



>> ACTU / L'ÉVÈNEMENT

LUTTE ANTIFRAUDE : LE RÉVEIL DES BANQUES FRANÇAISES

●●● d'information qui l'ont compris dans les banques. « Comme la demande n'est pas très forte, on cherche à minimiser les coûts, plutôt qu'à innover au bénéfice de nos clients », se désole un responsable technique d'une grande banque française. La captivité des clients constitue un frein. Et le discours des responsables en sécurité se heurte à celui du marketing. Le constat fait par Daniel Savoyen est pourtant sans appel : « Les fraudeurs trouvent des failles et posent des pièges car, aujourd'hui, nous avons peu ou pas d'outils déployés pour sécuriser les systèmes

de façon efficace. » Ce n'est pas en attendant la multiplication des actes délictueux, et en criant au loup devant le « phishing », que les banques rassureront sur leur capacité à contenir la fraude en ligne. Mais en agissant avec les moyens modernes déjà maîtrisés par les équipes techniques en interne. La Société Générale a fourni plus de cinq mille tokens à ses employés, et la BNP Paribas plus de dix mille. Mais à leurs clients, aucun. A quand un plus juste équilibre ? ●

CHRISTOPHE DUPONT ELISE

INTERVIEW. Maître Fabrice Perbost, avocat associé, département IT/IP, cabinet Kahn & Associé

“La plupart des escroqueries sur internet proviennent de vols effectués dans le monde réel”

Quel est le dispositif légal en vigueur, en matière d'utilisation frauduleuse de cartes bancaires en ligne ?

Maître Fabrice Perbost : Le cadre juridique actuel a été défini par la loi du 15 novembre 2001, relative à la sécurité quotidienne. Ainsi, l'article L-132-4 du Code monétaire et financier prévoit que le titulaire d'une carte bancaire n'est pas responsable si le paiement frauduleux a été effectué à distance, sans utilisation physique de la carte.

Dans le cas d'une opération de « phishing », la responsabilité de l'entreprise dont le nom a été utilisé pour soutirer des informations bancaires à des internautes peut-elle être invoquée ?

MFP : En aucun cas. Car le caractère pénal de cette infraction suppose, en plus de l'élément matériel, un élément intentionnel. Or, le fait d'avoir vu sa marque utilisée par un tiers pour susciter la confiance de la future victime, ne suppose en rien la participation volontaire de ladite marque. Pour que sa responsabilité soit engagée, il faudrait démontrer que la marque, ou plutôt la société qui la détient, a délibérément participé à l'escroquerie.



J.-L. DESBINS

Quelles garanties le DSI doit-il présenter pour se prémunir contre ce type d'action ?

MFP : Il doit être en mesure de prouver la bonne foi de son entreprise. Et démontrer qu'il a tout mis en œuvre pour protéger les internautes qui se connectent à son site, afin de préserver les données les concernant. De même, il doit avoir informé les salariés des risques qu'ils prennent en communiquant leurs coordonnées, notamment bancaires, sur la Toile.

Concrètement, comment fait-on lorsque l'on a vu ses cartes bancaires ainsi piratées sur internet ?

MFP : La loi, en l'espèce l'article L-132-5 (ou L-132-4) du Code monétaire et financier, est formelle : en cas d'utilisation frauduleuse d'une carte, son émetteur doit rembourser à son titulaire la totalité des frais bancaires qu'il a supportés. Ce même Code prévoit que le titulaire d'une carte de retrait ou de paiement a la possibilité de déposer une réclamation dans les soixante-dix jours à compter de la date de l'opération contestée. ●

PROPOS RECUEILLIS PAR
 NICOLAS ARPAGIAN

QUESTIONS/REponses

L'authentification forte à grande échelle est-elle réaliste ?

AOL semble le penser. Aux Etats-Unis, il propose un token d'authentification forte RSA SecureID à tous ses abonnés qui le souhaitent. L'US Bancorp s'apprête à faire de même pour dix mille de ses clients entreprises, avec Verisign. En Suède, la Swedbank a déployé 1,7 million de tokens. Trois cent cinquante mille clients du Crédit Suisse accèdent de cette manière à leur compte. Le coût des jetons est supporté par le client. Ces déploiements sont en outre maîtrisés par les banques, qui utilisent déjà les tokens pour leurs propres besoins.

A quel stade en sont les banques françaises ?

Durant l'été 2003, et suite à plusieurs cas de « phishing », l'ensemble des banques françaises s'est concerté au sein d'un groupe de travail. Elles sont d'accord sur la nécessité de proposer de l'authentification forte, mais ne se sont pas entendues ni sur une date ni sur des solutions. Il a été très fortement affirmé qu'il n'était pas nécessaire de disposer d'un système d'authentification unique à toutes les banques. Ce qui laisse toute latitude à chacune d'effectuer ses propres choix technologiques. La tradition de coopération étant très importante pour les banques françaises, il y a fort à parier qu'elles débiteront leurs déploiements dans une fenêtre de tir réduite dès que l'une d'entre elles donnera le coup d'envoi. Probablement début 2005.