13 août 2020 -16:35

Un tsunami de smishing en vue

Nous avons appris de source sûre que des cybercriminels prévoient de lancer plusieurs attaques sous forme de smishing dans les prochains jours voire semaines.

Les SMS sont un canal toujours plus utilisé pour envoyer des messages qui contiennent des liens frauduleux, dans l'idée d'escroquer des gens. Cette forme de phishing a été baptisée « smishing » ou « phishing par sms ». Ces dernières semaines, le smishing est en recrudescence et d'autres attaques sous forme de smishing sont à prévoir dans les prochaines semaines.

Les cybercriminels exploitent l'actualité pour titiller votre curiosité et vous faire cliquer sur des liens. En ayant recours au smishing, des escrocs font miroiter des choses liées à la crise du coronavirus. Les messages provenant soi-disant des autorités, d'une banque ou d'un service de livraison continuent eux aussi à tourner. Ne tombez pas dans le panneau et faites toujours preuve d'esprit critique.

Que faire?

- Ne cliquez pas sur le lien dans un SMS.
- Si vous avez bel et bien cliqué sur ce lien, ne remplissez pas les champs apparaissant à l'écran et coupez toute interaction avec le site.
- Vous pouvez transmettre les messages frauduleux, y compris les SMS, à suspect@safeonweb.be. Pour ce faire, il vous suffit de sélectionner le texte du SMS et de le copier dans un e-mail, puis de l'envoyer à suspect@safeonweb.be. Le contenu de votre signalement sera ensuite traité de manière automatique. Vous pouvez également nous faire parvenir des captures d'écran à l'adresse info@safeonweb.be

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

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

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

© 2020 - news.belgium.be