Internet : SÃ©curitÃ© des banques en ligne, le mythe !
Internet
PostÃ© par : JulieM
PubliÃ©e le : 13/2/2012 11:30:00

DerriÃ¨re la technologie et le produitâ¦ Le point de vue de lâexpert avec **Network Computing**. Cette master class a Ã©tÃ© organisÃ©e en partenariat avec**ActivIdentity**, passons au crible **deux mythes relatifs Ã la sÃ©curitÃ© des banques en ligne** et dÃ©montrons que les notions de service et de prÃ©fÃ©rences utilisateurs sâinscrivent au cÅur dâune politique de sÃ©curitÃ© efficace.

Deux mythes relatifs Ã la sÃ©curitÃ© des banques en ligne, des notions de service et de prÃ©fÃ©rences utilisateurs qui sâinscrivent au cÅur dâune politique de sÃ©curitÃ© efficace.

Mythe NÂ°1 : une politique de sÃ©curitÃ© en ligne renforcÃ©e incommode les utilisateurs et est source de mauvaises expÃ©riences pour eux.

Les banques appliquant les politiques de sÃ©curitÃ© les plus strictes disposent dâune meilleure capacitÃ© Ã satisfaire leurs clients et peuvent proposer plus de services que leurs concurrents moins fiables en la matiÃ¨re. Prenons lâexemple de cette banque, qui a lancÃ© son service en ligne en appliquant dÃ¨s le dÃ©part une authentification forte bi-facteurs basÃ©e sur un OTP (One-Time Password) pour chaque connexion : rapidement, elle a atteint 2,5 millions dâutilisateurs en ligne, malgrÃ© un processus de connexion basÃ© sur un protocole Â« dÃ©fi/rÃ©ponse Â».

Ãlaborer des systÃ¨mes en ligne qui soient Ã la fois riches en fonctionnalitÃ©s, fiables du point de vue de la sÃ©curitÃ© et pratiques pour les clients : voici le challenge auquel sont confrontÃ©es les institutions financiÃ¨res. Aussi, le fait dâoffrir aux utilisateurs la possibilitÃ© de choisir leurs options de sÃ©curitÃ© amÃ©liore la fidÃ©lisation, comme lâillustrent les exemples suivants.

â¢ En fonction de lâutilisation quâil entend faire du service , le client doit pouvoir choisir sa mÃ©thode dâauthentification favorite lorsquâil se connecte. En effet, un mot de passe pourra sâavÃ©rer suffisant pour visualiser le statut de ses diffÃ©rents comptes et rÃ©aliser un virement interne entre ces derniers.

â¢ Pour plus de praticitÃ©, il convient Ã©galement de permettre au client de configurer lui-mÃªme ses critÃ¨res de sÃ©curitÃ© selon ses usages. Lorsquâil est connectÃ© suivant une

mÃ©thode dâ□□authentification forte, via un OTP (One-Time Password) ou un message SMS, il doit Ãªtre possible de rÃ©initialiser le mot de passe ou bien dâ□□activer / de dÃ©sactiver totalement lâ□□accÃ¨s.

â□¢ Afin dâ□□autoriser le client Ã se connecter depuis le terminal de son choix, une banque en ligne proposera des applications dÃ©diÃ©es aux tÃ©lÃ©phones mobiles et aux tablettes. Cependant, lâ□□utilisation du navigateur Web intÃ©grÃ© Ã ce type dâ□□Ã©quipement nâ□□est gÃ©nÃ©ralement pas une bonne option. Mieux vaut concevoir ces applications en prenant en compte les questions de sÃ©curitÃ©, tout en restant attentif Ã leur compatibilitÃ© avec la politique de sÃ©curitÃ© et les Ã©quipements dâ□□authentification de lâ□□entreprise. De cette maniÃ¨re, quels que soient le terminal ou lâ□□application utilisÃ©s, lâ□□internaute aura accÃ¨s Ã un service de qualitÃ© constante dans un environnement familier et fiable.

â□¢ Certains clients souhaiteront obtenir leurs identifiants en se rendant directement dans leur agence, tandis que dâ□□autres prÃ©fÃ©reront que tout soit gÃ©rÃ© par tÃ©lÃ©phone. Quant aux plus connaisseurs, ils voudront parfois utiliser leur tÃ©lÃ©phone mobile en guise dâ□□OTP. Laissez-leur le choix.

Mythe NÂ°2 : lâ□□accÃ¨s Ã tout service doit, dÃ¨s les premiÃ¨res Ã©tapes, Ãªtre protÃ©gÃ© par les mesures de sÃ©curitÃ© les plus fortes.

Lâ□□augmentation du niveau de sÃ©curitÃ© doit Ãªtre liÃ©e au caractÃ¨re sensible des transactions rÃ©alisÃ©es. En effet, si la connexion Ã un compte en ligne peut Ãªtre protÃ©gÃ©e via une authentification par un simple mot de passe, lâ□□accÃ¨s Ã des virements requiert plus de rigueur. Inspirez-vous des meilleures pratiques prÃ©sentÃ©es ci-aprÃ¨s.

â□¢ Rendez les choses aussi faciles que possible. Par exemple, pour valider une transaction, nâ□□exigez une signature que si lâ□□argent est virÃ© vers des comptes extÃ©rieurs. Autorisez Ã©galement les transactions en diffÃ©rÃ©, que ce soit pour un paiement, un virement ou toute autre opÃ©ration nÃ©cessitant une signature.

â□¢ Pour effectuer la signature, ayez recours Ã une technologie sÃ©curisÃ©e, mais adaptÃ©e au niveau de risque. Les cartes Ã puce, les tokens matÃ©riels ou logiciels et les messages SMS sont autant de moyens de procÃ©der Ã la signature Ã©lectronique. Toutefois, pour permettre Ã un client de se connecter et de rÃ©aliser des opÃ©rations en ligne, une banque se contentera de lui demander un identifiant de sÃ©curitÃ© fort. De plus, lâ□□utilisateur devra pouvoir choisir, sans y Ãªtre contraint, dâ□□utiliser plusieurs identifiants.

â□¢ Les Ã©lÃ©ments validÃ©s par la signature Ã©lectronique doivent Ãªtre clairement identifiables. Cela est 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. Par exemple, dans le cas dâ□□un virement de 500â□¬ Ã©mis le 3 dÃ©cembre par le compte 12345678 vers le compte 87654321, les donnÃ©es relatives Ã la transaction peuvent Ãªtre rÃ©unies dans un sous-groupe, qui sera cryptÃ© (signÃ© Ã©lectroniquement) par le client, en utilisant un identifiant de sÃ©curitÃ© fort. Si lâ□□on a recours Ã un OTP, le nombre 5008321312 (500 Ã©tant le montant, 8 le dernier chiffre du compte Ã©metteur, 321 les trois derniers chiffres du compte destinataire et 312 la date de la transaction) sera enregistrÃ© dans le token dÃ©diÃ© au cryptage. Ce dernier retournera ensuite une version cryptÃ©e de ce numÃ©ro qui, une fois enregistrÃ© par le site Internet de la banque, sera validÃ© par son systÃ¨me comme Ã©tant la seule autre entitÃ© Ã avoir accÃ¨s Ã la mÃªme clÃ© de cryptage.

Si la fiabilitÃ© ne peut Ãªtre compromise, appliquer les meilleurs niveaux de sÃ©curitÃ© ne signifie pas nÃ©cessairement que lâ□□on appauvrit lâ□□expÃ©rience utilisateur. En rÃ©alitÃ©, en offrant

un certain niveau de contrÃ´le Ã lâ□□internaute, il est mÃªme possible dâ□□obtenir de meilleurs rÃ©sultats.