Nieuwsbrief FASv nr.05, november 2021

Phishing trends die je in de gaten moet houden

Via phishing proberen cybercriminelen je inlognaam, wachtwoord of betaalgegevens te stelen voor geld of identiteitsfraude. Tot 2010 gebeurde dat vooral via de post. Toen internetfraudeurs eenmaal door hadden dat het via e-mail veel goedkoper was en het naar meer mensen tegelijkertijd kon, was dat het belangrijkste kanaal. Tegenwoordig zijn er nog veel meer phishing kanalen bijgekomen, zoals WhatsApp. In dit blog vertellen we je de belangrijkste phishing trends van nu en hoe je zelf phishing kan herkennen en voorkomen.

Trend 1: Phishing tijdens de feestdagen

In december kopen we allemaal meer online dan normaal. Het aantal online aankopen stijgt door onder andere Black Friday, Cyber Monday en last minute Sinterklaas of kerstaankopen. De hele maand worden we extra verleid door speciale, tijdelijke aanbiedingen van bekende merken. Cybercriminelen spelen handig in op dit gevoel.
En sturen tijdens periode extra vaak valse e-mails met aanbiedingen die we echt niet mogen missen. Dit doen ze om zo aan je persoons- of betaalgegevens te komen.

Hoe herken je een neppe aanbieding?

- Het product is spotgoedkoop. Elders vind je het niet zo goedkoop.
- Het product is nergens meer te verkrijgen. Maar als je je inschrijft voor een speciale wachtlijst en je gegevens achterlaat, dan nog wel.
- De aanbieding is eigenlijk “te mooi om waar te zijn”.

Krijg je een mail die voldoet aan 1 van deze bovenstaande punten, dan klopt er waarschijnlijk iets niet. Klik dan ook niet zomaar op een link.

Trend 2: Phishing via WhatsApp

De meest toenemende vorm van internetcriminaliteit is phishing via WhatsApp. Uit onderzoek van de Fraudehelpdesk blijkt dat in 2020 al 9.605 meldingen hiervan zijn gemaakt. Dat is bijna 4 keer zo veel als in heel 2019. De slachtoffers van WhatsApp-fraude zijn in 2020 gezamenlijk opgelicht voor 3,3 miljoen euro.

Zo herken je phishing via WhatsApp

WhatsApp-fraude begint met een bericht dat je krijgt van iemand die je kent. Vaak is dat met een onbekend nummer: diegene zegt een nieuw nummer te hebben. Op de profielfoto zie je wel jouw bekende staan. Diegene vraagt je om geld te lenen, omdat hij zijn bankpas is verloren. Er komt een smoes waarom bellen op dat moment niet mogelijk is. Soms stuurt hij een spraakbericht waarin hij vaag te horen is. Het stemgeluid van jouw bekende is van social media geplukt om het geloofwaardiger over te laten komen.
In sommige gevallen wordt zelfs je hele WhatsApp-account gehackt. De oplichters doen dan alsof ze het account overzetten naar een nieuwe telefoon. WhatsApp stuurt een verificatiecode naar het oude nummer die de oplichters weten te onderscheppen. Zo hebben ze alle telefoonnummers uit jouw contactenlijst.

Wat te doen bij phishing via WhatsApp

Bel altijd eerst om te vragen of het bericht klopt, hoe goed je diegene ook kent. Maak geen geld over zolang je hem of haar niet telefonisch hebt gesproken. Heb je het geld al overgemaakt? Bel dan zo snel mogelijk je bank om de betaling te stoppen en maak een melding door online aangifte te doen van WhatsApp-fraude.
Om te voorkomen dat je account wordt gehackt, kan je een tweefactorauthenticatie instellen. Open WhatsApp en ga naar 'Instellingen'. Klik dan op 'Account', vervolgens op 'Verificatie in twee stappen' en als laatste op 'Inschakelen'. Voer zelf een code in. Deze wordt ongeveer wekelijks gevraagd om te controleren of jij nog steeds de eigenaar van het account bent. Lees meer over WhatsApp-fraude en wat je moet doen als je account is gestolen.

Trend 3: Phishing tijdens corona

Cybercriminelen haken in op actualiteiten om mensen op te lichten. Zo maken ze nu slim gebruik van de situatie rondom het coronavirus. Ze sturen bijvoorbeeld phishing e-mails, phishing WhatsApp-berichten of phishing sms'jes (ook wel smishing genoemd) met besmette links. Ook worden er steeds meer neppe webshops opgericht.

Zo herken je corona phishing

De phishing e-mails, WhatsApp-berichten, sms'jes en webshops hebben allemaal te maken met het onderwerp corona. Je ontvangt bijvoorbeeld een e-mail met daarin een besmette link over een coronavaccin. Als je op deze link klikt, wordt er een virus op je computer gezet. Of je krijgt een sms'je met daarin een link naar een webshop die zogenaamd mondkapjes verkoopt. Daar betaal je de mondkapjes, maar ontvang je ze nooit.

Wat te doen bij corona phishing

Krijg je een mail van een afzender die je nooit eerder hebt gezien? Verwijder dan direct de mail. Als je per ongeluk al de mail hebt geopend, zorg er dan voor dat je niet op de link klikt en verwijder de mail alsnog. Kijk op webshops altijd naar de betaalmethode. Als je ziet dat er geen normale betaalmethode (zoals iDEAL) tussen staat maar alleen een betaallink, wees dan voorzichtig. Je kan dan beter ergens anders shoppen.

Trend 4: Phishing mails via je bank, telecomprovider of de Belastingdienst

Fraudeurs sturen steeds vaker phishing berichten uit naam van je bank, je telecomprovider of de Belastingdienst. Ze proberen zo je paspoort, rijbewijs, wachtwoord of pincode in handen te krijgen. Daarmee stelen ze jouw geld of identiteit.

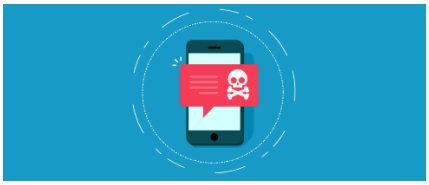
Zo herken de phishing mails

In een phishing mail van je bank, je telecomprovider of de Belastingdienst staat vaak een link die je naar een neppe website leidt die heel erg lijkt op de originele website. Jij denkt bijvoorbeeld dat je op de website van ING terecht gekomen bent, waar ze je vragen je oude pinpas op te sturen om te recyclen. Of je krijgt zogenaamd een e-mail van KPN waarin gevraagd wordt om geld over te maken voor een openstaande rekening.

Wat te doen bij phishing mails

Controleer als eerste de afzender. Phishers proberen vaak de afzender te laten lijken op het originele e-mailadres, om je er in te laten trappen. Ze zetten bijvoorbeeld 'KPN' vóór het apenstaartje, zoals kpn@mail.123.com . Klik linkjes en knoppen in e-mails nooit zomaar aan, maar beweeg er overheen met je muis (laptop of pc) of houd de link lang ingedrukt (mobiel). Je ziet dan het internetadres waar de link naar verwijst. Dit moet de originele website zijn. Linkjes in onze mails verwijzen bijvoorbeeld altijd naar een pagina op kpn.com. Controleer ten slotte de bijlage. Wij sturen alleen pdf's als bijlage. Heb je per ongeluk toch op een link geklikt in een KPN phishing mail? Of twijfel je of het een phishing mail is?
Ga dan naar onze phishing pagina om te zien wat je moet doen.

Trend 5: Smishing, phishing via sms



Phishing kan ook via sms naar je worden verzonden. Dat staat bekend als smishing. In een smishing sms doet de oplichter zich voor als een bedrijf of organisatie. De tekst bevat meestal een nepmededeling die het nodig maakt om via een link in de sms iets te gaan regelen.
De link doet zich voor als de site van het bedrijf of de organisatie, maar is dat niet. De oplichters verkrijgen zo je wachtwoorden om die verder te misbruiken.
Tip: Ga nooit in op sms verzoeken om een link te volgen en voer nooit wachtwoorden in op zo'n link. Doe nooit betalingen die erbij gevraagd worden. Bedrijven en organisaties zullen dit nooit per sms aan je vragen.

Bron: Redactie Beleef KPN