24 mar 2020 -09:45

Phishing et coronavirus: internautes, attention aux arnaques!

La guerre contre les faux messages est loin d'être gagnée. À l'occasion du *European Cyber Security Awareness Month* en octobre 2019, le Centre pour la Cybersécurité Belgique (CCB) et la Cyber Security Coalition Belgium avaient déjà lancé un appel insistant à la vigilance face au phishing, en demandant notamment de transférer les messages suspects à suspect@safeonweb.be. Cet appel a porté ses fruits : l'année dernière, 1 700 000 e-mails suspects nous ont été transmis et nous avons fait bloquer 4000 faux sites Internet.

En raison de la forte augmentation de faux messages au sujet du coronavirus et de l'augmentation du nombre de faux messages envoyés par sms, nous tenons à replacer les projecteurs sur la campagne de sensibilisation nationale afin de relancer une vague de sensibilisation contre le phishing auprès de la population belge.

https://youtu.be/w6AbMNCyoTE

1. Attention aux messages de phishing sur le coronavirus

Le Centre pour la Cybersécurité Belgique met en garde contre une forte vague de faux messages sur le coronavirus contenant :

1. des offres concernant des masques de protection, des gels hydroalcooliques, des produits de désinfection...
2. des liens vers de faux sites d'information
3. de fausses collectes de fonds pour les victimes du virus

Soyez donc vigilants face aux messages concernant le coronavirus et ne cliquez pas sans réfléchir sur les liens figurant dans ces messages suspects.

- Si vous cliquez sur des liens suspects, vous risquez de télécharger des virus sans le savoir.
- Si vous communiquez vos données bancaires sur un faux site, votre compte pourrait être vidé.
- Les produits proposés sur de faux sites de vente ne seront pas livrés, les fausses collectes de fonds ne font rien d’autre que voler votre argent

> « Le coronavirus nous préoccupe tous aujourd'hui. Chaque jour, nous lisons de nouveaux articles sur le virus : comment nous protéger ? Combien y a-t-il d'infections en Belgique ? Quel est le degré de dangerosité du virus ? Nous en parlons avec nos amis, nous envoyons des sms, des messages WhatsApp et des mails contenant des questions, des réponses et d'autres informations sur le COVID-19. Les cybercriminels surfent sur l'actualité et sont bien au courant des thèmes qui nous intéressent. C'est pourquoi vous devez toujours être sur vos gardes lorsque vous recevez des messages suspects contenant des liens sur un sujet d'actualité. »

Miguel De Bruycker
Directeur du CCB

" « Transférez les messages suspects à suspect@safeonweb.be pour que nous puissions faire bloquer les liens suspects. C'est comme ça que nous veillerons à un environnement en ligne sûr, qui ne laisse pas l'ombre d'une chance aux escrocs. » "

Phédra Clouner
Directrice adjointe du CCB

2. Les cybercriminels propagent des virus et ransomware en les cachant derrière des messages et applications liés au COVID-19

Surveillez la carte interactive de la Johns Hopkins University

Le CCB met en garde contre un programme permettant de suivre l'évolution du virus sur une carte du monde. Des concepteurs de sites Internet mal intentionnés exploitent ce tableau recensant les infections et décès liés au coronavirus de la Johns Hopkins University pour installer des virus capables de détecter et de dérober des mots de passe. Vous avez l'impression de visualiser la véritable carte de la Johns Hopkins University, alors qu'en réalité des hackers y ont associé un virus.

L'application COVID-19 Tracker contient un ransomware

Il existe également une application Android qui vous permet de suivre les cas de COVID-19 : COVID19 Tracker. En réalité, l'application est infectée par un ransomware, baptisé CovidLock. CovidLock utilise des techniques pour refuser à la victime l'accès à son téléphone en forçant un changement de mot de passe pour déverrouiller le téléphone. Une fois ce stratagème mis en place, vous recevez un écran vous incitant à payer 100 $ en Bitcoins dans les 48 heures. Si vous ne le faites pas, toutes les données seront supprimées de votre téléphone et vous risquez de voir tous vos contacts, photos, vidéos et comptes de médias sociaux diffusés sur Internet.

Que faire ?

- Ces messages et applications ont été conçus de manière très professionnelle et semblent tout à fait réels. Il s'avère parfois difficile de remonter à la source.
- Restez dès lors toujours sur vos gardes lorsque vous recevez un message inattendu qui ne vous est pas adressé personnellement.
- Réfléchissez à deux fois avant de cliquer sur une pièce jointe à ce message. Les fichiers .exe peuvent être particulièrement dangereux.
- Réfléchissez à deux fois avant de cliquer sur un lien.
- N'installez que des applications proposées sur l'App Store de Google ou Apple.
- N'exécutez pas JavaScript lorsque vous y êtes invité après avoir téléchargé une pièce jointe.
- Un antivirus est un logiciel essentiel qui permet de protéger votre ordinateur et vos données contre les virus. Même si aucun logiciel antivirus ne peut garantir une protection à 100 %, il est indispensable d'en installer un.
- Faites parvenir les messages suspect à suspect@safeonweb.be.

« Tant que le coronavirus fera la une de l'actualité, les cybercriminels continueront à l'exploiter pour escroquer les gens. Réfléchissez à deux fois avant de cliquer sur un lien »

3. Attention également au smishing

Ces dernières semaines, nous observons une augmentation du nombre de tentatives de phishing par sms : ce phénomène a été baptisé « smishing ». Les sms semblent venir d'une banque ou d'une organisation officielle, mais c'est en réalité des cybercriminels qui en sont à l'origine. Grâce à des liens vers de faux sites internet, les cybercriminels gagnent un accès à vos données bancaires et ont ainsi tout le loisir de vider votre compte. Réfléchissez donc à deux fois avant de cliquer sur un lien figurant dans un sms.

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be