Fraudes sur internet


© Alejandro Escamilla

Gare aux escrocs !

Le développement d'internet – et des multiples activités qui y sont proposées – a ouvert la voie à une nouvelle forme de criminalité : la cyber-criminalité. Le mot semble futuriste, comme une fiction lointaine qui nous concerne peu. Pourtant, à Namur comme ailleurs dans le pays, le nombre d'arnaques de ce type augmente. S'il est difficile d'intervenir après les faits, il reste un moyen efficace pour se protéger : la prudence.

Ils luttent contre le crime : la Computer Crime Unit

Au sein de la Police fédérale, la Computer Crime Unit, une équipe de cyber-spécialistes luttent contre la criminalité liée aux technologies informatiques, et notamment les escroqueries, la pédophilie ou les fraudes sur internet. Ils interviennent aussi à titre d'experts sur des enquêtes plus classiques où se mêlent internet et IRL*.

Cyber-criminels : comment font-ils ?

Plusieurs formes d'escroquerie sévissent sur internet. Parfois, la ficelle est grossière, et l'utilisateur attentif décèle l'arnaque. Parfois, le mode opératoire des criminels est plus sournois. Exemples :

- Vous recevez un mail d'une connaissance qui vous demande de lui transférer de l'argent parce qu'elle est dans une situation délicate à l'étranger.
- Des annonces sur des sites marchands entre particuliers vous proposent des biens à des prix trop attractifs pour être vrais : voiture, téléphone portable, appartement à louer. Le vendeur, joignable uniquement par mail, vous demande de lui envoyer une avance. Méfiance !
- Vous êtes spontanément contacté par téléphone par des personnes travaillant soi-disant chez un opérateur téléphonique ou internet, qui vous demande de procéder à diverses opérations sur votre ordinateur, et vous demande votre mot de passe.
- Votre ordinateur est bloqué sur une page affichant des logos officiels (Police, Sabam). Une fenêtre indique un blocage pour comportement illégal, et vous invite à procéder au paiement d'une amende pour récupérer votre accès à internet. C'est un cas typique de ransomware (logiciel – rançon).
- Dans le cadre d'une relation nouée sur un site de rencontre, le cybercriminel capture les images de vos échanges parfois très intimes, les diffuse sur internet et vous réclame de l'argent pour les retirer du net.

Dans tous les cas : ne faites rien de ce qui vous est demandé. Par contre, vous pouvez signaler ces tentatives d'attaque à la police.

Conseils de prudence

Toute sollicitation inhabituelle doit éveiller votre vigilance. Soyez critique et objectif, n'envoyez jamais d'argent et ne communiquez jamais de données personnelles, coordonnées bancaires, login ou mot de passe. De telles informations ne vous seront jamais légitimement demandées par téléphone, par mail ou par sms.

*** IRL : In Real Life (dans la vraie vie)**

Pour porter plainte

Vous avez été victime d'une arnaque ? Il est important de préparer votre dépôt de plainte en structurant un récit chronologique complet, afin d'expliquer clairement le problème rencontré. Munissez-vous de tout document utile (capture d'écran des profils sociaux, mails, preuve paiement) de façon à étoffer le dossier judiciaire. C'est toujours auprès de la Police locale qu'il vous faudra déposer plainte.

__Escroquerie__ : Faire usage de bons mots ou de propositions alléchantes, qui ne laissent pas indifférent, afin de soutirer des biens ou de l'argent à des personnes (utilisateurs d'Internet) naïves (au sens où elles ne se doutent de rien).
(Source : Police Fédérale)

Sites utiles

- **www.clicksafe.be** : portail de prévention de Childfocus pour un usage sûr et responsable d'internet par les enfants et les adolescents.
- **www.safeonweb.be** : site d'information et de prévention sur les questions de sécurité informatique, les menaces numériques et de sécurité sur internet.
- **Restez informé** : retrouvez conseils et infos utiles sur « Surfons tranquilles », l'émission de la RTBF, le mardi à 7h45, réalisée avec un commissaire de la FCCU.

Police Namur

__Infos__ : wwwpolnam.be