Delémont, le 05 novembre 2020

Communiqué de presse

Chiffres mensuels de la criminalité

Annexe au tableau daté du 02.11.2020

Le sport des cybercriminels, la pêche aux mots de passe

Parmi les différentes ruses des cybercriminels, la pêche aux mots de passe est une technique qui est souvent mise en œuvre mais qui, grâce à des précautions accessibles, est souvent esquivée. Selon les milieux, ce phénomène s'appelle « phishing » ou « hameçonnage ». Trois phases pour ces vols d'informations personnelles et confidentielles : prendre contact – intercepter des données personnelles – s'enrichir en utilisant les données.

Les cybercriminels ont pour objectifs de s'enrichir. Evidemment, ils vont le faire sur le dos des victimes. Derrière leur ordinateur, ils envoient des courriels en se faisant passer pour des collaborateurs de prestataires de service ou d'institutions bancaires. Le courriel envoyé, qui utilise les logos des entreprises précitées, indique que les informations de leur compte ou les données d'accès ne sont plus à jour. La victime visée est invitée à cliquer sur un lien pour lui permettre de les actualiser. Si la proie clique sur le lien et donne son mot de passe ou ses données spécifiques, le criminel pourra les utiliser pour faire des virements ou des achats. Le pêcheur a lancé sa ligne - Il y avait au bout un leurre crédible au premier coup d'œil - Le poisson a été ferré…

Il n'est pas rare de recevoir un courriel qui n'a pas sa place dans la messagerie. Par quelques précautions à la portée de tous, ces courriels sont identifiés et traités comme il se doit (considérer comme indésirable). Donc, pour se protéger contre le phishing :

- Ne pas cliquer sur le lien (cela pourrait également télécharger un logiciel malveillant).
- Contrôler que l'adresse mail de l'expéditeur et l'URL du lien transmis sont corrects en positionnant la souris sur ceux-ci. Ce qui s'affiche doit être identique à ce qui est inscrit dans l'email.
- Signaler cet email à son fournisseur de messagerie et/ou au centre informatique de votre société.
- Activer la double authentification pour tous ses comptes mail personnel et professionnel (prendre contact avec le service informatique de votre entreprise).
- En cas de doute, contacter par un autre moyen le prétendu expéditeur pour s'assurer qu'il en est bien à l'origine.

Rien de tel qu'un peu d'exercice pour déjouer l'arnaque. Le site « eBanking – En toute sécurité » de la Haute Ecole Spécialisée de Lucerne offre des informations claires, en français, et un exercice d'apprentissage sur le phishing. En quelques clics, les points clés de la sécurité sont présentés simplement.

- Lien vers le site et les informations principales : https://www.ebas.ch/fr/le-phishing/
- Lien vers l'exercice d'apprentissage : https://www.ebas.ch/fr/test-sur-le-hameconnage/

La méthode pour annoncer les tentatives de phishing est décrite sur le site précité.

Relevons qu'actuellement, de telles escroqueries sont annoncées uniquement à quelques reprises à la police cantonale jurassienne.

En cas d'abus, les plaintes peuvent être déposées à la police dans les réceptions qui ont été adaptées aux mesures actuelles de protection contre la COVID-19. La police est et reste accessible par d'autres canaux. En composant le 117 en cas d'urgence, via le 032 / 420 65 65 pour une requête non urgente, par courrier électronique et postal selon les adresses présentes sur le site internet de la police.

La prévention Suisse de la Criminalité et la Haute Ecole Spécialisée de Lucerne collaborent sur cette thématique de prévention. D'autres informations par ce lien :
https://www.skppsc.ch/fr/sujets/internet/phishing/

Personne de contact :
Daniel Affolter, cellule Prévention et Communication à la police cantonale jurassienne, 032 / 420 65 65

Annexes : *Image prétexte « Phishing source Prévention Suisse de la Criminalité »*
Affiche « Phishing - Ne mordez pas à l'hameçon ! »