Pourquoi les victime de phishing, se feront encore piéger ?

Pourquoi les victime de phishing, se feront encore piéger ?

Des chercheurs américains ont établi que les internautes se font avoir par des faux e-mails parce qu'ils ont tendance à surestimer leurs capacités à les identifier comme tels.

De : Societe Generale > [mailto:AvisDePaiement@societegenerale.fr]
Envoyé : mercredi 18 mars 2015 12:19
À :
Objet : Avis de Paiement

SOCIETE GENERALE
Banque & Assurances

ESPACE ENTREPRISES

Bonjour Monsieur / Madame ,

A votre demande, veuillez trouver ci joint le paiement e-conseils pour votre reference.

Se il vous plait, cliquez ici

Cordialement

IMPORTANT : N'UTILISEZ PAS LA FONCTION "repondre a" ,
LAQUELLE NE NOUS PERMET PAS DE TRAITER VOTRE DEMANDE.

Vous pouvez télecharger gratuitement la derniere version du logiciel Acrobat Reader a partir du site d'Adobe a l'adresse suivante :
http://www.adobe.fr/products/acrobat/readstep2.html

Ce message et toutes les pieces jointes (ci-apres le « Message) sont confidentiels et etablis a l'intention exclusive de ses destinataires
utilisation ou diffusion non autorisee est interdite. Si vous avez recu ce Message par erreur, merci de nous en avertir immediatement
declinent toute responsabilite au titre de ce Message s'il a ete altere, deforme, falsifie ou encore edite ou diffuse sans autorisation.

Groupe societe generale

Un e-mail de type phishing prétendant provenir de la Société générale et incitant le destinataire à cliquer sur un lien en lui promettant un paiement.
Le phishing est peut-être une vieille arnaque par e-mail, mais elle marche encore très bien. Pas seulement parce que ces faux e-mails officiels sont de mieux en mieux faits mais aussi parce que les internautes se croient beaucoup plus forts qu'ils ne le sont en réalité pour les détecter… Trois chercheurs américains sont arrivés à cette conclusion après avoir mené une expérience assez pointue auprès de 600 personnes. Le compte rendu a été publié dans Journal of the Association for Information Systems. Et le bilan est sans appel : les internautes se surestiment largement.
L'idée était en effet de voir comment les internautes jugeaient leurs propres compétences à repérer des e-mails frauduleux, plutôt que de voir s'ils étaient capables de déjouer cette arnaque. Pour rappel, les courriers de phishing se présentent comme des courriers officiels de banque, d'assurance, de site d'e-commerce, d'opérateurs de télécommunication, parfois des impôts, avec texte à tonalité toute administrative, mentions légales et logo officiel pour les plus soignés. Ils demandent généralement au destinataire de cliquer sur un fichier attaché (en réalité un virus) ou de mettre à jour ses informations en cliquant sur un lien renvoyant vers un formulaire. L'internaute n'aura plus qu'à remplir. Le plus souvent, il est question de saisir des identifiants et des données bancaires… La force de cette arnaque réside dans le fait que c'est la victime qui a donné elle-même les informations. Il suffit pour cela que le mail soit bien fait, bien rédigé, l'adresse de l'expéditeur assez trompeuse.

Une étude en forme de sondage

Les trois chercheurs américains, issus de l'université du Texas (à Arlington et San Antonio) et de l'université Columbia, ont demandé à six cents participants de se soumettre à un sondage concernant l'examen de seize e-mails (présentés sous forme de fichier image). Tous étaient d'authentiques messages réellement envoyés, mais la moitié était du phishing, l'autre moitié de vrais e-mails d'entreprises.
De chaque message, les personnes ont dû dire si elles pensaient qu'il émanait réellement de l'entreprise censée l'avoir envoyé ou s'il était faux. Elles devaient aussi noter leur propre jugement sur une échelle de 50 à 100 : 50, si elles avaient répondu au hasard sur la fiabilité de l'e-mail, 100 si elles étaient parfaitement sûres de leur coup. Les chercheurs ont également demandé aux répondants à quel point ils étaient familiers (de « pas du tout » à « très ») de l'entreprise expéditrice et, à la fin, les participants étaient tenus d'estimer le pourcentage de bonnes réponses qu'ils pensaient avoir fournies.
Les enquêteurs ont également noté le temps mis par chaque participant à répondre à la première question (l'e-mail est-il légitime ou non), et ce pour les seize e-mails. Le tout était agrémenté de questions plus génériques sur la capacité des répondants à distinguer, dans l'absolu, des e-mails légitime d'emails de phishing, sur leurs activités en ligne, leur expérience, en tant que victime, du phishing.

Avoir été victime d'e-mails de phishing n'aide pas plus à les repérer

« Nous avons comparé chaque jugement des répondants sur la confiance qu'ils avaient dans leurs propres réponses à la justesse effective de la réponse, explique Jingguo Wang, de l'université du Texas à Arlington. *Nous avons découvert que 80% des participants avaient une confiance moyenne plus élevée que le taux de justesse de leurs réponses.* » Et quand il s'est agi pour les participants d'estimer combien de bonnes réponses ils avaient donné quant à la légitimité ou non des e-mails, les chercheurs se sont aperçus que 45% s'étaient surestimés.
L'enseignement de cette étude ? *« La confiance qu'ont les internautes dans leur propre jugement et dans leur efficacité à détecter du phishing n'est qu'un faible indicateur de ce qu'il en est vraiment, on ne peut pas se fier à cette confiance »* continue Jingguo Wang. Pire: même le fait que des participants aient eux-mêmes été victimes de phishing ne les aide pas à mieux reconnaître ce type d'e-mail. Le meilleur moyen d'apprendre à les détecter reste donc des séances de formation en bonne et due forme, à la fois sur la forme des messages eux-mêmes et sur la surconfiance des internautes, sur les raisons qu'ils ont de s'estimer si habiles à déceler ce genre de mails alors qu'ils ne sont pas tant que ça.
Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr

---

Réagissez à cet article

Original de l'article mis en page : Pour détecter du phishing, l'internaute moins fort qu'il ne le croit – Sciencesetavenir.fr