La Caisse d'allocations familiales donne l'alerte !

Après le fisc (*cf.* Micro Hebdo *n°605*), c'est au tour de la CAF de lancer une campagne d'alerte contre le phishing. Ces derniers mois, des milliers d'internautes ont en effet reçu un e-mail semblant émaner de la Caisse d'allocations familiales les invitant, sous prétexte d'un remboursement de prestations familiales au titre de l'année 2009, à se connecter sur un site et à communiquer leurs données confidentielles (code d'accès, numéro d'allocataire, numéro de compte bancaire), dans le but de les escroquer à l'aide des coordonnées bancaires imprudemment communiquées. L'expéditeur de ces messages qui se fait passer pour la CAF (notamment en utilisant son logo), explique aux destinataires qu'ils sont bénéficiaires de 161,82 euros et que, pour percevoir cette somme, ils doivent cliquer sur un lien, puis fournir leurs coordonnées bancaires...

Chaque semaine, Me Alain Bensoussan, avocat à la cour d'appel de Paris et spécialiste en droit de l'informatique, vous informe de vos droits.

MARC MARTIN

La CAF a émis une alerte sur son site contre cette escroquerie électronique à grande échelle, bien connue sous le nom de « *phishing* » ou « hameçonnage ». La CAF recommande sur son site (https://www.caf.fr/PopUpEnSavoirPlus.html) de supprimer aussitôt tout courriel de ce type. Aux allocataires qui auraient communiqué leurs coordonnées bancaires, elle recommande de prendre rapidement contact avec leur banque afin de faire opposition. C'est déjà la troisième alerte de ce type pour la CAF (octobre 2009 et février 2010). Selon le rapport 2009 de l'APWG, une association qui lutte contre le phishing, l'Europe serait de plus en plus touchée par ce phénomène. Cette cybercriminalité de masse se propage grâce au spam (diffusion de mails en grand nombre). Le « *phisher* » envoie des millions de spams en confiant cette tâche à un sous-traitant spécialisé, un spammeur. Elle est très difficile à endiguer, car, pour éviter le filtrage, le phisher dispose d'un site Internet dont l'adresse IP change continuellement, de manière à ne pouvoir être localisé. La plus grande prudence s'impose donc.