Informations générales

Campagne Safeonweb, octobre 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 les criminels sous le slogan : « *OK n'est pas toujours OK !* ». Pendant la campagne, nous souhaitons attirer l'attention sur le thème par le biais de spots radio, de vidéos sur les médias sociaux, de bannières et d'autres matériels de campagne.

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.

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.

Il n'est pas tellement difficile de sécuriser votre smartphone. 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'apps*) non sécurisée, vous augmentez les risques d'installer une application dangereuse, voire un virus.

Le slogan de la campagne de cette année est donc : OK n'est pas toujours OK ! Après tout, cliquer sur OK pour télécharger une application peut avoir des conséquences très désagréables.

Résumé

- Les smartphones ne cessent de conquérir les consommateurs, et presque tous les citoyens de plus de 16 ans en possèdent un.
- L'utilisation des smartphones est de plus en plus intensive : on les utilise de plus en plus jeune, de plus en plus longtemps et pour des applications de plus en plus diverses.
- Les criminels et les escrocs y voient une belle opportunité.
- Le nombre de virus spécialement développés pour les smartphones augmente
- Les utilisateurs ne sont pas conscients de ce problème.
- La prévention est possible et simple **: ne télécharger que des applications provenant d'appstores officiels**
- 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 appstore 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.

1. Augmentation de l'utilisation des appareils mobiles (smartphones et tablettes)

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, p. 4-6)

Non seulement presque tout le monde en possède un, mais l'utilise en plus très souvent pour des applications diverses.

Les utilisateurs ne peuvent plus s'en passer, mais s'inquiètent tout de même de la sécurité de certaines actions qu'ils effectuent avec leur smartphone. *(IMEC, Digimeter 2021, p. 114 + 124)*

Les enfants reçoivent leur premier smartphone de plus en plus tôt. Selon le rapport d'Apestaartjaren (2022), il semblerait que ce soit dès l'âge de 8 ans. A partir de 13 ans, chaque jeune semble être l'heureux propriétaire d'un smartphone. (https://www.apestaartjaren.be/, 2022, p. 9)

2. Augmentation des malwares mobiles

Nous nous fions de plus en plus aux appareils mobiles, et les cybercriminels y voient l'occasion parfaite de mettre la main sur nos informations et notre argent, ou tout simplement de faire des dégâts. Dans cette perspective, ils développent un certain nombre de menaces spécialement conçues pour agir sur des plateformes mobiles : **les malwares mobiles.**

https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/mobile-malware

Les **malwares mobiles** (ou virus pour appareils mobiles) sont des logiciels malveillants conçus spécifiquement pour les appareils mobiles, tels que les smartphones et les tablettes, dans le but d'accéder à des données privées. (ENISA Threat Landscape 2021 (p. 47)

3. Cas actuel : Virus FluBot

La propagation du virus FLUBOT, qui a touché les internautes ordinaires, est sans aucun doute la cyberattaque qui a le plus inquiété le CCB en 2021 Des milliers de smartphones ont été infectés par ce virus en un rien de temps car les utilisateurs ont malencontreusement téléchargé une application. Le virus a ainsi pu se propager de manière invisible 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)

L'infrastructure de FluBot a été démantelée en 2022 par une action policière de grande envergure. Flubot a peut-être disparu, mais des dizaines d'autres virus sont prêts à lancer une attaque.

https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

4. Comment éviter de télécharger un malware mobile ? Installez uniquement des applications provenant des stores d'applis officiels/reconnus

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.

Sécurisez votre smartphone en 5 étapes

Etape 1 : Téléchargez uniquement des applications dans des appstores officiels

Les appstore officiels sont l'App Store si vous utilisez un iPhone et le Google Play Store si vous utilisez une autre marque d'appareil. Avant de télécharger une application, vérifiez donc toujours d'où elle provient.

N'installez alors que des applications provenant d'une source officielle (Google Play, App Store) ou d'un fournisseur officiel (par exemple LG, Samsung, SONY, Amazon, etc.). N'installez jamais une application provenant d'une source inconnue.

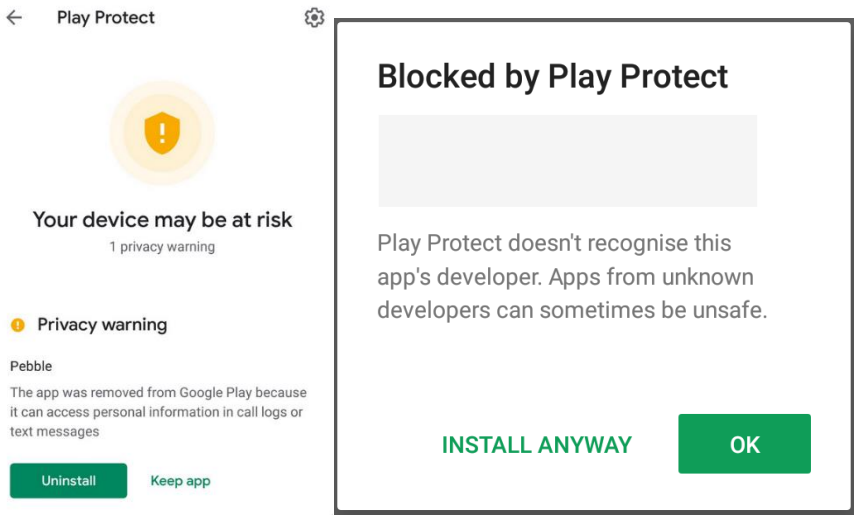
Google et Apple mettent tout en œuvre pour s'assurer que les applications qu'ils proposent ne contiennent pas de malwares. Même si quelqu'un parvient à proposer une application malveillante dans l'une de ces boutiques, Google ou Apple la détectera rapidement et agira en conséquence. Les autres fournisseurs n'offrent pas les mêmes garanties de sécurité.

Etape 2 : Détectez les messages suspects

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 appstore peu sécurisé, il est probable que cette application soit dangereuse, voire que ce soit un virus.

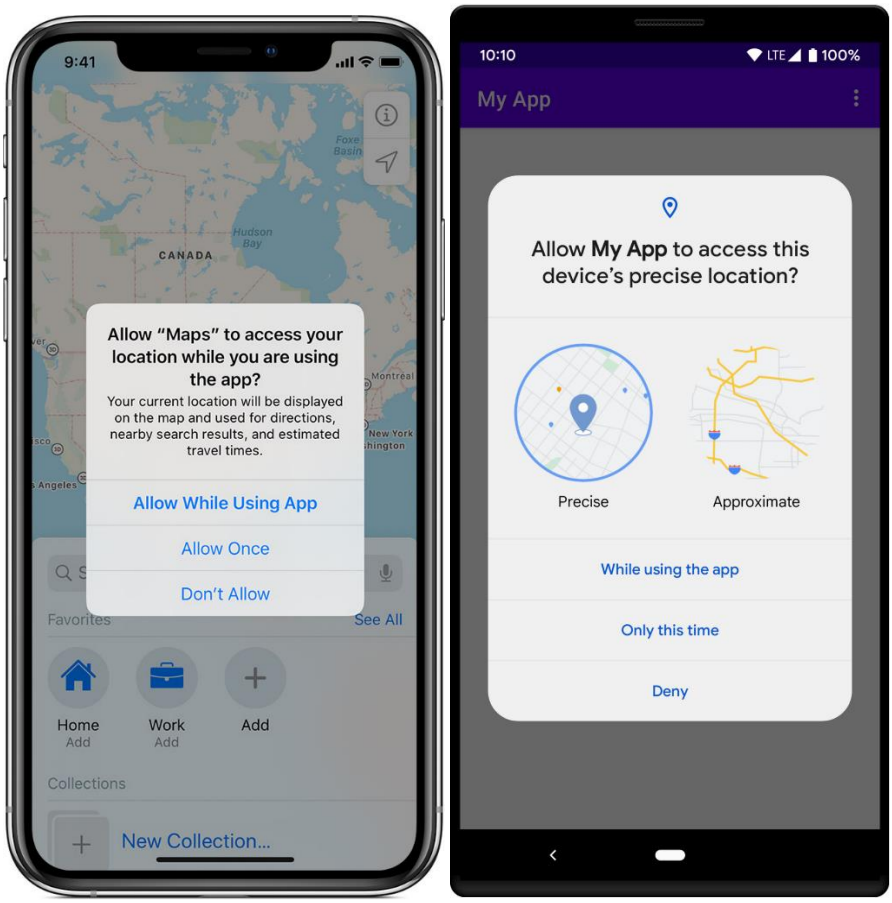
Etape 3 : N'ignorez pas les alertes de sécurité

Votre smartphone vous signale que l'application que vous essayez d'installer n'est pas fiable ? Arrêter immédiatement l'installation de l'application.



Etape 4 : N'autorisez qu'un accès minimal aux applications

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. Une application « calculatrice » n'a pas vraiment besoin d'accéder à vos contacts, vos photos ou votre localisation.



Etape 5 : Assurez-vous que votre smartphone et vos applications sont toujours à jour

On vous demande d'effectuer des mises à jour ? Faites-le dès que possible. Éteignez régulièrement votre smartphone. Lors du redémarrage, certaines mises à jour sont automatiques. Chaque programme et chaque application a des vulnérabilités, également appelées bugs ou erreurs logicielles, qui permettent aux cybercriminels de nuire à vos appareils ou d'en prendre le contrôle. Ces vulnérabilités sont heureusement détectées et réparées. C'est notamment à cela que servent les mises à jour.

Comment protéger encore plus efficacement votre smartphone ? Découvrez d'autres astuces sur :

https://www.safeonweb.be/fr/securisez-vos-appareils-mobiles