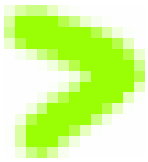
JURITICE

-- FAQ --

FAQ



Quelle est la conduite à tenir en cas de "phishing" sur le site de l'établissement ?

Catherine Guinoiseau

vendredi 20 avril 2007

Le phénomène de filoutage (« phishing ») est un acte de malveillance informatique aujourd'hui courant. En qualité d'utilisateur, il appartient à chacun d'être vigilant sur la provenance des pages dont les contenus sollicitent la communication d'un identifiant ou d'un mot de passe quels qu'ils soient. Ainsi, on se gardera de les communiquer sur une page dont l'accès a été indiqué par un lien figurant sur un message électronique reçu dans la boîte aux lettres. Par prudence, l'accès vers la page sera effectué à partir du site officiel de la structure en cause. Par ailleurs, il est important de vérifier si la connexion sécurisée (https://) est activée lors de l'entrée de ces identifiant et mot de passe afin que ceux-ci ne soient pas interceptés. Bien entendu, la sécurité du terminal utilisé doit être garantie par l'utilisation d'un antivirus, d'un pare-feu efficaces, et le nettoyage régulier de tous cookies, rootkits, chevaux de Troie… qui s'installent sur la machine à l'insu du propriétaire. Un phénomène de plus en plus répandu est également l'utilisation d'un serveur ou d'un poste comme plate-forme de diffusion d'actes malveillants. Ainsi, la France serait aujourd'hui le troisième pays le plus touché par les PC zombies. L'armée de PC zombies se monterait au total, dans le monde, à 6.049.594 ordinateurs… Un délinquant inventif peut parfaitement utiliser les ordinateurs de son établissement si ces derniers ne sont pas suffisamment sécurisés afin de dissimuler sa réelle identité pour pratiquer des actes par exemple de filoutage. La conduite à tenir, dès lors que de tels agissements sont révélés, est de déposer plainte auprès des services de Police ou de Gendarmerie contre X, dès lors que l'auteur des agissements n'est pas connu. Le deuxième réflexe qui doit être observé est d'isoler les données litigieuses qui pourront être décelées mais de les conserver afin que les services d'enquête puissent les recueillir et les examiner. Une solution efficace mais plus coûteuse peut également être constituée par un constat d'Huissier de Justice, lequel devra être compétent en matière de constat informatique. La journalisation de l'activité sur le réseau pourra être également un outil efficace et indispensable pour déterminer la provenance des agissements (identification des comptes par exemple). Le troisième réflexe est bien évidemment celui de sécuriser le réseau et, notamment, de mettre en œuvre toutes les solutions permettant d'éviter que le phénomène se reproduise. Les solutions peuvent être uconstituées par un cloisonnement des postes et des espaces sur le réseau, une désactivation de l'ensemble des identifiants et mot de passe suivie d'une réattribution à chaque utilisateur, une vérification de la sécurité des applications utilisées, et éventuellement la suspension de leur utilisation...