Persbericht 1 oktober 2019, Brussel

“Relax. Denk twee keer na voor je op een link klikt”

Oktober: maand van de cybersecurity

In het kader van de **European Cyber Security Month** lanceren het Centrum voor Cybersecurity België (CCB) en de Cyber Security Coalition voor de vijfde keer samen een **sensibiliseringscampagne** rond **cyberveiligheid**. We gaan opnieuw de strijd aan tegen **phishing**.

Phishing blijft het grootste cyberveiligheidsprobleem voor burgers in België. Het is een belangrijke toegangspoort voor cybercriminelen tot toestellen en informaticasystemen. Dit jaar (januari – september) ontvingen we al **meer dan 1 miljoen berichten op verdacht@safeonweb.be**. Vorig jaar waren er dat, verspreid over het hele jaar, 648.000. We zien dit jaar een grote stijging.

> *“Phishing wordt door cybercriminelen gebruikt om malware te verspreiden, persoonlijke gegevens te bemachtigen en geld te stelen. Door de Belgische bevolking weerbaar te maken tegen phishing vangen we als het ware drie vliegen in één klap. Hoe meer berichten we ontvangen via verdacht@safeonweb.be, hoe meer valse websites we kunnen blokkeren. Hoe sneller mensen ons verdachte berichten toesturen, hoe sneller we die valse websites blokkeren, waardoor er minder slachtoffers vallen. Wij vragen de Belgische bevolking dan ook om verdachte berichten te blijven doorsturen naar verdacht@safeonweb.be”*
>
> - Miguel De Bruycker, directeur CCB

Tijdens de campagnemaand oktober willen we de aandacht vestigen op het thema via radiospotjes, filmpjes op social media, banners en andere campagnematerialen. Op de campagnewebsite https://campagne.safeonweb.be/nl staan nuttige tips en informatie. Je vindt er ook de digitale gezondheidsindex terug, zodat je je cyber security kennis kan testen. Al het campagnemateriaal kan je downloaden op https://safeonweb.be/nl/campagnemateriaal

We gaan met onze boodschap ook letterlijk naar de burger toe: we houden een actie in 5 grote treinstations en we gaan op tour met de Federal Truck naar 6 academische instellingen.

> *"Met de Federal Truck gaan wij zelf naar de bevolking toe. Bij verschillende academische instellingen in Brussel, Vlaanderen en Wallonië houden we halt en nodigen we studenten uit om meer te weten te komen over phishing"*
>
> - Phédra Clouner, vice-directeur CCB

Federale overheidsdiensten, academische instellingen, grote en kleine bedrijven, maar ook vzw's en andere organisaties ondersteunen de campagne. **Dit jaar zullen meer dan 500 partners** het campagnemateriaal helpen verspreiden.

"Ook binnen het bedrijfsleven vormt phishing nog steeds een groot probleem. Daarom raad ik organisaties aan zeker gebruik te maken van deze gratis materialen om hun medewerkers, klanten en professionele contacten te wapenen tegen phishing."

- Jan De Blauwe, voorzitter Cyber Security Coalition

Een van de partners die dit jaar de campagne ondersteunt is de zoekertjessite 2dehands.be. *"Wij ondersteunen als partner de campagne tegen phishing"* aldus Alain Buyle, woordvoerder 2dehands *"Maandelijks handelen miljoenen mensen succesvol op ons platform en hoewel het in bijna alle gevallen goed gaat, is elk geval van oplichting er een te veel. Naast de maatregelen die we zelf implementeren, geven we dan ook graag de tips van de campagne mee om veilig te handelen"*

De nationale sensibiliseringscampagne tegen phishing legt nadruk op **valse berichten**. Phishing gebeurt immers vandaag op verschillende platformen, en niet enkel per e-mail: ook per SMS, Whatsapp, via Facebook Messenger en andere platformen worden mensen met valse berichten om de tuin geleid. Ook gebruikers van 2dehands kunnen te maken krijgen met phishing. De meest courante vorm is die waarbij malafide gebruikers vertrouwelijke gegevens proberen te bemachtigen door de transactie te laten plaatsvinden op een ander platform dan deze die wordt voorzien op 2dehands.be. Vervolgens proberen ze via valse websites bankgegevens en andere persoonlijke gegevens te stelen. *"We raden alle gebruikers aan twee keer na te denken voor ze klikken op een link of in te gaan op de vraag de transactie te laten plaatsvinden op een ander platform"* Alain Buyle, woordvoerder 2dehands.

Iwein Segers en **Jérôme de Warzée** zijn de digitale gezondheidscoaches bij deze campagne.

Tipfilmpjes
De campagne wordt gelanceerd op 1 oktober 2019 en duurt de hele maand. Om de campagne te ondersteunen stellen we naast gratis materiaal (afdrukbare posters, banners en online visuals) ook verschillende tipfilmpjes ter beschikking. Aan de hand van deze filmpjes leggen we stap voor stap uit hoe veilig je een link controleert, wat een verdachte domeinnaam is, hoe je de afzender controleert en meer.

Phishing, phishing en nog eens phishing

Herken valse berichten
"Met deze campagne willen we alle internetgebruikers wapenen tegen phishing: zowel de professionele als de occasionele gebruikers, jongeren en ouderen" aldus Miguel de Bruycker, directeur van het Centrum voor Cybersecurity België.

Phishingberichten:

- krijg je meestal onverwacht en zonder reden
- zijn dwingend of willen je nieuwsgierig maken
- bevatten taalfouten of zijn vreemd geschreven
- hebben een vage aanspreektitel of gebruiken je e-mailadres als aanspreking
- komen van een onbekende afzender
- hebben een link die niet naar een veilige website leidt

"Niet enkel e-mails kunnen valse berichten zijn. Steeds vaker proberen oplichters hun slag te slaan via valse sms-berichten. Dat fenomeen heet Smishing*. Ook via sociale media zoals Facebook en WhatsApp kan je phishingberichten ontvangen."*

- Miguel De Bruycker, directeur CCB

verdacht@safeonweb.be

In 2018 ontvingen wij dankzij verdacht@safeonweb.be 648.000 berichten. Dit jaar ontvingen we er al **meer dan 1 miljoen**. In 2018 konden we dankzij dit initiatief en de hulp van de Belgische bevolking 4-5 valse websites per dag laten blokkeren. In 2019 konden we gemiddeld genomen **meer dan 30 valse websites per dag** laten blokkeren, dit is ongeveer **7 keer meer**.

Na deze campagne herkent iedereen een vals bericht, en weet wat te doen: weg ermee, verwijderen dat bericht. De Bruycker: *"Maar we gaan nog een stapje verder. We vragen iedereen om verdachte berichten door te sturen naar verdacht@safeonweb.be en ze vervolgens te wissen. De verdachte berichten die we ontvangen op verdacht@safeonweb.be worden door het Centrum voor Cybersecurity België automatisch gescand met geavanceerde anti-virustechnologie. Gevaarlijke links komen op een zwarte lijst en worden geblokkeerd door de voornaamste webbrowsers. Zo maken we van het internet weer een veiligere plek."*

Cybercriminelen zijn steeds creatiever

Cybercriminelen zijn steeds creatiever in hun pogingen om mensen om de tuin te leiden:

- ze sturen valse berichten die zo overtuigend zijn dat je de bijlage opent,
- ze beloven je een grote beloning als je hun enquête invult en je gegevens achterlaat,
- ze bedreigen je als je niet reageert,
- en ze gebruiken steeds meer kanalen (e-mail, WhatsApp, Messenger, …).

Gelukkig zijn veel internetgebruikers alert genoeg en lopen ze niet in de val! Toch kan iedereen slachtoffer worden.

Phishing, het kan iedereen overkomen

Phishing is een gekende techniek om bankgegevens te stelen en malware te verspreiden. Cybercriminelen gebruiken ook valse berichten om persoonlijke gegevens te stelen om bijvoorbeeld accounts over te nemen. En dit kan iedereen overkomen!

Deze zomer werd het Instagramaccount van Belgium. Uniquely Phenomenal gehackt via phishing. De cybercriminelen stuurden een valse e-mail die zogezegd van Instagram zelf kwam, met de melding dat er copyright problemen waren op het account. Om dit op te lossen moest men zich opnieuw aanmelden via een link in het bericht. Door op de link te klikken, werd men naar een valse website gestuurd die bijna identiek dezelfde was als de officiële Instagramwebsite. Door de inloggegevens in te geven, kregen de cybercriminelen toegang tot het account. De informatie was geloofwaardig en goed

geschreven. De valse e-mail zag er ook professioneel uit. Kortom, het kan iedereen overkomen. En het kan voor veel ellende zorgen, zoals imagoschade.

Gelukkig werd de toegang snel hersteld door contact te nemen met Instagram. Om phishing te vermijden in de toekomst werden alle medewerkers gesensibiliseerd en werd de toegang tot het Instagramaccount beveiligd met Two Factor Authentication (2FA).

#####

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