Problèmes liés à la banque en ligne

Sujet: **Trafic des paiements** Numéro de cas: **2004/05**

> Un courriel informe le client de problèmes affectant les services électroniques de «sa» banque. Afin de résoudre ces problèmes, on lui demande de communiquer les identi.ants personnels requis pour accéder auxdits services (notamment numéro de contrat, code personnel et numéro de liste à biffer). Le client accède à cette demande et constate par la suite que l'on a disposé de ses avoirs en banque par voie électronique.

La banque électronique est un moyen très sûr de traitement des opérations bancaires. Pour pouvoir communiquer avec la banque, le client doit d'abord se légitimer. L'Ombudsman n'a connaissance d'aucun cas où l'on serait parvenu à pénétrer dans le système sans connaître les identi.ants (numéro de contrat, code personnel et numéro de liste à biffer ou processus similaire). Lorsqu'une erreur est signalée, c'est le plus souvent qu'il y a eu négligence ou intervention du client. L'escroc peut en effet se procurer les données requises de manière conventionnelle, par exemple en les volant ou en les copiant. Les identifiants informatiques doivent donc être conservés en lieu sûr et séparément les uns des autres. Le code, notamment, ne doit jamais .gurer à proximité de la liste de numéros à biffer.

Mais «l'intervention» du client peut aussi consister en ce que l'escroc parvient à le convaincre de lui communiquer ses identi.ants personnels. Tel peut être le cas lorsque, comme dans l'exemple précité, le client les donne de son plein gré, en pensant avoir affaire à sa banque. Mais il arrive aussi que l'escroc accède à l'ordinateur du client et le manipule de telle sorte que le client pense être connecté au site de la banque, alors qu'en réalité il s'agit d'un site de l'escroc – mais qui ressemble à s'y méprendre à celui de la banque.

Des moyens relativement simples permettent toutefois de prévenir ces risques. En premier lieu, le principe absolu est qu'une banque ne demandera jamais à un client ses identi.ants personnels. Toute demande de cet ordre, même la plus habilement présentée, est un faux. Le client ne doit donc en aucun cas y répondre. En second lieu, il appartient au client de sécuriser son ordinateur au moyen d'un parefeu et d'un anti-virus régulièrement mis à jour et de se conformer aux recommandations en vigueur (ne pas ouvrir sans ré.échir des courriels d'origine inconnue, ne pas installer de logiciels proposés par des fournisseurs douteux, etc.). Il est important aussi que le client se connecte directement au site Internet of.ciel de l'établissement bancaire et se déconnecte au moyen de la fonction du programme prévue à cet effet («logout»), plutôt que de se contenter de fermer la fenêtre du navigateur. Ensuite, il convient de vider la mémoire cache du navigateur, a.n qu'un éventuel pirate ne puisse pas voir les sites récemment visités par l'utilisateur. En.n, il est utile de véri.er si les ordres ont été correctement saisis (via «Paiements/ordres en suspens»), et ce pour deux raisons: d'une part, le client s'assure ainsi que tout est en ordre, puisque seule la banque possède les données requises; d'autre part, ceci permet de con.rmer que l'ordre a bien été enregistré et que donc – si les conditions requises sont remplies – il sera exécuté à la date prévue.

Des informations complémentaires relatives à la sécurité informatique ainsi que de nombreuses astuces, liste de contrôle et présentation pas à pas sont disponibles notamment sur le site Internet de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (www.melani.admin.ch).