



# CASES articles

Le phishing : une juteuse arnaque pour les criminels

## Vol d'identité et cambriolage de banque grâce au phishing

**Pour plus de sécurité, adoptez les réflexes CASES !**

### Les attaques de phishing sont de plus en plus sophistiquées

**Le vol de données privées et d'informations connaît une professionnalisation croissante dans le cyberspace. Outre les attaques bien connues de phishing par le biais d'e-mails sous forme de spam, les attaques ciblées sont de plus en plus employées. Les méthodes d'attaque sont caractérisées par une technique de plus en plus sophistiquée, ce qui rend également plus difficile la poursuite des malfaiteurs. Le phishing étant un marché lucratif pour les cybercriminels, il est fortement recommandé aux internautes d'adopter les réflexes de sécurité adéquats et d'appliquer des mesures de protection techniques.**

Le Luxembourg n'est pas épargné par les attaques de phishing à l'échelle mondiale et bon nombre d'utilisateurs luxembourgeois ont déjà reçu des e-mails de phishing. Ce sont en particulier les banques qui sont visées par ces attaques touchant le Luxembourg depuis 2007. Les criminels, qualifiés de phishers, tentent par ce biais d'obtenir l'identité des utilisateurs, leurs mots de passe et leurs numéros de carte de crédit.

Le portail de sécurité PhishTank, qui a pour vocation de collecter des informations sur les attaques de phishing, établit des statistiques sur les cibles privilégiées au niveau mondial. Aux deux premières places de ce classement figurent eBay et PayPal, suivis de la Bank of America Corporation.

### Attaques de phishing et méthodes courantes

L'attaque typique d'un phisher peut se résumer en quelques étapes. Dans un premier temps, le phisher se procure les adresses e-mail de victimes potentielles. Ensuite, il crée une adresse e-mail et un texte semblant légitimes et officiels. Le texte de l'e-mail est structuré de manière à inciter les destinataires à cliquer sur un lien hypertexte manipulé. Ce lien doit les attirer vers une page Internet falsifiée, ressemblant à s'y méprendre à la page originale. Ceci se fait d'ailleurs à l'insu de l'utilisateur. L'e-mail est ensuite envoyé aux victimes potentielles qui figurent sur la liste d'adresses du phisher. Au cours de la dernière étape, l'attaquant recueille les données que ses victimes ont révélées sur la page Internet falsifiée. Il peut ensuite les utiliser à sa guise : l'utilisation abusive de l'identité des usagers d'Internet ainsi bernés est maintenant possible. Le phishing est donc une forme moderne d'usurpation d'identité et de cambriolage de banque.

Différentes formes d'attaques de phishing s'inspirent de la méthode décrite précédemment. La méthode la plus simple consiste en l'envoi en masse d'e-mails de phishing sous forme de spam.

Mais les pirates ont de plus en plus souvent recours à des attaques ciblées, nommées « spear phishing ». À cet effet, ils utilisent des informations détaillées obtenues lors de vols de données, comme celui perpétré au détriment du portail de recherche d'emploi [www.Monster.com](http://www.Monster.com) en 2007.

Le phishing représente pour les criminels un segment de marché lucratif dans lequel ils ne risquent guère de poursuites. Les mécanismes de protection, pourtant en amélioration constante, sont encore en retard par rapport aux méthodes hautement professionnelles de phishing. Ceci est en particulier le cas lorsque des malwares sont utilisés, tels que des chevaux de Troie, vers, virus, etc. Les phishers exploitent alors les faiblesses des utilisateurs et mettent en œuvre des méthodes d'attaque techniques, telle l'installation d'un cheval de Troie sur l'ordinateur de leur victime. Les attaquants travaillent en général avec des leurres (offres alléchantes), comme des jeux gratuits ou très bon marché par exemple. Dès que l'utilisateur installe un tel jeu, son ordinateur est automatiquement infecté par un cheval de Troie, sans qu'il en soit conscient.

Les attaques les plus récentes exploitent également les vulnérabilités de pages Internet fortement fréquentées afin d'infecter leurs visiteurs à l'aide de chevaux de Troie.

### Tendances et conséquences possibles du phishing

Les cybercriminels ne se limitent pas à employer des méthodes professionnelles lors de leurs attaques, ils sont également passés maîtres dans l'art d'effacer leurs traces. La tendance est à l'utilisation de « Fast Flux » ou « Double Flux ». Dans ce cas, des centaines, voire des milliers d'adresses IP sont attribuées à un nom de domaine. L'adresse IP du nom de domaine concerné peut alors être modifiée très rapidement, toutes les trois minutes par

exemple, ce qui rend très difficile de remonter jusqu'à la page de phishing et de la neutraliser.

Dave Jevans, président de l'Anti-Phishing Working Group (APWG), estime que l'escroquerie au phishing est en progression et qu'elle devient plus complexe : « *Nous constatons une utilisation croissante de JavaScripts, de pop-up et de scripts intersites conçus pour tromper même les utilisateurs expérimentés. Notre certitude de pouvoir utiliser l'Internet en toute sécurité pour effectuer des transactions commerciales et pour communiquer est en danger* », regrette-t-il.

Les préjudices occasionnés par le phishing sont difficiles à estimer. La confiance que l'on place dans les applications et l'utilisation du net pâtissent des risques liés à la perte de données. Les solutions d'e-commerce et d'e-banking requièrent des standards de sécurité toujours plus élevés, tant du côté des fournisseurs que de celui des utilisateurs.

## Éviter le phishing

Ce sont bien souvent l'inconscience des dangers et des risques du cyberspace ainsi que des connaissances techniques insuffisantes, tant des fournisseurs que des utilisateurs, qui rendent possibles les attaques de phishing.

Les usagers d'Internet devraient adopter les réflexes de sécurité CASES. Ils devraient ainsi veiller à ne pas communiquer de données personnelles par le biais de formulaires leur parvenant par e-mail. En outre, ils ne devraient jamais se connecter à un site en utilisant le lien présent dans un e-mail et ne jamais répondre à des e-mails leur demandant des informations confidentielles. Les e-mails reçus devraient être vérifiés avec soin, de même que les mouvements sur le compte bancaire. Il convient également de se rappeler que les institutions légitimes et les prestataires de services sérieux ne demandent jamais de données confidentielles par e-mail. De plus, il est recommandé d'utiliser un logiciel anti-virus régulièrement mis à jour, un pare-feu correctement paramétré ainsi qu'un programme anti-spyware.

### Cheval de Troie :

Un cheval de Troie est un programme ou une partie de programme semblant inoffensif, mais ayant pour but d'infecter un ordinateur ou un serveur à l'insu de l'utilisateur.

Ce programme ouvre un port réseau déterminé permettant à l'intrus de contrôler à distance l'ordinateur ainsi infecté. Un port réseau constitue une « porte virtuelle » donnant accès à un service proposé par un ordinateur connecté au réseau. Cette « porte » permet la réception et l'émission des données échangées à travers le réseau.

La fonction de protection du navigateur contre le phishing devrait en outre être activée. Les utilisateurs devraient veiller à ce que leur système d'exploitation et leurs programmes soient toujours à jour. De plus amples informations à ce sujet sont disponibles sur le portail de sécurité luxembourgeois [www.cases.lu](http://www.cases.lu).

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)