§on que jâ□□ai appris Ã envisager la question. Le vÃ©ritable risque encouru par les clients des banques en ligne, câ□□est de se faire voler de lâ□□argent sur leurs comptes. Partant de ce constat, il convient de se concentrer sur les moyens de sÃ©curiser les virements Ã proprement parler et non pas uniquement lâ□□accÃ¨s au service* Â», poursuit **M. Arrehead**.

Fort de son expÃ©rience auprÃ¨s de banques ayant rÃ©ussi la mise en place de leurs systÃ¨mes en ligne, il estime que celles-ci se sont contentÃ©es de cette approche et partage quelques-unes de leurs recommandations :

1. Rendez les choses aussi simples que possible. Pour valider une transaction, nâ□□exigez une signature que si lâ□□argent est virÃ© vers un compte nâ□□appartenant pas au client et autorisez les transactions en diffÃ©rÃ©.

2. Ayez recours Ã une technologie sÃ©curisÃ©e, mais adaptÃ©e au niveau de risque pour effectuer la signature. Les cartes Ã puce, les tokens matÃ©riels ou logiciels et les messages SMS sont autant de moyens appropriÃ©s pour procÃ©der Ã la signature Ã©lectronique.

3. Assurez-vous que lâ□□utilisateur identifie clairement ce Ã quoi se rapporte la signature Ã©lectronique. Cela permet de se prÃ©munir contre les menaces du type Â« man-in-the-middle Â», un risque particuliÃ¨rement important aujourdâ□□hui en raison des rÃ©centes attaques dont ont Ã©tÃ© victimes certains des fournisseurs de certificats comptant parmi les plus fiables et du piratage des mÃ©canismes liÃ©s aux protocoles de sÃ©curisation (SSL/TLS) utilisÃ©s par les navigateurs Web. (blog activIdentity)

4. Sauvegardez les informations relatives Ã la transaction, y compris la signature Ã©lectronique du client, en les archivant dans une base de vÃ©rification des donnÃ©es sÃ©curisÃ©e et inviolable. En effet, il peut sâ□□avÃ©rer trÃ¨s utile dâ□□Ãªtre en mesure de prouver quâ□□un virement a Ã©tÃ© correctement effectuÃ© et validÃ©, mÃªme aprÃ¨s plusieurs annÃ©es.

En conclusion, **M. Arrehead** souligne : Â« *De toute Ã©vidence, chaque banque a ses propres atouts, des dÃ©fis Ã relever et des besoins spÃ©cifiques en matiÃ¨re de sÃ©curitÃ©. Votre solution de sÃ©curitÃ©, y compris les mÃ©canismes dâ□□authentification et de validation des virements, doit donc nÃ©cessairement Ãªtre dÃ©finie avec prÃ©cision pour satisfaire ces exigences.* Â»