

# Charleroi Internet

**Si vous êtes victime de hacking, vous pouvez vous adresser à la Regional Computer Crime Unit**

**CHARLEROI** ESCROQUERIE SUR INTERNET

## Une employée victime de "phishing"

La boîte mail d'une travailleuse de la RCA a été bloquée et utilisée à des fins frauduleuses

Plusieurs fonctionnaires de la ville de Charleroi ont reçu un mail très étrange les invitant à verser 2.900€ pour secourir une victime, bloquée à l'étranger. L'arnaque est assez connue. Le problème, c'est que le courriel a été envoyé au départ de la boîte mail d'une employée de la régie communale autonome, véritablement victime, elle, de "phishing".

Imaginez que vous ne sachiez plus entrer dans votre boîte mail. Pire, que certains de vos contacts vous signalent que vous leur avez envoyé un mail assez étrange où vous leur réclamez de l'argent. Voilà la mésaventure qui est arrivée à une employée de la régie communale autonome. Pour expliquer comment ce type d'escroquerie peut survenir, Eric Absil, inspecteur principal à la Regional

Computer Crime Unit, pointe deux possibilités. "Soit le hacker craque le mot de passe s'il s'agit du nom de pépé, de mémé ou du toutou, soit - et c'est la technique la plus utilisée - le fraudeur demande à la victime en se substituant à Gmail ou Microsoft Hotmail, d'entrer ses coordonnées et son mot de passe."

Et voilà, le tour est joué: l'auteur de l'escroquerie envoie un mail bien rôdé aux contacts de la victime en usurpant son identité. Il lui reste alors à attendre que quelqu'un morde à l'hameçon pour lui soutirer un maximum d'argent.

Selon la RCCU, cette technique appelée "phishing" ou hameçonnage est de plus en plus courante et fait l'objet, sur ces six derniers mois, d'une dizaine de plaintes enregistrées. Les cas sont évidemment plus nombreux. "On estime que le chiffre noir est bien plus

élevé", précise Eric Absil. Pour les victimes, il n'existe pas des tonnes de solutions: "pour récupérer son compte, il faut suivre une procédure au niveau de Microsoft. De notre côté, on peut guider les gens mais nous n'avons pas la possibilité de débloquer leur compte."

La prudence doit donc être de mise. À éviter, on l'aura compris: communiquer son mot de passe ou sa phrase secrète, choisir un mot de passe qui comprend d'autres caractères que les alphanumériques. Autre mise en garde: "méfiez-vous dès qu'on vous demande d'envoyer de l'argent via Western Union."

En Afrique de l'Ouest et en Côte d'Ivoire, plus précisément, il semble que ce type d'arnaque soit élevé au rang de sport national. "Ils ont un bagou extraordinaire: ils vendraient des lunettes à un aveugle." «

L.F.



La victime envisage de déposer plainte. (photo prétexte)

■ VINCENT ROCHER

### Un Carolo victime du "broutage ivoirien"

Hier matin, la Regional Computer Crime Unit a été confrontée à un cas d'arnaque "à la webcam". Le modus operandi est le suivant: la future victime chatte via webcam avec une femme (généralement originaire de Côte d'Ivoire) et reçoit par la suite un courrier stipulant que la jeune femme est mineure et que le chateur est condamné à payer une certaine somme d'argent. Pour que le chantage soit efficace,

des extraits de la vidéo montrant la victime sont joints au courrier. Cette escroquerie est appelée le "broutage ivoirien".

#### > Infos utiles:

Si vous êtes personnellement confronté à une infraction liée à l'informatique, vous pouvez alors contacter les services de police de deux manières: si vous n'êtes pas victime mais vous souhaitez signaler une infraction sur Internet, vous pouvez le faire

sur [www.ecops.be](http://www.ecops.be).

Si vous êtes vous-même victime de fraude Internet ou une autre infraction sur Internet, vous pouvez vous adresser à votre service de police local, lequel pourra pour une enquête ultérieure demander l'appui de la RCCU ou de la FCCU. Si vous êtes victime de hacking ou de sabotage informatique, vous pouvez directement vous adresser à la RCCU de votre arrondissement.