23 avr 2020 -13:17

À la recherche de masques buccaux ? Gare aux fausses boutiques en ligne

Le Centre pour la Cybersécurité Belgique vous met en garde : soyez prudent dans votre recherche en ligne de masques buccaux. Les fraudeurs créent de fausses boutiques en ligne.

Alors que la vie sociale s'apprête à reprendre son cours, nous nous préparons tous à sortir en toute sécurité. Les entreprises commandent des masques buccaux pour leurs collaborateurs, et les particuliers en recherchent eux aussi.

Souvent, l'internaute est encouragé par un message de phishing à surfer sur un faux site web ou une boutique en ligne pour acheter ces masques. Les citoyens peuvent transmettre ces messages suspects à suspect@safeonweb.be. Nous ferons alors bloquer les liens vers ces sites suspects.

> "En mars, nous avons reçu en moyenne plus de 8600 e-mails suspects par jour et avons pu faire bloquer 4500 URL's uniques.Au mois d'avril, nous avons reçu jusqu'à présent en moyenne plus de 1000 courriers suspects par jour. Le phénomène est en augmentation mais heureusement, les internautes ont de plus en plus le réflexe d'envoyer ces messages à suspect@safeonweb.be"
>
> Phédra Clouner
> Directrice adjointe du CCB

Au cours des dernières semaines, 1165 nouveaux noms de domaine .be ont été enregistrés, faisant référence au COVID-19 et plus spécifiquement aux masques buccaux. Des criminels voulant s'en servir pour lancer de faux sites Internet et boutiques en ligne se cachent probablement derrière une partie de ces enregistrements de noms de domaine.

Cependant, DNS Belgique - qui gère tous les noms de domaine .be, .brussels et .vlaanderen - garde un œil sur la situation.

"L'une de nos principales préoccupations est de faire en sorte que ces zones .be soient sûres, afin que l'internaute se sente en sécurité lorsqu'il surfe sur un site web portant les extensions .be, .brussels ou .vlaanderen. Pour ce faire, des contrôles quotidiens sont effectués lors de l'enregistrement de nouveaux noms de domaine avec ces extensions. Toute personne qui tenterait de s'enregistrer avec de fausses données se heurterait alors à un mur. Même si notre priorité est de mettre l'accent sur la cybersécurité, il en va de soi que l'internaute doit rester vigilant."

Philip Du Bois
DNS Belgium

Comment ce protéger ? 3 tips

1. Gardez toujours votre esprit critique avant de procéder à un achat. Le produit est plus avantageux que sur les autres boutiques en ligne ou son prix est anormalement bas ? Si une offre est trop belle pour être vraie, c'est généralement qu'elle n'est pas vraie. Il y a un risque que les produits commandés ne vous parviennent jamais ou qu'il s'agisse de contrefaçons.

2. Faites de préférence uniquement vos achats sur les boutiques en ligne que vous connaissez déjà et qui sont fiables. Une boutique en ligne a l'obligation d'indiquer clairement ses nom, adresse et numéro d'entreprise. Si ces données ne figurent pas sur le site de la boutique en ligne, ne l'utilisez pas.

3. Vous avez reçu une promotion par e-mail ou sms ? Ne cliquez jamais sur le lien figurant dans le message. Le risque est grand qu'il vous amène sur un faux site Internet ou une fausse boutique en ligne. Transferrez le message à suspect@safeonweb.be.

Lisez plus:

- Pour plus d'info concernant DNS Belgium : Lut Goedhuys: 0477 67 66 97
- Pour plus d'info concernant le CCB: Responsables communication ci-dessous

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