16 okt 2023 -10:29

Phishing: Het zit in de details! Installeer de Safeonweb browser extensie en laat je nooit meer vangen

Campagne geeft internetgebruikers nieuwe tools om veilig online te zijn

Op 16 oktober lanceren het Centrum voor Cybersecurity België (CCB), Febelfin en de Cyber Security Coalition een nieuwe sensibiliseringscampagne over phishing, onder de slogan: *Phishing: het zit in de details!* Deze vorm van online oplichting blijft talloze slachtoffers maken, zowel bij particulieren als bij bedrijven en organisaties. Het CCB en Febelfin ontwikkelen twee nieuwe tools om zich beter te kunnen wapenen tegen deze fraudevorm.

Phishing in cijfers

- In 2022 werd er in totaal 39,8 miljoen euro buit gemaakt naar aanleiding van phishing, een stijging in vergelijking met 2021: 25 miljoen euro. Dit is vooral te wijten aan de enorme stijging van het aantal uitgestuurde phishingberichten.

- 69% van de Belgen heeft de afgelopen 6 maanden minstens één phishingbericht ontvangen.
- 8% van de Belgen heeft nog nooit gehoord van phishing. Vooral jongeren weten niet wat phishing is (23%).
- 8% van de Belgen geeft aan slachtoffer te zijn geworden van phishing. Bij jongeren ligt dit percentage hoger, namelijk 12%.
- Slechts 62% van de Belgen die slachtoffer werden van phishing wisten welke stappen ze moesten ondernemen.

Bron: storytelling_phishing_nl_230602.pdf (febelfin.be)

- In 2023 (januari-september) werden er al meer dan 7 miljoen berichten doorgestuurd naar verdacht@safeonweb.be, dat is meer dan in het recordjaar 2022 waarin we 6 miljoen berichten kregen.
- Dat zijn er dagelijks gemiddeld 26.425.
- In een recente peiling die het Centrum voor Cybersecurity België liet uitvoeren (september 2023), geeft 28% van de respondenten aan dat ze geen idee hebben hoe ze een valse website kunnen herkennen.

- 78% zegt nooit op een verdachte link te klikken, maar 22% zou dit dus toch wel doen.
- 57% schat de kans om zelf slachtoffer te worden van phishing, hoog in.
- + 600 partners voeren jaarlijks campagne met Safeonweb (CCB). We bereikten hiermee de voorbije jaren de helft van de Belgische bevolking (+18 jaar).

Bron: Safeonweb, 2023

"Phishingberichten zijn een ware plaag. Ze blijven in grote aantallen circuleren en slachtoffers maken.Waarom krijgen we dat fenomeen de wereld niet uit? De mens is gemakkelijk nieuwsgierig of bang te maken. We kunnen niet weerstaan aan een aantrekkelijk aanbod.Phishers spelen in op die typische eigenschappen van de mensen.Ze proberen via allerhande smoesjes hun slachtoffers te benaderen en te overtuigen.Dat heet "social engineering".

Maar daarnaast zijn phishingberichten ook steeds moeilijker te ontmaskeren: ze zijn professioneel opgemaakt, verwijzen naar zeer overtuigende websites, enz.en oplichters gebruiken nieuwe AI toepassingen graagom overtuigende, aantrekkelijke en persoonlijke boodschappen te versturen."

Miguel De Bruycker
Directeur-generaal, Centrum voor Cybersecurity België

Waarom krijgen we phishing de wereld niet uit?

Phishing is geen nieuw fenomeen. Er is een constante in het phishingverhaal. De fraudeurs hengelen naar (bank)gegevens via verschillende kanalen zoals e-mail, telefoon, brief, sms, sociale media of WhatsApp. Ze proberen mensen financieel op te lichten door zich voor te doen als betrouwbare organisaties of instellingen (banken, overheidsdiensten, nutsbedrijven...).

Het verzonden bericht bevat een link naar een valse website, waar het slachtoffer wordt gevraagd om persoonlijke bankcodes in te voeren. Zodra de fraudeurs deze persoonlijke bankcodes in handen krijgen,

kunnen ze namens het slachtoffer transacties uitvoeren.

Phishing: het zit in de details!

Nochtans is het niet onmogelijk om phishingberichten en phishingwebsites ontmaskeren. Het zit in de details en tevens de slogan van de nieuwe campagne. Om er bijvoorbeeld voor te zorgen dat je niet naar een website van een oplichter surft, moet je de URL van de website leren lezen. Hoe doe je dat?

Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, … en voor de allereerste slash "/", ook echt de naam van de organisatie? Dan kan je gerust zijn dat je naar de echte website gaat. Maar zie je op die plaats wat anders? Een rare combinatie, of het domein dat je verwacht maar met een klein verschil? Kijk dan uit want oplichters kunnen die gebruiken.

Een voorbeeld:

- Bij de link www.safeonweb.be/tips is het domein safeonweb. Hier ga je naar de juiste website.
- Bij de link www.safeonweb.tips.be/safeonweb is 'tips' het domein en word je naar een andere website geleid.

Gouden tip: Heb je twijfels? Klik dan niet op een link in een bericht, maar ga zelf naar de website door de URL die je kent en gewoonlijk gebruikt, in te typen in je browserbalk.

Nieuwe tool helpt onbetrouwbare websites te herkennen:

Omdat het voor vele mensen moeilijk blijft om een URL goed te lezen en begrijpen, lanceren we een extra hulpmiddel: de Safeonweb browser extensie, die je helpt de betrouwbaarheid van een website te beoordelen. De extensie kent een vertrouwensniveau toe aan elke website: hoog, gemiddeld of laag. Dit niveau is gebaseerd op bekende factoren over het domein van de website, de eigenaar ervan en het certificatieniveau dat is verkregen bij een certificeringsautoriteit.

De call to action bij de campagne is dan ook: Installeer de Safeonweb browser extensie in je browser. Deze waarschuwt als je een onveilige website bezoekt en het gevaarlijk is om je gegevens in te voeren.

Hoe werkt de Safeonweb browser extensie?

Wanneer je een website bezoekt, toont de extensie het betrouwbaarheidsindex dat aan het domein van de website werd gegeven: groen, oranje of rood.

Het doel van de Safeonweb browser extensie is alleen om informatie te verstrekken over de verificatie van de organisatie en / of de eigenaar van de website, niet de inhoud ervan. Zelfs met een hoge betrouwbaarheidsindex kan een website altijd worden gehackt en kwaadaardige software bevatten. Wees voorzichtig met wat je deelt en ondertekent. Onderteken nooit een transactie (via itsme® of jouw kaartlezer) op verzoek van iemand die zich voordoet als "helpdesk" of "bankmedewerker".

Hoe installeer ik de Browserextensie?

Volg deze stappen om de Safeonweb-Browserextensie op je Chrome-browser te installeren:

- Open de Chrome Web Store
- Zoek de Safeonweb-browserextensie en selecteer ze.
- Klik op de knop 'Toevoegen aan Chrome'.
- Klik in het pop-upvenster op de knop 'Extensie toevoegen'.
- Selecteer het puzzelstukje in de rechterbovenhoek van je browser en “pin” de Safeonweb-extensie.
- Het Safeonweb-pictogram verschijnt aan de rechterkant van de adresbalk. De kleur ervan verandert afhankelijk van het vertrouwensniveau van de website die je bezoekt.

Andere Safeonweb tools voor veilig surfen

Naast de Safeonweb browser extensie heeft Safeonweb ook nog 3 andere reeds bestaande tools:

1. E-mailadres:verdacht@safeonweb.be
2. De Safeonweb app
3. De Safeonweb e-learning

Febelfin daagt je uit met de‘Hacker Hotline’

Met de Hacker Hotline, een mobiele escape room, wil Febelfin jongeren op een ludieke manier bewust maken van de gevaren van online fraude en hen helpen om zichzelf hier tegen te wapenen. Spelers worden uitgedaagd om slimmer te zijn dan de phisher… Het spel sluit naadloos aan bij deze nieuwe campagne want je wint het spel alleen door op details te letten

Over het spel zelf

Iedereen kan slachtoffer zijn van online fraude. In de Hacker Hotline ben jij het aanspreekpunt van slachtoffers van phishing en oplichting. Het is jouw taak om via de telefoon- en videolijn hulp te bieden aan paniekerige mensen,een race tegen de klok. Het spel wordt nog spannender wanneer dehacker ook plotseling op het toneel verschijnt. Ontdek meer in deze video of via deze link.

De Hacker Hotline is een samenwerking tussen Febelfin en het creative agency Hurae.

"“The Hacker Hotline’ is een mobiele escape room waarmee Febelfin naar jongeren, partners, scholen en evenementen trekt om te sensibiliseren voor online fraudevormen zoals bijvoorbeeld phishing. Tijdens het spel leer je meer over de technieken die fraudeurs gebruiken om mensen in de val te lokken en leer je jezelf te wapenen tegen dergelijke fraude. Eenmaal je uit de bus ontsnapt bent, heb je alle tools in handen om ook in het echte leven veilig online te gaan. Ondertussen leer je ook kernbegrippen kennen zoals twee factor authenticatie of leer je wat een sterk wachtwoord is.”"

Karel Baert
CEO Febelfin.

Samen campagne voeren

Alleen door samen te werken met overheden, politie, justitie, telecomsector…, kunnen we de strijd tegen phishing aan. Daarom sloegen het CCB, Febelfin en de Cyber Security Coalition, samen met meer dan 600 partners, de handen in elkaar voor een nieuwe, brede sensibiliseringscampagne. Want de waakzaamheid van de internetgebruiker moet omhoog. Een alerte burger is er twee waard.

De bedoeling is om een zo breed mogelijk publiek aan te spreken zodat de campagne niemand kan ontgaan. Zo zal de campagne te zien zijn via tal van kanalen: de centrale boodschap wordt de wereld in gestuurd via televisiespots en in de bioscoop. Ook via sociale media zal gesensibiliseerd worden voor de gevaren van phishing. Al het campagnemateriaal kan je downloaden op https://safeonweb.be/nl/campagnemateriaal

"Elk jaar blijft het bedreigingslandschap zich ontwikkelen, waardoor een collectieve reactie van het bedrijfsleven, de overheid, de academische wereld en burgers nodig is. De nationale bewustwordingscampagne van de CCB en zijn partners biedt een essentieel platform voor alle belanghebbenden om een actieve rol te spelen in het versterken van onze digitale verdediging."

Séverine Waterbley
Voorzitter van de FOD Economie en Bestuurslid Cyber Security Coalition

Meer informatie?

Aarzel niet om het Centrum voor Cyber Security België of Febelfin te contacteren voor meer informatie:

- Centrum for Cybersecurity Belgium:

- Katrien Eggers via katrien.eggers@ccb.belgium.be, 0485765336
- Michele Rignanese via michele.rignanese@ccb.belgium.be, 0477 38 87 50

- Febelfin: Isabelle Marchand via press@febelfin.be of 02/507.68.31

Wie is wie?

Over het Centrum voor Cybersecurity België

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen. www.ccb.belgium.be

Over Febelfin

Febelfin, of ook de federatie van de Belgische banksector. Als sectorfederatie zijn wij de spreekbuis van banken en vertegenwoordigen wij onze leden bij bv. beleidsmakers, toezichthouders, beroepsfederaties en belangenverenigingen. Febelfin vertegenwoordigt ongeveer 245 financiële instellingen in België.
De missie van Febelfin: Een financiële sector laten groeien die ten dienste staat van de maatschappelijke behoeften.

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. Meer dan 1,200 vertegenwoordigers van onze 160 lid organisaties nemen deel aan onze activiteiten en dragen zo bij aan onze missie.

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