



CASES LUXEMBOURG

Série d'articles CASES : arnaques, escroqueries et attrape-nigauds

## Les escrocs du monde numérique

Pour plus de sécurité, adoptez les réflexes CASES !

### Tout ce qui brille n'est pas or

La diversité des offres farfelues est vaste, même dans le monde numérique. Les utilisateurs devraient connaître les formes d'arnaque courantes, ce qui éviterait des pertes d'argent et des tracas inutiles. Les victimes d'une arnaque ne doivent pas avoir peur de porter plainte. C'est la seule façon de mettre un terme aux agissements du cybercriminel. Les victimes peuvent trouver de l'aide et des conseils auprès d'organisations comme le centre de protection des consommateurs.

Le SMS envoyé le 13.04.2009 sur le téléphone mobile de Jan est clair : « demande de rappel ». Cet élève de 9 ans d'une école primaire luxembourgeoise montre fièrement son téléphone mobile pendant un cours sur la sécurité de l'information. « Cet appel sera surtaxé », explique la collaboratrice CASES Gabriela Rapp aux enfants. Elle ajoute que ce genre de piège marche non seulement sur les enfants, mais aussi sur les adultes. Or, avec les messages d'origine inconnue, la plus grande prudence est de rigueur.

Pour les collaborateurs du portail luxembourgeois CASES, cette scène se répète régulièrement lors des cours sur la sécurité de l'information pour les enfants et adolescents. « Ils représentent une proie facile pour les escrocs. Mais les adultes et entreprises tombent aussi dans les filets des cyberescrocs. Ces arnaques vont de l'acquisition de bonne foi de produits falsifiés à l'illusion de fausses connaissances en ligne, qui soutirent de l'argent à la victime. Les utilisateurs doivent donc connaître les principales formes d'arnaque et maîtriser les réflexes de sécurité qui conviennent », déclare François Thill, directeur de CASES.



### Escroqueries à l'achat et à la vente

#### Offres d'achat

De plus en plus d'utilisateurs proposent en ligne des objets dont ils veulent se débarrasser. Des contacts sont alors noués via Internet avec de nombreux acheteurs potentiels. Les offres d'achat frauduleuses typiques ressemblent à ça : « Bonjour. J'ai vu votre annonce pour la voiture d'occasion. Je suis prêt à l'acheter pour 2 800 euros. Je pourrais venir en prendre possession la semaine prochaine. Je compte régler par mandat postal. Vous pourrez prélever l'argent avec le code que je vous enverrai par e-mail. » La prudence est de rigueur avec ce genre de réponse. Plusieurs utilisateurs ont déjà fait la triste expérience de voir la marchandise enlevée sans que l'argent n'arrive jamais.

La possibilité d'un transfert de liquide n'est pas mauvaise en tant que telle. Quelqu'un verse une somme dans un bureau n'importe où dans le monde et

reçoit un code pour ce versement. Cette personne communique le code au vendeur pour qu'il puisse recevoir l'argent à l'autre bout de la planète. Ces systèmes sont pratiques car ils font gagner du temps et ne demandent pas de longues formalités. Mais il est conseillé aux utilisateurs de n'avoir recours à cette forme de transaction que s'ils connaissent bien le partenaire commercial. Pour les transactions entre étrangers, cette forme de transfert d'argent est vivement déconseillée. La prudence est aussi de mise avec les personnes inconnues qui proposent de payer par chèque. Rien n'indique que le chèque est couvert. Une vérification de provision prend du temps. Celui qui remet la marchandise avant toute vérification ne peut pas être certain qu'il recevra le paiement. Les utilisateurs doivent aussi être méfiants si l'offre d'un acheteur potentiel semble trop séduisante.

#### Messages trompeurs

« Perdez 10 kg facilement et sans efforts. Achetez les pilules minceur. Une silhouette de rêve en un mois sans modifier votre alimentation » ; « Trois nuits gratuites dans un hôtel cinq étoiles. Réservez sans attendre. Achetez un coupon hôtel » ; « Sautez sur l'occasion : un appareil photo à prix sensationnel ». Voilà des exemples de messages rencontrés sur Internet. Il s'agit souvent de messages destinés à induire l'internaute en erreur. Le but est d'attirer le consommateur dans un magasin ou l'amener à faire un achat.

Les utilisateurs doivent ouvrir l'œil et se méfier. Les escrocs aiment les avoir par des offres alléchantes. Il est important de lire les petits caractères. Avant de prendre une décision, l'utilisateur doit avoir lu et compris toutes les mentions écrites.

### **Billets de dernière minute**

Beaucoup d'utilisateurs se réjouissent parce qu'ils ont pu dénicher des tickets d'entrée pour le match de football, le concert ou le théâtre en toute dernière minute. Internet et ses prestataires ont été d'un grand secours : « Un événement " sold out " ? Nous avons encore des tickets. Payez en ligne et retirez vos tickets à la caisse. » Il n'est pas rare que la joie cède la place à la désillusion car l'arnaque n'est pas loin. Certains utilisateurs en ont déjà fait les frais. Parfois, la perte concerne non seulement le prix des tickets mais aussi les frais de déplacement et de nuitée.

Avant d'acheter un billet pour une manifestation par des voies non officielles, l'utilisateur doit toujours vérifier l'identité du vendeur et l'authenticité des billets. Il arrive en outre que des vendeurs annoncent qu'une manifestation est « sold out » alors que des tickets sont encore disponibles auprès de l'organisateur officiel et parfois à un prix plus avantageux. Ici aussi, il convient de vérifier les informations. Pour acheter des billets nominatifs, l'utilisateur doit en outre s'assurer qu'il sera admis à l'entrée avec un billet qui n'est pas établi à son nom. Ce n'est pas toujours le cas.

### **Mêmes produits mais bien moins chers**

Internet regorge d'offres pour les

mêmes produits à des prix plus bas. Exemples typiques : « Batteries pour ordinateur portable de stock ! Vente promotionnelle par deux » ; « Achetez ce parfum à son véritable prix ! » ; « Jeux de freins super avantageux, marques de distributeur. Vous ne verrez pas la différence ». Mais la marchandise convoitée ne répond pas toujours aux normes de qualité européennes. Les utilisateurs doivent être prudents ici car les produits proposés sont très vraisemblablement des contrefaçons. Explosions, empoisonnement ou dysfonctionnements peuvent entraîner des blessures sérieuses ou même mettre la vie de l'utilisateur en danger. De plus, le marché du faux empiète sur l'économie traditionnelle et sert souvent à financer la criminalité ou le terrorisme.

### **Le prix ridicule**

« Réservez votre voyage sans attendre. Tout compris. Cinq jours sur une plage de rêve pour 199 euros ». Ces messages promettent TOUT aux internautes. Mais le terme « TOUT » peut signifier des choses très différentes. Il est important ici de lire les petits caractères avant de conclure un contrat afin d'éviter des coûts supplémentaires inattendus.

### **L'arnaque aux gains**

#### **C'est très simple de gagner**

Recevoir un SMS de ce genre est très fréquent aujourd'hui : « Sonneries gratuites ! Envoyez un SMS avec RING au 1234 ». Les utilisateurs paient alors très cher pour les SMS qu'ils envoient mais aussi pour ceux qu'ils reçoivent. La marchandise n'est pas aussi gratuite qu'annoncé. L'utilisateur perd de l'argent en se retrouvant en outre parfois lié par un abonnement onéreux. C'est pourquoi il est généralement conseillé de ne pas répondre aux messages inconnus de ce type et de surveiller sa facture de téléphone mobile.

### **Le gros lot sans effort**

Il y a aussi des messages qui font croire aux utilisateurs qu'ils ont gagné une importante somme d'argent lors d'un tirage en ligne : « Félicitations, vous avez gagné 25 000 euros. Votre adresse e-mail a été tirée au sort dans un jeu de loterie. » La joie laisse souvent place à la désillusion. Il faut verser des frais de traitement pour recevoir le lot. Les utilisateurs ne

### **Conseil de sécurité : règles pour réduire les risques d'arnaque**

Lors d'achats en ligne, les utilisateurs doivent toujours vérifier si leur partenaire commercial est connu et si ce dernier peut être considéré comme fiable. S'il est inconnu, la prudence est de mise. Si les coordonnées du contact, comme l'adresse physique et le numéro de téléphone, ne figurent pas sur le site visité, toute transaction commerciale doit généralement être interrompue.

L'utilisateur ne doit jamais communiquer de données bancaires, un numéro de carte de crédit ou un code secret. L'achat d'articles ou de services doit toujours passer par des connexions sécurisées.

Même les mentions en petits caractères doivent faire l'objet d'une lecture attentive, un simple clic de souris suffisant à accepter l'intégralité des conditions générales. Celles-ci contiennent souvent des dispositions défavorables au consommateur.

Si un partenaire commercial demande le silence, il est plus que probable qu'il s'agit d'une arnaque. Les utilisateurs doivent s'informer et parler avec d'autres personnes de la proposition du partenaire commercial.

Quand quelque chose semble trop beau pour être vrai, il convient d'être vigilant. Cela vaut aussi bien pour l'achat que pour la vente ou les jeux-concours.

Il est conseillé aux utilisateurs de façon générale d'enregistrer le déroulement de transactions commerciales, ce qui permet d'avoir des preuves en cas d'escroquerie. Les victimes ne doivent pas avoir honte de leur naïveté mais porter plainte. C'est la seule solution pour mettre la main sur l'escroc.

doivent pas aller plus loin car les escrocs veulent seulement avoir leur argent par de fausses promesses. Personne ne voit jamais la couleur du gain.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)