Le phishing continue d'empoisonner les banques

D'après la FSA (Financial Services Authority), le régulateur des services financiers britannique, le phishing est à l'origine d'une augmentation des arnaques bancaires en ligne de **8%** en deux ans.

Dans un rapport, l'autorité indique à la Chambre des Lords (House of Lords) qu'elle est préoccupée par cette situation.

Pour la FSA, il n'y a pas de doute, le phishing ou hameçonnage est à l'origine de ce problème qui ne fait que progresser.

L'utilisation massive par les escrocs de la toile de faux courriels bancaires pour récupérer les informations personnelles explique la progression de la fraude.

La FSA et l'association des banques Apacs ont apporté des preuves à la chambre haute du parlement du Royaume-Uni. Ils ont expliqué que ce problème progresse, mais qu'il était encore assez loin d'avoir atteint sa vitesse de croisière, ce qui est d'autant plus angoissant.

Les banques doivent miser sur plus de transparence

D'après nos informations, le FSA et l'Apacs auraient indiqué que le total de l'argent usurpé allait progresser de **90%** l'an prochain.

Sur les six premiers de 2005 le nombre d'attaques par phishing était de **312**, et sur les six premiers mois de l'année 2006 de **5.059**.

Mais pour le chef de la sécurité de l'Apacs, Philip Withaker, ce chiffre est trompeur, car en réalité il s'explique du fait d'un meilleur taux de détection.

En Grande-Bretagne, pas moins de 45 millions de livres ont été subtilisés en 2006 via le phishing. Et d'après l'Apacs, une banque est particulièrement ciblée. Malheureusement pour la liberté d'information, il est actuellement impossible de savoir laquelle puisque l'Apacs représente les banques et pas les consommateurs.

Et le souci de communication avec les consommateurs ne risque pas d'évoluer tout de suite. En effet, la FSA et l'Apacs ont indiqué qu'elles ne lanceraient pas d'alerte sur des failles de sécurité remarquées sur des sites.

Reste que pour mieux lutter contre le phishing les banques doivent être plus transparentes et mieux informer leurs clients des risques et des comportements à surveiller. Il s'agit aussi degénéraliser les outils d'authentification forte.

Et ce qui est vrai pour la Grande-bretagne, l'est aussi pour l'Hexagone.