Zeitschrift: Générations
Herausgeber: Générations, société coopérative, sans but lucratif
Band: - (2016)
Heft: 76

Artikel: Stop aux e-mails malveillants!
Autor: Santos, Barbara
DOI: https://doi.org/10.5169/seals-830534

Stop aux e-mails malveillants !

Les courriels peuvent être source de virus et d'arnaques. Sachez comment les détecter !

Chaque jour, nous recevons en moyenne 35 e-mails non désirés. Si la plupart sont filtrés par nos fournisseurs de messagerie, certains passent entre les mailles du filet et cachent de redoutables arnaques.

Gains à la loterie, fermeture de compte… Les expéditeurs malintentionnés rivalisent d'idées pour soutirer des informations ou de l'argent. Quelques réflexes permettent toutefois de repérer rapidement ces pièges.

Le premier sera de toujours vérifier l'adresse de l'expéditeur. Et nul besoin d'être un as de l'informatique pour faire le tri : si vous ne connaissez pas l'adresse ou que celle-ci ne semble pas sérieuse, mélangeant notamment des chiffres et des lettres, jetez directement le courriel. S'il s'agissait vraiment d'une personne de confiance, elle trouvera un autre moyen de vous contacter.

NON AUX SOLLICITATIONS !

Autre indice mettant la puce à l'oreille : les sollicitations. Pour arriver à leurs fins, les importuns ont presque toujours besoin qu'on leur donne des informations, soit en remplissant un formulaire, soit en cliquant sur un lien. C'est la technique du phishing *(lire ci-contre)*. Ignorez toutes les demandes de données personnelles, de mises à jour ou de téléchargement si vous n'avez rien demandé. D'autant plus si une requête se montre pressante ou comporte des fautes d'orthographe.

Et, en cas de doute avec un courriel provenant d'une personne ou d'une entreprise connue, rien ne vaut un traditionnel coup de fil avant d'ouvrir quoi que ce soit. Une société de confiance ne vous contactera jamais par e-mail pour envoyer ou obtenir des informations confidentielles.

Selon Cathy Maret, porte-parole de Fedpol, l'arme absolue pour détecter les fraudes reste l'instinct de méfiance : « Il faut considérer nos actes sur le web comme s'ils étaient faits sur la place du village ou publiés dans le journal. »

PIÉGÉ ? LES BONS GESTES

Si vous pensez avoir commis un faux pas, commencez par modifier tous vos mots de passe en refusant la mémorisation proposée par les navigateurs.

Ensuite, signalez le cas à l'autorité compétente* : « Nous pouvons ouvrir une enquête et, si la fraude se passe en Suisse, l'adresse incriminée sera fermée », affirme Cathy Maret. Dans tous les cas, faites réviser votre ordinateur par un spécialiste. Car un appareil infecté peut également envoyer des mails frauduleux, à votre nom et à votre insu.

BARBARA SANTOS

**SCOCI : service de la lutte contre la criminalité sur internet de Fedpol : www.scoci.ch*

LEXIQUE DES ARNAQUES

Hoax : rumeurs annonçant un danger (virus informatique, santé publique, pétition, etc.) et demandant à être relayées à vos contacts.

Phishing : technique pour obtenir des renseignements confidentiels, souvent déguisée sous forme de messages venant d'un expéditeur connu (banque, opérateur, messagerie), imitant le graphisme et les logos officiels.

Scam : escroquerie promettant un gain en échange d'une avance financière pour couvrir des frais de notaire ou de voyage. Certains font même miroiter une histoire d'amour.

Sextorsion : extorsion de faveurs ou d'argent sous la menace de publication d'images privées, souvent à caractère sexuel et prises à l'insu de la victime, via la webcam.

Spam : messages publicitaires, inoffensifs à l'ouverture, mais qui peuvent mener vers des sites d'arnaque ou de commerce illégal.

Jobtravel