

## PHISHING : la carte bancaire inactive

Les escrocs savent surfer sur l'actualité pour accomplir leurs méfaits.

Dernier exemple en date signalé par l'un des 165 correspondants du Réseau anti-arnaques : alors que la presse évoque le sort réservé aux comptes bancaires sans mouvement, (*facturation de frais voire clôture*), le message émanant de [support@c-entropay.com](mailto:support@c-entropay.com), et comportant en objet la mention « Avis de compte E-carte bleue inactif » incite le consommateur à cliquer sur un lien.

*« Nous avons constaté que votre compte n'a pas été utilisé pendant 183 jours. Afin de protéger votre compte, nous l'avons désormais classé comme inactif.*

*Quelles sont les conséquences pour vous ? Vous devez réactiver votre compte avant de pouvoir l'utiliser. Votre mot de passe vous sera également demandé. Si vous ne réactivez pas votre compte celui-ci restera inactif. »*

De tels messages visant à obtenir les codes d'accès à votre compte et les références de votre carte bancaire relèvent du phishing (*hameçonnage*) : ils n'émanent pas de votre banque.

Comment les détecter ? Le style original du texte et les fautes d'orthographe peuvent vous alerter. Mais, surtout, c'est l'adresse mél d'origine qui doit attirer votre attention.

INFO-ALERTE est une mise en garde hebdomadaire diffusée par le :  
Réseau anti-arnaques, association partenaire de l'UFC-Que Choisir  
BP 60512, La Chapelle Saint Laurent, 79306 BRESSUIRE cedex  
([contact@arnaques-infos.org](mailto:contact@arnaques-infos.org)) - Site : [www.arnaques-infos.org](http://www.arnaques-infos.org)  
SIRET : 503 805 657 00031  
Reproduction autorisée sous réserve de mentionner l'origine.  
Directeur de la publication : **Pascal TONNERRE**

