11 oct 2022 -09:43

Campagne Safeonweb 2022 « OK n'est pas toujours OK »

Cette année, le Centre pour la Cybersecurité Belgique et la Cybersecurity Coalition ont de nouveau mobilisé toutes leurs forces pour lutter, avec plus de 500 autres partenaires, contre la criminalité informatique sous le slogan : « *OK n'est pas toujours OK !* ». Pendant la campagne, nous souhaitons attirer l'attention sur une thématique particulière par le biais de spots radio, de vidéos sur les médias sociaux, de bannières et d'autres matériels de campagne. L'objectif cette année est de sensibiliser au moins la moitié de la population belge à la sécurisation des appareils mobiles.

"Celui qui a accès à votre smartphone a accès à votre vie. C'est pourquoi il est si important de sécuriser correctement votre appareil."

Miguel De Bruycker
Directeur Centre pour la Cybersécurité Belgique

"Plus de 95 %des ménages belges disposent d'un appareil mobile, dont la sécurisation est trop souvent négligée. Une diffusion de notre message via les stations radios et les chaines télévision couvrant le territoire sera assurée, pour que nous puissions acquérir les bons réflexes également en ce qui concerne nos appareils mobiles."

Phédra Clouner
Directrice adjointe du CCB

Apprenez à sécuriser correctement votre smartphone

Avoir un smartphone en poche est aujourd'hui la chose la plus commune qui soit, tant chez les plus jeunes que les aînés. Le nombre d'applications ainsi que les usages que nous en faisons au quotidien se multiplient: p.ex. pour rester en contact avec nos connaissances, faire des achats, regarder des films, se divertir ou faire les devoirs.

- 93 % des Flamands (16+) possèdent un smartphone et 59 % disposent également d'une tablette (IMEC, *Digimeter 2021*, p. 24 et suivantes).
- 96 % des ménages wallons disposent d'au moins un appareil mobile. C'est 4 % de plus qu'en 2019. (*Baromètre 2021 de maturité numérique des citoyens wallons*, pp. 4-6)

Les logiciels malveillants mobiles sont en augmentation

C'est sur ce terrain qu'opèrent les criminels et les fraudeurs: ils développent des virus spécialement conçus pour cibler les appareils mobiles et passent à l'attaque.

En 2021, nous avons assisté à une cyberattaque des plus inquiétantes: la propagation du virus FLUBOT qui visait indistinctement tous les internautes. Ce virus a infecté plus de 11 000 smartphones en un temps record par le biais du téléchargement d'une application par des utilisateurs inattentifs. Le virus a pu ainsi se propager ensuite de manière inaperçue à tous les contacts des victimes. Un appareil infecté a parfois envoyé plus de 10 000 messages. Entre le 6 et le 13 septembre 2021, une moyenne de 2 millions de messages par jour a été détectée et bloquée par les opérateurs (Chiffres de l'IBPT, 2021).

OK n'est pas toujours OK !

Il est nécessaire de bien protéger son smartphone pour bloquer les cybercriminels ou autres intrusions, si vous ne voulez pas qu'une personne mal intentionnée ait accès à votre appareil, car les dégâts peuvent être considérables.

La principale source d'infection des appareils est le téléchargement d'applications douteuses. Soyez donc prudents lorsque vous recevez un e-mail ou un SMS vous invitant à télécharger une application. En passant par une boutique d'applications (*store d'applis*) non sécurisée, vous augmentez les risques d'installer une application dangereuse, voire un virus.

Vous pouvez également sécuriser votre smartphone en suivant ces conseils :

- Restez toujours très prudent lorsque vous recevez un e-mail ou un SMS vous demandant de télécharger une application. SI vous téléchargez une application par le biais d'un *store d'applis* peu sécurisé, il est probable que cette application soit dangereuse, voire que ce soit un virus.
- Votre smartphone vous signale que l'application que vous essayez d'installer n'est pas fiable ? Arrêter immédiatement l'installation de l'application.
- L'installation d'une application nécessite souvent l'accès à d'autres données : par exemple, à vos photos, vos contacts ou votre localisation. Autorisez cet accès uniquement si ces données sont nécessaires et utiles pour l'utilisation de l'application.
- On vous demande d'effectuer des mises à jour ? Ne tardez pas à le faire.

"Je suis très fier des résultats que nous avons obtenus en étroite collaboration avec le CCB.Il reste encore beaucoup de travail à faire, mais en unissant nos forces, je suis convaincu que nous pouvons et allons continuer à sensibiliser le grand public et les entreprises aux menaces de cybersécurité dans le monde contemporain."

Jan De Blauwe
Président de la Cyber Security Coalition

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Michele Rignanese
Porte-parole FR
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Porte-parole NL
+32 485 76 53 36
katrien.eggers@cert.be