COMMENT RECONNAÎTRE UN COURRIER ÉLECTRONIQUE FRAUDULEUX ?

INTRODUCTION

Le courrier électronique est un support privilégié pour la diffusion de canulars, de virus et de désinformation ainsi que pour les tentatives de fraude et de vol d'informations personnelles (mots de passe, numéros de carte bancaire, etc.).

Cette fiche pratique se propose de vous donner les éléments clés pour identifier les courriels frauduleux et pour déterminer la meilleure manière de les traiter.

Vous pouvez également vous reporter à tout moment aux articles et documents de la section **[Sécurité des Systèmes d'Information]** sur **Eduline** (dans la rubrique **[Infos académiques]**).

L'HAMEÇONNAGE

L'hameçonnage (ou « phishing ») est actuellement le type de message frauduleux le plus répandu. Il s'agit pour l'expéditeur de tenter de vous tromper en simulant un courrier électronique émanant d'une banque, d'une institution ou encore d'un fournisseur de service internet. Le but est de vous attirer sur un site internet factice sur lequel on vous demande de saisir des informations confidentielles, par exemple des informations de connexion (identifiant et mot de passe) ou des coordonnées bancaires, afin de vous les voler.
Bien souvent, vous pouvez vous rendre compte de la supercherie en observant l'adresse internet sur laquelle vous envoie le lien du message. Elle n'a rien à voir avec l'adresse de l'organisme en question.

Dans tous les cas et quoi qu'il arrive, aucun organisme réel ne vous demandera par mail ou par téléphone votre mot de passe ou vos coordonnées bancaires, ni même ne vous demandera d'aller les saisir sur une page web pour les confirmer.
Ce genre de message est à coup sûr une tentative de phishing et la meilleure solution consiste à jeter le courriel à la poubelle sans état d'âme.

LES CANULARS

Les chaînes de solidarité, les demandes à l'aide de la part d'un inconnu ou les messages vous annonçant que vous avez gagné à la loterie existaient déjà par le courrier papier. Le format numérique a permis leur multiplication effrénée. À cela s'ajoutent les messages alertant sur de nouveaux virus effrayants et le plus souvent imaginaires.
Certains de ces canulars ont été initiés uniquement pour le plaisir pervers de leur auteur, d'autres ont des buts plus concrets comme l'engorgement des serveurs de messagerie, la désinformation visant certaines sociétés, certains organismes ou des personnes physiques, la propagation de véritables virus ou encore des tentatives de fraude.

Ce type de message est dans 99,99 % des cas un canular. D'une manière générale, ne propagez un message à tous vos correspondants que si vous avez vérifié l'information de façon certaine. Pour vous aider, consultez le site www.hoaxbuster.com. Il recense la plupart des « hoax » (canulars). D'autres sites sont utiles, comme les encyclopédies virales des éditeurs d'antivirus.

LES MESSAGES PORTEURS DE VIRUS

Les messages visant à propager des virus continuent d'être diffusés régulièrement. On appelle ces virus des « vers » ou des « chevaux de Troie ». Ils sont bien souvent destinés à l'installation d'autres virus nommés « cryptolockers » ou « ransomwares » qui vous interdisent l'accès à vos données en les chiffrant. Une fois que vous êtes infecté, un pirate vous contacte et exige une rançon en échange du système de déchiffrement de vos fichiers.

Les messages frauduleux sont généralement émis par un programme qui dispose d'un carnet d'adresses volé. C'est ainsi que vous pouvez recevoir un message venant de l'adresse de courriel d'une de vos connaissances et vous parlant d'un sujet totalement incongru, qui, de plus, est souvent en anglais ou en mauvais français, et contient une pièce jointe ou un lien Internet que le texte vous invite à ouvrir.

Si vous ouvrez la pièce jointe ou visitez la page Internet, cela pourrait bien déclencher l'installation d'un virus sur votre ordinateur. Il ne resterait alors plus qu'à espérer que votre antivirus est bien à jour afin qu'il interrompe automatiquement le processus.
La bonne réaction face à ce type de message et purement et simplement de le supprimer, et en aucun cas d'ouvrir la pièce jointe ou de cliquer sur le lien.