

**Attention à ce mail suspect.
Ne cliquez pas !**



**Attention
à ce mail
suspect.
Ne
cliquez
pas !**

Il s'agit en réalité d'un ransomware, un logiciel malveillant qui vise à prendre vos données et fichiers personnels en otage et les bloquer !

Après la fausse facture de Free, c'est cette fois la marque et le logo bpost qui ont été détournés par des hackers avec l'ambition d'essayer de *pomper* vos données personnelles et de les prendre en otage afin de réclamer, par après, une « rançon » contre la libération de celles-ci ! Pour ce faire, les pirates utilisent ce qu'on appelle un *ransomware*.

Pour tenter d'arriver à leurs fins, les hackers ont donc emprunté les traits de bpost afin de vous demander de cliquer sur un lien permettant, soi-disant, de retrouver trace d'un colis qui n'a pas encore été livré. Le piège est en marche. Le principe est donc simple et diabolique puisque les utilisateurs qui reçoivent ce fameux mail ont, en théorie, toute confiance en l'institution.

Sujet : Le colis n'a pas été livré.



Le colis n'a pas été livré.

Suivez votre envoi

Code: 2975268
Poids: 2.78 kg

Télécharger des informations

Dernières nouvelles

Collection de timbres-poste 2017

En 2017, bpost présentera une fois encore une nouvelle collection d'émissions limitées de timbres-poste. Les émissions phares cette année seront:

Organisation de bpost pour la fin d'année 2016

Samedi 24 et 31 décembre Points de vente: les bureaux de poste habituellement ouverts le samedi, sont ouverts. Les Points Poste appliqueront les heures d'.

Nouveaux tarifs 2017 pour les envois nationaux

Le 1er janvier 2017, bpost revêt à la hausse les tarifs conventionnels et préférentiels pour les envois nationaux.



Oups...

Nous n'avons pas trouvé d'envoi portant la référence ou le code-barres introduit.

Etes-vous certain que votre envoi est bien par bpost? Si oui, vérifiez si vous avez bien saisi correctement la référence ou le code-barres. Il est possible que votre envoi ne soit pas encore connu par nos systèmes. Nous vous conseillons de réessayer plus tard ou de contacter l'expéditeur.

Pour plus d'informations cliquez ici.

Quelle référence/quel code-barres puis-je utiliser ?

Pour chercher votre envoi, vous pouvez utiliser la référence ou le code-barres que bpost ou l'expéditeur vous a envoyé(e). Vous l'avez reçu par sms, par e-mail, par preuve de dépôt d'un bureau de poste ou par avis de passage que votre facteur a laissé dans votre boîte aux lettres. Assurez-vous également de spécifier le code à barres complet.

Copyright © 2015-2017 bpost | Service clients | Clause de non-responsabilité | Conditions générales

En effet, s'il est trop tard et que vous avez déjà appuyé sur le bouton de votre souris, le mal est fait. Le logiciel ainsi installé aura tout le loisir de prendre connaissance de vos données et fichiers personnels, voire même prendre le contrôle de votre poste de travail, bloquant au passage l'accès à vos précieuses infos via une clé de cryptage... permettant aux malotrus de réclamer une rançon contre la libération de vos données ou de votre ordinateur ! Inutile de préciser que dans bien des cas, la spirale infernale est enclenchée !

L'excellente série de Netflix *Black Mirror* avait d'ailleurs centré un de ses épisodes sur cette problématique, les protagonistes perdant au fil de celui-ci, le contrôle total sur les événements.

Que faire en cas d'infection ?

Si vous avez installé ledit logiciel, il faudra de toute façon passer, au minimum, par la case du scan antivirus. Sans plus attendre également, il est fortement conseillé de débrancher immédiatement tous les disques durs externes et autres qui pourraient être plus facilement sauvegardés, d'autant plus s'ils contiennent des sauvegardes de vos fichiers. Idem, pensez à déconnecter vos espaces de stockage virtuel (Dropbox, iCloud,...)

Dans certains cas, certains logiciels sont capables de combattre l'infection. Une petite recherche sur Google et différents forums s'impose donc.

Il est aussi très important de rappeler qu'il ne faut surtout pas rentrer dans « le jeu » et donc absolument éviter de payer la rançon demandée. Rien ne dit en effet que les pirates la joueront *fair play*... De plus, il est aussi très utile de prévenir les autorités compétentes...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européenne relative à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Vous avez reçu un mail suspect de bpost ? Ne cliquez pas ! (PHOTOS) – DH.be