13 jul 2023 -10:57

Dit jaar al 4,4 miljoen phishingberichten in de mailbox van Safeonweb

Afgelopen 6 maanden kregen wij bijna 4,4 miljoen berichten in de mailbox van verdacht@safeonweb.be, wat bijna 2 miljoen meer is dan de eerste 6 maanden van 2022. Dat bewijst minstens 2 zaken: phishing is nog niet op de terugweg én mensen sturen deze valse berichten steeds vaker door naar Safeonweb.

Met deze informatie konden wij meer dan 320.000 verdachte links laten blokkeren. Minder aandachtige internetgebruikers die toch op zo'n link in een bericht klikten, werden doorverwezen naar een waarschuwingspagina en dus niet opgelicht. Dankzij al deze berichten kunnen wij wekelijks waarschuwingen publiceren op onze website en sociale media. Op die manier verwittigen we mogelijke slachtoffers zo snel mogelijk en brengen we mensen voortdurend op de hoogte van de meest recente phishingberichten.

We merken dat phishingberichten die wij ontvangen er steeds geloofwaardiger uitzien. De berichten worden zo gemaakt dat ze heel erg lijken op echte berichten. Daardoor is het gewoon heel moeilijk geworden om echte en valse berichten van elkaar te onderscheiden. We zien dat bestaande berichten of nieuwsbrieven bijna volledig worden gekopieerd of nagemaakt, waarna er één of meerdere valse links aan het bericht toegevoegd worden. De bedoeling is je vertrouwen te wekken en je te laten doorklikken naar een valse webpagina.

Laat je nooit meer vangen!

De belangrijkste manier om er zeker van te zijn of een bericht correct is, is de links in dat bericht goed te analyseren. Je doet dat door met de muis over de link of de knop te gaan zonder te klikken. Het adres van de website waarnaar de link verwijst of de URL verschijnt dan. In onderstaande voorbeelden zie je dat dat adres niet naar Engie of e-box verwijst.

Samen met de Cyber Security Coalition lanceerden we daarom Surfen zonder zorgen, een reeks eenvoudige en toegankelijke online opleidingen over cybersecurity. In het eerste deel Kijk uit waar je naartoe gaat!, leer je de links in valse berichten die in onze e-mailboxen en op onze mobiele telefoons binnenkomen, herkennen.

Ga naar Surfen zonder zorgen: https://surfenzonderzorgen.safeonweb.be/nl/modules/1

Welke verdachte berichten deden de ronde tussen januari en juni?

We zagen vooral veel 'klassiekers'. De jaarlijks terugkerende berichten van overheden of energieleveranciers over premies, belastingen, pensioenen, vakantiegeld, enz. zijn een grote inspiratiebron voor oplichters. Ze doen zich voor als de Overheidsdienst Financiën, de Federale Pensioendienst, de Vlaamse Overheid, Engie, enz...

De berichten lijken soms via My e-Box, Doccle of Mijn Burgerprofiel (Vlaanderen.be) te komen maar ze zijn

vals. Met de regelmaat van de klok duiken dergelijke berichten op.

Wat ook voor veel ergernis zorgt, zijn de steeds terugkerende valse berichten die van pakjesdiensten lijken te komen. Er moeten dan zogezegd extra kosten betaald worden, er ontbreken gegevens of er wordt gevraagd een applicatie te downloaden. Een gelijkaardig scenario lijkt van banken te komen. Je wordt gevraagd om je gegevens te bevestigen, om een nieuwe kaartlezer aan te vragen of om toegang te behouden tot je bankrekening. Ook hier is het gewoon de bedoeling om gegevens van jou te verzamelen en te misbruiken.

Een belangrijke tip om oplichting te voorkomen: klik niet op een link in een bericht

Ga zelf (via de browser en dus niet via een link in een bericht) naar de loginpagina van de organisatie om de informatie te controleren. Voor de voorbeelden hierboven ga je dus zelf naar bv. je loginpagina van bpost of een andere pakjesbezorger, je energieleverancier, e-Box of Doccle. Als je informatie over je bankrekening wil nakijken, ga dan via je homebanking website of je bankenapp.

Meer dan enkel phishing

Bij phishing is het altijd op de één of andere manier de bedoeling om gegevens van het slachtoffer vast te krijgen. Soms worden deze gegevens onmiddellijk gebruikt, bv. om je bankrekening te plunderen, maar in andere gevallen worden je gegevens bewaard en doorverkocht aan andere cybercriminelen die er op hun beurt gebruik van maken om je op één of andere manier op lichten.

Zo zijn er verschillende scenario's bekend waarbij het slachtoffer wordt overtuigd om zelf een overschrijving uit te voeren. De oplichter probeert je vertrouwen te wekken of je net bang te maken, met als enige bedoeling dat je zelf geld zal overmaken. Voorbeelden hiervan zijn relatiefraude, beleggingsfraude, WhatsAppfraude en sextortion scam.

Meer weten over verdacht@safeonweb.be?

De 5 meest gestelde vragen.

Volg Safeonweb nu ook op Instagram!

https://www.instagram.com/safeonweb.be/

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

Katrien Eggers
Woordvoerder(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Woordvoerder(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be