Achtergrondinformatie

Safeonweb campagne, oktober 2022

OK is niet altijd OK

Het Centrum voor Cybersecurity België en de Cybersecurity Coalition slaan dit jaar de handen opnieuw in elkaar en gaan samen met meer dan 500 partners de strijd aan tegen deze oplichters met de slogan: OK is niet altijd OK! Tijdens de campagne schreeuwen we het van de daken via radiospotjes, filmpjes op social media, banners en andere campagnematerialen.

Iedereen, van zeer jong tot oud, heeft tegenwoordig een smartphone op zak. We gebruiken hem voor steeds meer toepassingen: om met vrienden in contact te blijven, om aankopen te doen, om films te bekijken, om te gamen of om huiswerk te maken.

Criminelen en oplichters zien hierin een grote opportuniteit. Ze ontwikkelen virussen die speciaal ontwikkeld zijn om mobile toestellen te treffen en gaan in volle aanval.

De cyberaanval die ons in 2021 de meeste zorgen baarde en die gewone internetgebruikers trof, was ongetwijfeld de verspreiding van het FLUBOT-virus. Meer dan 11000 smartphones werden in een mum van tijd besmet met dit virus omdat gebruikers achteloos een applicatie downloadden. Zo kon het virus zich ongemerkt verspreiden naar alle contacten van de slachtoffers.

Het is niet zo moeilijk om je smartphone veilig te houden. De belangrijkste manier waarop toestellen besmet raken is door het downloaden van onbetrouwbare apps. Wees daarom voorzichtig als je een e-mail of een sms'je ontvangt waarin gevraagd wordt om een app te downloaden. De kans is groot dat je via een onveilige app winkel een gevaarlijke app of zelfs een virus installeert.

De slogan van de campagne van dit jaar is daarom: **OK is niet altijd OK!** Op OK klikken om een app te downloaden, kan immers heel vervelende gevolgen hebben.

CENTRE FOR CYBER SECURITY BELGIUM
CYBER SECURITY COALITION
Safeonweb.be
.be

Samenvatting

- Steeds mensen gebruiken een smartphone, bijna de volledige bevolking vanaf 16 jaar
- Steeds intensiever gebruik van smartphones: voor meer verschillende toepassingen, langere duur en vanaf steeds jongere leeftijd
- Criminelen en oplichters zien hierin een grote opportuniteit
- Het aantal virussen dat speciaal ontwikkeld wordt om smartphones te treffen, neemt toe
- De gebruiker is zich niet bewust van het probleem
- Preventie is mogelijk en eenvoudig: **download enkel apps uit officiële appstores**
- Je kan je smartphone ook veilig houden door de volgende tips te volgen:
    - Wees altijd heel voorzichtig als je een e-mail of een sms'je ontvangt waarin gevraagd wordt om een app te downloaden. De kans is groot dat je via een minder veilige app winkel een gevaarlijke app of zelfs een virus installeert.
    - Krijg je een waarschuwing dat je een onbetrouwbare app wil installeren? Stop onmiddellijk met het installeren van de app.
    - Als je een app installeert wordt er vaak toegang gevraagd tot andere gegevens: bv. je foto's, je contacten of je locatie. Geef enkel toestemming als dat nodig en nuttig is voor het gebruik van de app.
    - Krijg je de vraag om updates uit te voeren? Doe het zo snel mogelijk.

1. Stijgend gebruik van mobile devices (smartphones en tablets)

93% van de Vlamingen (16+) heeft een smartphone op zak en 59% heeft ook een tablet ter beschikking (IMEC, Digimeter 2021, p.24 ev.).

96% van de Waalse gezinnen heet minstens één mobiel toestel ter beschikking. Dat is 4% meer dan in 2019. (BAROMÈTRE 2021 de maturité numérique des citoyens wallons, p.4-6)

Niet alleen heeft bijna iedereen een smartphone te beschikking, het toestel wordt bovendien zeer frequent gebruikt voor verschillende toepassingen.

Gebruikers kunnen niet meer zonder, maar maken zich wel zorgen over de veiligheid van bepaalde acties die ze met hun smartphone verrichten. *(IMEC, Digimeter 2021, p.114 + 124)*

Kinderen krijgen hun eerste smartphone op steeds jongere leeftijd. Volgens het onderzoeksrapport van Apestaartjaren (2022) blijkt dat al op 8-jarige leeftijd te zijn. Vanaf de leeftijd van 13 jaar blijkt elke jongere de trotse bezitter te zijn van een smartphone. (https://www.apestaartjaren.be/, 2022, p.9)

2. Toename van mobiele malware

Omdat we steeds meer op mobiele apparaten vertrouwen, zien cybercriminelen deze als een uitgelezen kans om onze informatie en ons geld in handen te krijgen, of om gewoon kwaad te doen. Met dit in gedachten ontwikkelen ze een aantal bedreigingen die speciaal zijn ontworpen om op mobiele platforms te werken, nl. **mobile malware.**

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

Mobile malware (of virussen voor mobiele apparaten) is kwaadaardige software die speciaal is ontworpen voor mobiele apparaten, zoals smartphones en tablets, met als doel toegang te krijgen tot privégegevens. (ENISA Threat Landscape 2021 (p. 47)

3. Actuele case: FluBot-virus

De cyberaanval die het CCB in 2021 zorgen baarde en die gewone internetgebruikers trof, was ongetwijfeld de verspreiding van het FLUBOT-virus. 11000 smartphones werden in een mum van tijd besmet met dit virus omdat gebruikers achteloos een applicatie downloadden. Zo kon het virus zich ongemerkt verspreiden naar alle contacten van de slachtoffers. Een geïnfecteerd toestel stuurde soms meer dan 10 000 berichten uit. Tussen 6 en 13 september 2021 werden gemiddeld 2 miljoen berichten per dag gedetecteerd en geblokkeerd door de operatoren. (Cijfers BIPT, 2021)

De infrastructuur van FluBot werd in 2022 ontmanteld door een grootschalige politie-actie. Flubot is misschien van de radar verdwenen maar er staan tientallen andere virussen klaar om een aanval in te zetten.

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

4. Hoe mobile malware voorkomen? Installeer enkel apps van een officiële/erkende app winkel

Een goede beveiliging van je smartphone is nodig om cybercriminelen of andere indringers buiten te houden. Je wil immers niet dat iemand met slechte bedoelingen toegang krijgt tot je toestel want die kan heel wat schade berokkenen.

Beveilig je smartphone in 5 stappen

Stap 1: Download enkel apps uit officiële app winkels

De officiële app winkels zijn de App Store als je een iPhone gebruikt en de Google Play Store als je een ander merk toestel gebruikt. Voordat je een app downloadt, is het dus belangrijk dat je goed kijkt wie deze app aanbiedt.

Installeer dus alleen applicaties uit een officiële app store (Google Play, App Store) of van een officiële verkoper (bv. LG, Samsung, SONY, Amazon, enz.). Installeer nooit een app van een bron die je niet kent.

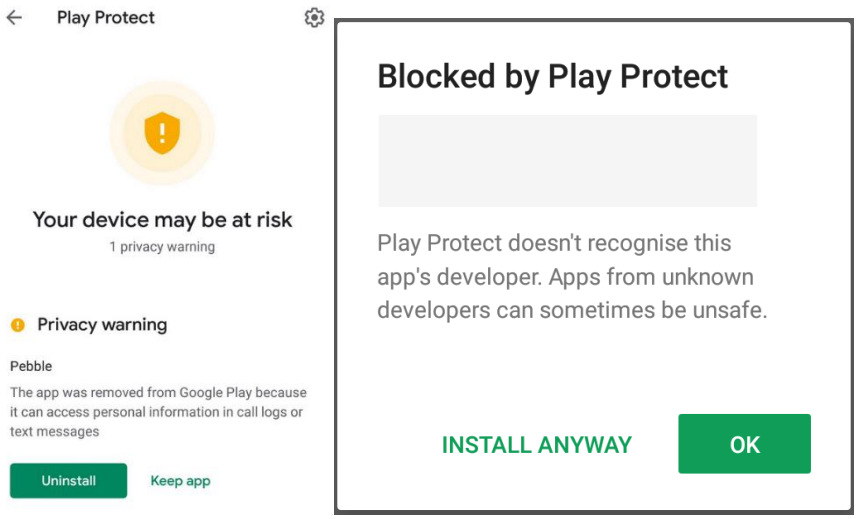
Google en Apple doen veel moeite om ervoor te zorgen dat de apps die zij aanbieden geen malware bevatten. Zelfs als iemand erin slaagt een kwaadaardige applicatie in een van deze winkels aan te bieden, zullen Google of Apple dit snel ontdekken en hun fout herstellen. Het probleem met andere aanbieders is dat ze niet dezelfde veiligheidsgarantie bieden.

Stap 2: Kijk uit voor verdachte berichten

Wees altijd heel voorzichtig als je een e-mail of een sms'je ontvangt waarin gevraagd wordt om een app te downloaden. De kans is groot dat je via een minder veilige app winkel een gevaarlijke app of zelfs een virus installeert.

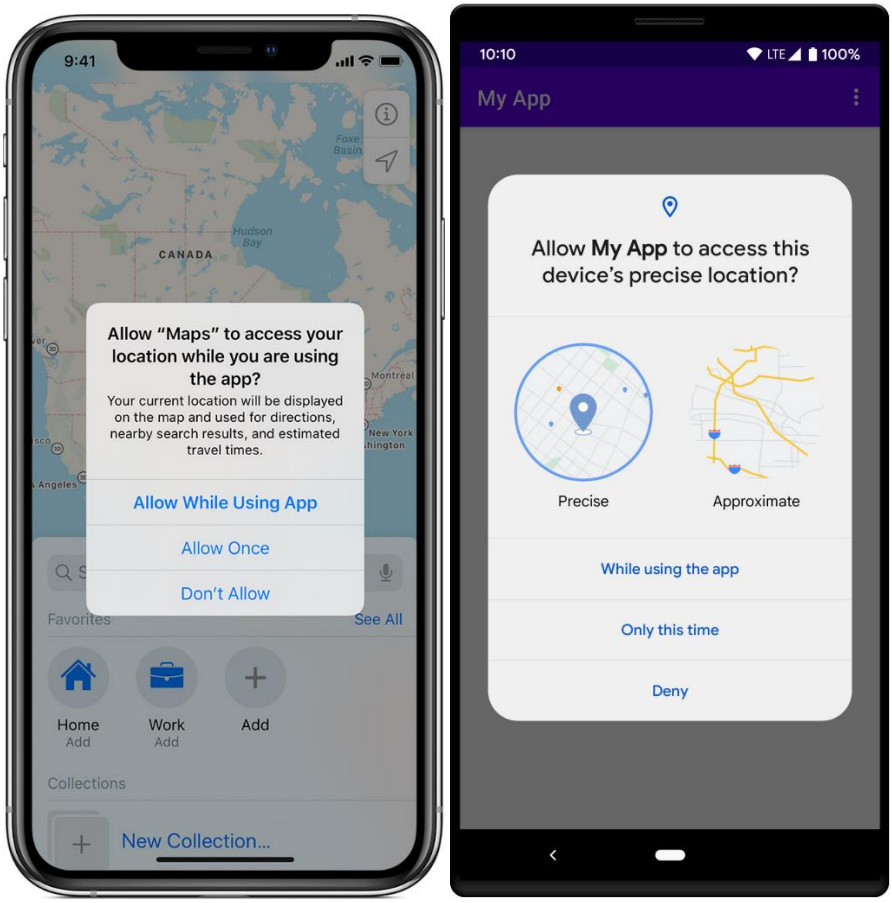
Stap 3: Negeer veiligheidswaarschuwingen niet

Krijg je een waarschuwing dat je een onbetrouwbare app wil installeren? Stop onmiddellijk met het installeren van de app.



Stap 4: Geef alleen minimale toegang aan apps

Als je een app installeert wordt er vaak toegang gevraagd tot andere gegevens: bv. je foto's, je contacten of je locatie. Geef enkel toestemming als dat nodig en nuttig is voor het gebruik van de app. Een rekenmachine-app heeft echt geen toegang nodig tot je contacten, foto's of locatie.



Stap 5: Zorg dat je smartphone en apps steeds up-to-date zijn

Krijg je de vraag om updates uit te voeren? Doe het zo snel mogelijk. Zet je smartphone regelmatig eens uit. Bij het opnieuw opstarten gebeuren sommige updates automatisch. Elk programma en elke app bevat zogenaamde kwetsbaarheden, ook bekend als software bugs of errors, die het mogelijk maken voor cybercriminelen om schade te berokkenen of de controle over je toestellen te nemen. Deze kwetsbaarheden worden gelukkig ontdekt en hersteld. Dit is precies wat er gebeurt als je een update uitvoert.

Hoe kan je je smartphone nog beter beschermen? Nog meer tips op:

https://www.safeonweb.be/nl/beveilig-mobiele-toestellen