PrimaryCare

La sécurité sur Internet – 2e partie: Phishing

Angel Vilaseca

Continuons notre voyage dans le bestiaire internet. Imaginez que vous recevez l'e-mail suivant. Notez qu'il ne s'agit pas d'une simulation, un de mes amis l'a réellement reçu.

Dear Customer:
Recently there have been a large number of cyber attacks pointing our database servers. In order to safeguard your account, we require you to sign on immediately.
This personal check is requested of you as a precautionary measure and to ensure yourselves that everything is normal with your balance and personal information.
This process is mandatory, and if you did not sign on within the nearest time your account may be subject to temporary suspension.
Please make sure you have your Citibank(R) debit card number and your User ID and Password at hand.
Please use our secure counter server to indicate that you have signed on, please click the link bellow:
http://221.139.2.111/citifi/
!! Note that we have no particular indications that your details have been compromised in any way.
Thank you for your prompt attention to this matter and thank you for using
Citibank(R)
Regards,
Citibank(R) Card Department
(C)2004 Citibank. Citibank, N.A., Citibank, F.S.B.,
Citibank (West), FSB. Member FDIC.Citibank and Arc
Design is a registered service mark of Citicorp.

C'est un message qui a de quoi inquiéter, si on est client de la banque en question, n'est-ce pas? D'accord, mais surtout, ne faites pas ce qu'on vous demande dans ce mail!
C'est une nouvelle menace qui plane depuis quelques mois sur les internautes: le *phishing*, encore appelé «hameçonnage» ou «pêche aux données personnelles». L'étymologie du mot *phishing* pour *fishing* est à rapprocher de *phreaking*, pour *freak*, *freaking*, qui désignait dans les années 1970, une des activités des premiers hackers. Elle consistait, au moyen d'appareils électroniques bricolés, à envoyer des tonalités subaudibles dans la ligne téléphonique, afin de pouvoir téléphoner sans payer, ou encore empêcher la compagnie de téléphone de pouvoir vous localiser.
Le principe du phishing n'est pas nouveau. Depuis la nuit des temps, des escrocs, se faisant passer pour un employé de banque, appelaient des personnes pour leur demander de «confirmer» leurs coordonnées bancaires, puis utilisaient ces données pour puiser dans leur compte. Naturellement, l'escroc devait appeler les personnes une par une. Désormais, le progrès permet de faire mieux ... hélas.
Les victimes du phishing reçoivent un faux courriel, apparemment authentique, utilisant l'identité par exemple d'une institution financière, de votre fournisseur d'accès Internet ou d'un site commercial connu, dans lequel on demande aux destinataires, sous différents prétextes, de mettre à jour ou de «valider» leurs coordonnées bancaires ou personnelles.
En général, le message contient une menace pour le cas où on ne ferait pas dans un court délai ce qu'il demande, par exemple de fermer votre compte ou bien de vous facturer une pénalité.
Pour mettre à jour les coordonnées, l'e-mail contient un lien sur lequel il vous demande de cliquer et qui vous mène vers un site Web, qui a exactement le même aspect que celui de l'institution citée dans l'e-mail mais qui est en réalité une copie conforme fabriquée par le hacker. Là, on vous demande de donner vos coordonnées et mots de passe.
Le pirate récupère ces informations, dans le but de les utiliser pour détourner des fonds à son avantage. Ces e-mails sont envoyés au hasard, à un maximum de destinataires, selon les mêmes techniques que le spam. Beaucoup seront ignorés par les destinataires avertis, ou qui ne possèdent pas de compte dans la banque citée, mais un certain nombre se laisseront prendre, transmettront leurs données et le hacker s'empressera de siphonner leur compte en banque avant de disparaître.
Il semblerait qu'en 2003, aux Etats-Unis, le phishing ait touché près de 10 millions de personnes. Il aurait coûté 48 milliards de dollars aux institutions et 5 milliards aux particuliers (chiffres non vérifiés).
Pour se prémunir contre le phishing, il faut savoir que:

- Aucune société ou institution ne vous demandera jamais d'envoyer vos données personnelles par courriel! Ne divulguez jamais vos codes d'accès personnels (mots de passe, NIP).
- Si vous avez l'impression que vos échanges par courriel sont inhabituels, contactez immédiate-

* Der Ärztegrossist Zur Rose hat ein Artikel-unabhängiges Sponsoring für die Rubrik «Medizinische Informatik» übernommen. Die Beiträge in dieser Rubrik entstehen vollkommen unabhängig von diesem Sponsoring und durchlaufen den normalen redaktionellen Review-Prozess. Durch die direkte Beteiligung an den Produktionskosten ermöglicht das Rubrik-Sponsoring die kostenlose Zustellung von PrimaryCare an alle Hausärztinnen und Hausärzte in der Schweiz. Die Herausgebergesellschaften und die Redaktion danken der Firma «Zur Rose» herzlich für ihre Unterstützung.

ment (par téléphone) la société avec laquelle vous croyez être en rapport.

Un petit rappel des mesures de sécurité classiques pour les mots de passe n'est jamais de trop.

Utilisez un mot de passe avec un maximum de caractères. Evitez les noms, prénoms, dates de naissance, etc. Le mieux, c'est une combinaison de lettres majuscules et minuscules, de signes et de chiffres. Si possible, le mot de passe doit être modifié régulièrement. Il ne faut pas le noter à proximité du lieu où il sera utilisé (exemple: NIP noté sur la carte de crédit!)

Le problème, c'est comment se rappeler d'une combinaison de lettres et de chiffres qui ne veut rien dire! Un bon moyen mnémotechnique est de choisir une phrase (par exemple: Maman a acheté 3 petits Cochons, 1 qui ... etc.) et de prendre l'initiale de chaque mot, plus la ponctuation, ce qui dans notre exemple, donnerait: Maa3pC,1q.

Voilà un excellent mot de passe, correspondant en tous points aux critères demandés. De plus, comme ce sont les souvenirs les plus anciens qui disparaissent en dernier, ce mot de passe devrait être même longtemps à l'épreuve de la maladie d'Alzheimer!

Dr Angel Vilaseca
8, pl. du Rondeau
CH-1227 Carouge
avilaseca@bluewin.ch