29 jan 2025 -08:39

44% van de Belgen stuurt phishingberichten door naar verdacht@safeonweb.be

In 2024 stuurden oplettende burgers meer dan 9 miljoen berichten door naar verdacht@safeonweb.be. In recordjaar 2023 waren dat er nog 10 miljoen. Gemiddeld kregen we in 2024, 25.900 berichten per dag toegestuurd. We willen alle internetgebruikers die dit blijven doen van harte bedanken! Samen maken we het internet een veiligere plek.

Met deze informatie konden wij precies 1.644.732 verdachte links detecteren en omleiden. Minder aandachtige internetgebruikers die toch op zo'n link klikken, worden namelijk door ons omgeleid naar een waarschuwingspagina en dus niet opgelicht.

Uit een survey van het Centrum voor Cybersecurity België (Safeonweb, 12/2024) blijkt dat 44% van de Belgen berichten doorstuurt naar verdacht@safeonweb.be. In 2023 was dat 39%, dus het e-mailadres blijft aantrekkelijk. Voor ons is dit een bijzondere bron aan informatie die we in eerste plaats gebruiken voor ons phishing schild (BAPS Systeem), maar ook om burgers te waarschuwen.

Dankzij al deze berichten kunnen wij gerichte waarschuwingen publiceren op Safeonweb.be, Facebook, Instagram en X over phishingberichten die de ronde doen. Deze 'alerts' versturen we ook via de Safeonweb App. In 2024 publiceerden we 81 waarschuwingen over de meest voorkomende actuele phishingberichten.

Phishing? Niets nieuws onder de zon. Of toch?

Phishing blijft in 2024 een van de meest gebruikte en evoluerende aanvalsmethoden in cybercriminaliteit. (zie ENISA Threat Landscape, 2024)

Op het eerste gezicht zijn de meeste phishingberichten zeer gelijkaardig met die van de voorbije jaren. Je hebt de berichten die van overheidsdiensten, politie, banken, Itsme, enz. lijkten te komen en daarnaast ook de aanbiedingen in de categorie 'te mooi om waar te zijn', van onwaarschijnlijke promoties, tot éénmalige koopjes, en zelfs de 'verloren erfenis' dook weer op.

Oplichters volgen nog steeds zeer nauwlettend de actualiteit en gebruiken actuele gebeurtenissen om hun phishingberichten geloofwaardig te maken. Zo zien we bv. jaar na jaar rond de eindejaarsperiode meer berichten verschijnen rond Kerstpromoties of te leveren pakjes.

Toch zien we 5 verschuivingen.

1. Smishing en vishing zitten in de lift

Smishing (phishing via sms) en vishing (phishing via telefoongesprekken) nemen toe. Cybercriminelen gebruiken dit om rechtstreeks respons- en 2FA-codes te ontfutselen. Een voorbeeld. Ze bellen hun slachtoffer op en doen zich voor als iemand van Cardstop die wil helpen omdat er zogezegd een verdachte transactie gebeurde op de bankrekening. De oplichter zal het slachtoffer overtuigen om bv. responscodes door te geven of om Itsme te openen en de authenticatie te voltooien.

2. Meer phishing via social media

Platformen zoals LinkedIn, Facebook, Instagram en WhatsApp worden steeds vaker gebruikt om phishinglinks te verspreiden. De principes zijn dezelfde als bij phishing per e-mail of sms.

3. Meer gepersonaliseerde aanvallen

Door gelekte persoonsgegevens van eerdere datalekken worden aanvallen gepersonaliseerd, wat de geloofwaardigheid van phishing, en ook smishing en vishing verhoogt. Oplichters gebruiken deze gegevens om je vertrouwen te wekken. Als je opgebeld wordt door een zogezegde bankmedewerker die jouw naam, geboortedatum en andere gegevens kent, ben je geneigd te geloven dat dit werkelijk een bankmedewerker is.

4. AI en deepfake-technologie maken phishing geloofwaardiger

Cybercriminelen maken ongetwijfeld vaker gebruik van AI om phishingberichten te personaliseren, waardoor ze overtuigender worden. Deepfake-audio en -video kunnen ingezet worden om CEO-fraude en spearphishing te verfijnen, door het nabootsen van de stem van de CEO van een bedrijf. Hoewel dergelijke praktijken op dit ogenblik zeker mogelijk zijn, hebben we nog geen concrete voorbeelden kunnen detecteren.

5. Https is geen garantie op veiligheid

Jaar na jaar merken we dat meer criminelen SSL-certificaten gebruiken om hun phishing URL’s er betrouwbaarder uit te laten zien. Dat wil concreet zeggen dat je als internetgebruiker er niet meer kan van uitgaan dat een URL die begint met https per definitie veilig is.
https://safeonweb.be/nl/blog/een-https-website-altijd-veilig-waar-niet-waar

Belgisch Anti-Phishing Shield (BAPS)

Dit phishing schild beschermt de burgers van ons land tegen cybercriminelen. Het is het pronkstuk van het Centrum voor Cybersecurity België (CCB). Met deze spitstechnologie behoren we als klein land tot de absolute wereldtop.

Hoe werkt het?

1. Het Centrum voor Cybersecurity België (CCB) ontvangt informatie over mogelijk schadelijke websites wanneer internetgebruikers verdachte berichten doorsturen naar verdacht@safeonweb.be.

2. De bijlagen en andere links worden vervolgens uit de verdachte berichten gehaald. De URL's worden ook uit schermafbeeldingen en QR-codes gehaald.

3. Het analyseert de URL/link/bijlage. Als het een schadelijke site blijkt te zijn, wordt deze opgenomen in een lijst en naar onze partners gestuurd (ISP's, Google Safe Browsing en Microsoft SmartScreen).

4. Wanneer een internetgebruiker op een link klikt die naar een kwaadaardige site leidt, vergelijkt de ISP in kwestie het DNS-verzoek met de lijst van kwaadaardige sites.

5. De gebruiker wordt vervolgens omgeleid naar een waarschuwingspagina en kan de kwaadaardige site niet bezoeken.

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