CLCV
CONSOMMATION LOGEMENT ET CADRE DE VIE
citoyens au quotidien

Journée mondiale des droits des consommateurs 2017

JOURNÉE MONDIALE DES DROITS DES CONSOMMATEURS 2017

Apprendre à reconnaître le phishing

Le phishing (ou hameçonnage ou filoutage) est une escroquerie qui a fait plus de 2 millions de victimes en France en 2015.

Une imitation soignée

Un mail de phishing est envoyé par un pirate informatique, il imite un message qu'aurait pu envoyer un interlocuteur avec lequel on a l'habitude de correspondre. Il comporte le nom et le logo habituellement utilisés par le professionnel dont l'identité est usurpée.

Ces mails frauduleux sont des imitations qui semblent par exemple émaner du fournisseur d'énergie, de la banque ou du fournisseur téléphone/internet. Des organismes comme la sécurité sociale ou les impôts peuvent également être l'objet de phishing.

Les pirates vont décrire une situation d'urgence pour inciter le consommateur à agir le plus vite possible et ainsi ne pas trop réfléchir au bien-fondé de la demande. Les scénarios utilisés sont très nombreux : éviter une coupure du service suite à un soi-disant impayé, recevoir le remboursement d'un trop perçu imaginaire.

Le but du phishing est toujours le même, obtenir des coordonnées bancaires ou des codes confidentiels pour pouvoir ensuite prélever frauduleusement sur le compte en banque de la victime.

Un piège de plus en plus perfectionné

Les avertissements répétés auprès du grand public se heurtent à une évolution constante de cette arnaque :

- Les scénarios développés par les pirates sont multiples et les mails de phishing ne sont aujourd'hui plus des imitations grossières repérables aux nombreuses fautes d'orthographe.
- Certains pirates informatiques sont en mesure d'adresser des mails de phishing avec les nom et prénom de leur victime.
- Un mail de phishing peut contenir deux sortes de pièges :

- Un lien cliquable qui mène vers un faux site internet du professionnel dont l'identité est usurpée, l'internaute est alors incité à rentrer ses codes d'accès.
- Une pièce jointe qui, si elle est ouverte, infectera l'ordinateur avec un logiciel malveillant qui prendra discrètement possession de l'ordinateur en captant les données sensibles (comme les données bancaires). Ce logiciel malveillant peut également prendre possession de la boite mail du consommateur et envoyer en son nom des mails de phishing à ses contacts.

Les règles à adopter

Face à cette recrudescence de mails de phishing et aux refus de remboursement, très contestables, opposés par certaines banques la prudence doit être de mise :

- Doit être considéré comme frauduleux un email qui vous demande des coordonnées bancaires ou de l'argent, même s'il comporte vos nom et prénom et/ou semble provenir d'une adresse mail connue. En cas de doute, et malgré l'urgence qui est décrite, il faut prendre le temps de vérifier directement auprès de l'expéditeur supposé s'il en est bien l'auteur.
- Sur ces emails suspects, il ne faut jamais ouvrir les pièces jointes, utiliser les liens cliquables ou les coordonnées téléphoniques qui y figurent. Tous ces éléments font partie du piège.
- Il existe certains outils pour vous aider à lutter contre ce fléau. La plupart des navigateurs internet disposent d'une fonctionnalité d'avertissement contre le phishing et il existe des logiciels de filtre anti-pourriel. Mais ces logiciels ne sont pas parfaits et ne remplacent pas la vigilance de l'internaute.

Enfin, il est indispensable d'installer sur son ordinateur un antivirus et un anti-malware et de les mettre à jour très régulièrement.