Persbericht 20 maart 2020, Brussel

"Phishingberichten rond het coronavirus misleiden de internetgebruiker"

De strijd tegen valse berichten is nog niet gestreden. Tijdens de *European Cyber Security Awareness Month*, in oktober 2019, deden het Centrum voor Cybersecurity België (CCB) en de Cyber Security Coalition Belgium al een luide oproep om aandachtig te zijn voor phishing en verdachte berichten door te sturen naar verdacht@safeonweb.be. Met resultaat, want vorig jaar ontvingen we 1.700.000 verdachte mails en werden er 4.000 valse websites geblokkeerd.

Omwille van de **sterke stijging van valse berichten rond het coronavirus** en de **toename van het aantal valse berichten per sms**, herhalen we de nationale sensibiliseringscampagne om de Belgische bevolking opnieuw te sensibiliseren voor phishing.

1. Opgepast voor phishing rond het coronavirus

Het Centrum voor Cybersecurity België waarschuwt voor een sterke stijging van valse berichten over het coronavirus:

1. met aanbiedingen voor mondkapjes, alcoholgels, desinfecterende middelen,…
2. met links naar valse nieuwssites
3. met valse geldinzamelacties voor slachtoffers van het virus

Wees daarom waakzaam voor berichten over het coronavirus en klik niet zomaar op links in verdachte berichten.

- Door te klikken op verdachte links kan je zonder het te weten virussen downloaden
- Wanneer je je bankkaartgegevens invult op een valse website wordt je rekening geplunderd
- Producten van valse verkoopssites worden niet geleverd, valse geldinzamelacties stelen je geld

"Het coronavirus houdt ons vandaag allemaal in de ban. Elke dag lezen we nieuwe berichten over het virus: hoe moeten we ons beschermen? Hoeveel besmettingen zijn er in België? Hoe gevaarlijk is het virus? We spreken erover met onze vrienden, we sms'en, whatsappen en mailen met vragen, antwoorden en andere informatie over COVID-19. ***Cybercriminelen spelen in op de actualiteit en weten welke thema's ons interesseren.*** *Wees daarom steeds op je hoede wanneer je verdachte berichten krijgt met links over een actueel onderwerp."*

- Miguel De Bruycker, Directeur CCB

"Stuur verdachte berichten door naar verdacht@safeonweb.be zodat wij verdachte links kunnen laten blokkeren. Zo zorgen we voor een veilige internetomgeving waar oplichters geen kans krijgen."

- Phédra Clouner, Adjunct-directeur CCB

2. Cybercriminelen verspreiden virussen en ransomware verborgen achter COVID-19 berichten en applicaties

Kijk uit voor interactieve kaart Johns Hopkins University

Het CCB waarschuwt voor een programma waarmee je de evolutie van het virus op een wereldkaart kan volgen. Een dashboard van coronavirusinfecties en -doden van de Johns Hopkins University, wordt door kwaadaardige websites misbruikt om virussen te installeren die wachtwoorden kunnen detecteren en stelen. Het lijkt dus alsof je de echte kaart van de Johns Hopkins University ontvangt, maar eigenlijk is er een virus aan toegevoegd door hackers. De installatie ervan gebeurt enkel als JavaScript is ingesteld.

COVID-19 Tracker App bevat ransomware

Dan is er ook een Android App waarmee je gevallen van COVID-19 kan opvolgen: COVID19 Tracker App. In werkelijkheid is de app geïnfecteerd met ransomware, die de naam CovidLock kreeg. CovidLock gebruikt technieken om het slachtoffer de toegang tot zijn of haar telefoon te ontzeggen door een wijziging van het wachtwoord om de telefoon te ontgrendelen, te forceren. Hierna krijg je meteen een scherm te zien waarop uitgelegd wordt hoe je binnen de 48 uur $100 aan Bitcoin moet betalen. Wanneer je dat niet doet, wordt alle data van je toestel verwijderd en dreigt men om al je contacten, foto's, video's en alle sociale media accounts publiek te lekken op het internet.

Wat moet je doen?

- Deze berichten en applicaties zijn zeer professioneel gemaakt en lijken dan ook echt. Het is soms moeilijk om de bron te achterhalen.
- Wees daarom altijd op je hoede als je een onverwacht bericht krijgt dat niet persoonlijk aan jou gericht is.
- Denk 2 keer na voor je een bijlage in een bericht aanklikt. Vooral .exe bestanden kunnen zeer gevaarlijk zijn.
- Denk ook altijd 2 keer na voor je op een link klikt.
- Installeer enkel App's uit de officiële App Store van Google of Apple.
- Voer geen JavaScript uit als daarnaar gevraagd wordt na het downloaden van een bijlage.
- Een virusscanner zorgt ervoor dat je computer niet vatbaar is voor virussen. Het is het belangrijkste stukje software om je computer en je gegevens te beschermen. En ook al biedt geen enkele virusscanner 100% bescherming, toch blijft het cruciaal om er eentje te installeren.
- Stuur verdachte berichten door naar verdacht@safeonweb.be

"Zolang het coronavirus voorpaginanieuws blijft, zullen criminelen het blijven gebruiken om mensen te misleiden. Vertrouw berichten niet zomaar en denk tweemaal na voor je op een link klikt"

3. Wees ook waakzaam voor smishing

De jongste weken zien we een toename van het aantal phishingberichten per sms: smishing. De sms'sen lijken van een bank of officiële organisatie te komen, maar worden eigenlijk verstuurd door cybercriminelen. Via links naar valse websites komen cybercriminelen zo aan je bankgegevens, en plunderen ze je rekening. Denk daarom twee keer na vooraleer je op een link in een sms klikt.

#####

Over het Centrum voor Cybersecurity België:
Het Centrum voor Cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in België. Het CCB stelt tot doel het superviseren, het coördineren en het waken over de toepassing van de Belgische strategie betreffende cyberveiligheid. Door het optimaliseren van de informatie-uitwisseling zullen de bevolking, de bedrijven de overheid en de vitale sectoren zich gepast kunnen beschermen.
www.ccb.belgium.be

Perscontact Centrum voor Cybersecurity België

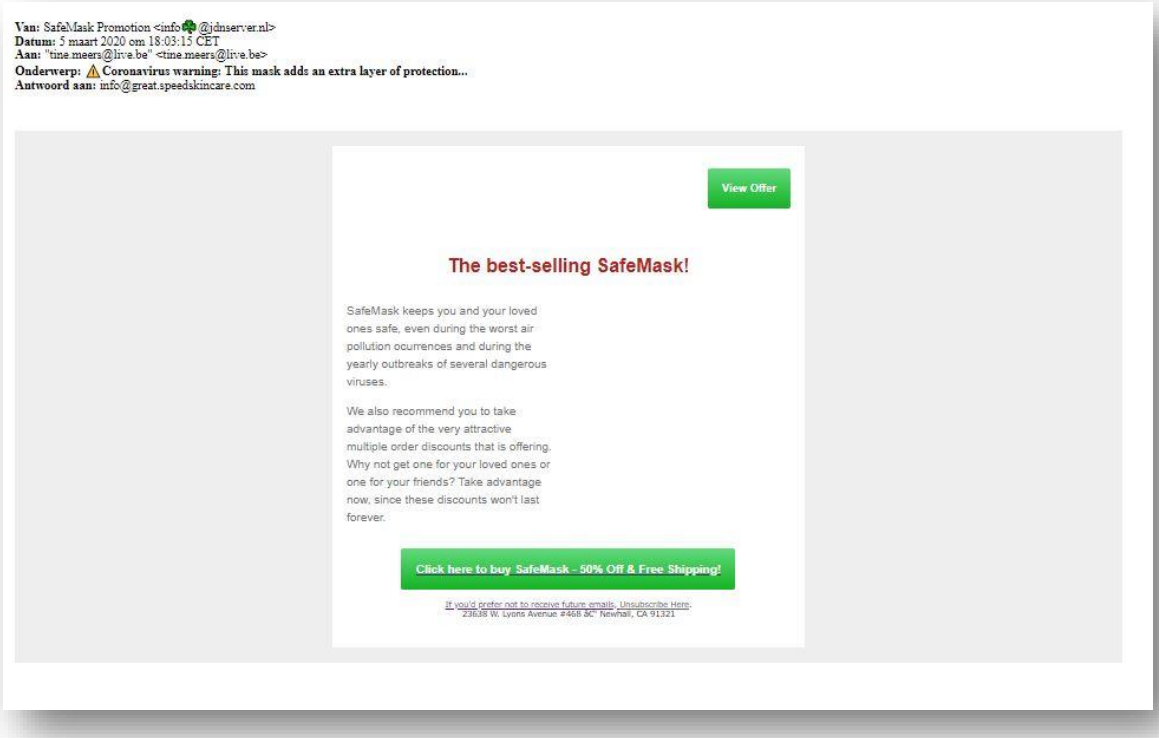
Andries Bomans
T: +32 471 66 00 06
Andries.bomans@ccb.belgium.be

Katrien Eggers
T: +32 485 76 53 36
Katrien.eggers@cert.be

Over de Cyber Security Coalition:
De *Cyber Security Coalition* heeft als missie de Belgische cyberveiligheid weerbaarder te maken door een sterk ecosysteem voor cyberbeveiliging op nationaal niveau uit te bouwen. Dit is mogelijk door de vaardigheden en expertise van de academische wereld, bedrijven en de overheid samen te brengen in een op vertrouwen gebaseerd platform dat zich focust op het bevorderen van informatie-uitwisseling, operationele samenwerking, het formuleren van aanbevelingen voor efficiëntere beleidslijnen en richtlijnen, en tenslotte het uitvoeren van gezamenlijke bewustmakingscampagnes voor burgers en organisaties.
www.cybersecuritycoalition.be

Perscontact Cyber Security Coalition
Sofie De Moerloose
T: 0478 78 96 07
info@cybersecuritycoalition.be


Corona worse than Ebola?
start now
Learn how to survive the Corona Virus Pandemic sweeping the world!
BREAKING:
Military Source Exposes Shocking TRUTH About Coronavirus And The "1 Thing" You Must Do Before It's TOO LATE
WARNING!
This presentation is for you...
Watch This Important Health Bulletin Before It's TOO LATE
DIGITAL DOWNLOAD
Pandemic Guide
To unsubscribe please click here
If you do not wish to continue receiving email newsletters CLICK HERE


Van: SafeMask Promotion <info@jdnserver.nl>
Datum: 5 maart 2020 om 18:03:15 CET
Aan: "tine.meers@live.be" <tine.meers@live.be>
Onderwerp: ⚠ Coronavirus warning: This mask adds an extra layer of protection...
Antwoord aan: info@great.speedskincare.com
View Offer
The best-selling SafeMask!
SafeMask keeps you and your loved ones safe, even during the worst air pollution ocurrences and during the yearly outbreaks of several dangerous viruses.
We also recommend you to take advantage of the very attractive multiple order discounts that is offering. Why not get one for your loved ones or one for your friends? Take advantage now, since these discounts won't last forever.
Click here to buy SafeMask - 50% Off & Free Shipping!
If you'd prefer not to receive future emails, Unsubscribe Here.
23638 W. Lyons Avenue #468 SC Newhall, CA 91321