24 mrt 2020 -09:45

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.

https://youtu.be/nYpOGhihqY4

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.

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

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

Katrien Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be