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

BRUSSEL, 16 OKTOBER 2023
Op 16 oktober lanceren het Centrum voor Cybersecurity België[1] (CCB), Febelfin en de Cyber Security Coalition een opvallende sensibiliseringscampagne over phishing: *Phishing: het zit in de details!* Deze vorm van online oplichting is in opmars en blijft talloze slachtoffers maken, zowel bij particulieren als bij bedrijven en organisaties.

Phishing in cijfers

- In 2022 werd er in totaal 39,8 miljoen euro buit gemaakt naar aanleiding van phishing, een stijging in vergelijking met vorig jaar (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 (bron: Febelfin ism IndiVille, maart 2023)
- 8% van de Belgen heeft nog nooit gehoord van phishing. De oudere leeftijdsgroep scoort op dit vlak beter, 4% heeft nog nooit van phishing heeft gehoord, wat een verbetering is ten opzichte van 2022 (7%). Hoewel er sprake is van een lichte verbetering ten opzichte van 2021 (24%) en 2022 (30%), is het aantal jongeren die niet weet wat phishing is, te hoog (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.

[1] Het CCB is de nationale autoriteit voor cyberveiligheid in België en staat onder gezag van de Eerste Minister.

- + 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

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.

> *Phishingberichten zijn een ware plaag. Ze blijven in grote aantallen circuleren en slachtoffers maken. Waarom krijgen we dat fenomeen de wereld niet uit? Er zijn verschillende redenen. 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 bevatten zelden nog schrijffouten, zijn professioneel opgemaakt, verwijzen naar zeer overtuigende websites, enz. De cybercriminelen hebben zich geprofessionaliseerd. De toekomst ziet er niet onmiddellijk rooskleurig uit. De opmars van AI opent veel positieve perspectieven, maar ook oplichters zullen de verschillende toepassingen maar al te graag gebruiken om overtuigende, aantrekkelijke en persoonlijke boodschappen te versturen.*
>
> **Miguel De Bruycker**, directeur-generaal, Centrum voor Cybersecurity België

Phishing: het zit in de details!

Nochtans is het niet onmogelijk om phishingberichten en phishingwebsites ontmaskeren. Het zit in de details. Om ervoor te zorgen dat je niet naar een website van een oplichter klikt, 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!

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.

Oplichters kunnen URL's gebruiken met een klein verschil. Kijk dus altijd heel goed naar de URL voordat je er op klikt. 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.

Het Centrum voor Cybersecurity België lanceert de Safeonweb browser extensie

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 te beoordelen van elke website die je bezoekt. 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 extensie in je browser. Deze zal je waarschuwen als je een onveilige website bezoekt en wanneer het gevaarlijk is om je gegevens in te voeren.

Surf voor meer informatie over het installeren en gebruiken van deze nieuwe tool naar www.safeonweb.be.

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

1. **E-mailadres: verdacht@safeonweb.be**

Stuur verdachte bericht door naar verdacht@safeonweb.be. Uit al de berichten die jullie naar verdacht@safeonweb.be sturen, onderzoeken wij verdachte links. Als een minder aandachtige internetgebruiker op die link klikt, krijgt die een duidelijke waarschuwing om niet naar die pagina te surfen.

2. **De Safeonweb app**

Wij verzamelen informatie over veel voorkomende verdachte berichten en delen deze via de Safeonweb app. Zo ben je snel op de hoogte wanneer verdachte berichten de ronde doen. Je kan de Safeonweb app vinden in de officiële appstores (App Store en Google Play Store).

3. **De Safeonweb e-learning**

Leer verdachte berichten herkennen in 10 minuten: Ga naar surfenzonderzorgen.safeonweb.be

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 snel geld verdienen en hen helpen om zichzelf hiertegen te wapenen. Spelers worden uitgedaagd om slimmer te zijn dan de phisher… Het spel sluit naadloos aan bij deze nieuwe campagne.

> *‘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.

Voor wie is het?
In de eerste plaats is de escape game er voor jongeren om ze bewust te maken van de gevaren van snel geld verdienen en fraudevormen zoals phishing en onder andere whatsapp fraude. Maar ook het grote publiek heeft baat bij meer sensibilisering en kan het spel spelen. De Hacker Hotline kan ingezet worden door organisaties, verenigingen, scholen of partners die willen waarschuwen voor online fraude.

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 die wil informeren en waarschuwen. Want de waakzaamheid van de internetgebruiker moet omhoog. Een alerte burger is er twee waard en dat is het doel van deze sensibiliseringscampagne.

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 Cybersecurity 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