Forum Standaardisatie
Standaard Samenwerken

Recente voorbeelden spoofing

Relatie phishing, spoofing en standaarden

Phishing is een aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails (e-mailphishing). Maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.

Voor een grotere kans op succes bij een phishing-aanval kan de aanvaller iemand misleiden door te doen alsof hij iemand anders is. Dit noemen we *spoofing*. Er zijn veel soorten spoofing. Een aanvaller kan zich in een e-mail voordoen als een ander door het afzendadres te vervalsen (e-mailspoofing).

Door het juist toepassen van de e-mailbeveiligingsstandaarden DKIM, SPF en DMARC kan een organisatie spoofing van de eigen domeinnamen voorkomen. Zie voor meer informatie de themapagina 'Bestrijd e-mailfraude' op de website van Forum Standaardisatie.

Nieuws- en opiniewebsite Vox.com legde onlangs in begrijpelijke taal uit hoe e-mailspoofing werkt en voorkomen kan worden: Why coronavirus scammers can send fake emails from the WHO.

Herkenbaarheid overheid online

Naast misbruik van authentieke domeinnamen van de overheid d.m.v. e-mailspoofing, gebruiken aanvallers ook domeinnamen die lijken van de overheid te zijn voor phishing. Zo is recent het domein inspectie.nl misbruikt voor phishing namens Inspectie SZW, terwijl het domein niet van de overheid is. Dit voorbeeld staat niet op zichzelf en het benadrukt het belang van herkenbaarheid van de overheid online, om burgers in staat te stellen phishing te kunnen herkennen.

De overheid lijkt internetdomeinen soms als wegwerpartikelen te zien, en heeft onvoldoende oog voor de risico's die daarmee ontstaan. Zo is het de vraag hoe verstandig het is om te midden van fenomenen als corona-phishing en 'fake news' het domein databronnencovid19.nl (RIVM, authentiek) in het leven te roepen. Een ander voorbeeld is het domein publiekebeproeving.nl (VWS, authentiek) dat één dag voor de corona-appathon in het leven werd geroepen voor het stemmen op corona-apps. De houder van domein publiekebeproeving.nl is Trimm Multimedia B.V. en het certificaat is van Let's Encrypt. Een burger kan niet verifiëren of dit domein echt van de overheid is, of wellicht fake news of een phishingsite. Beide domeinnamen hebben tevens geen strikt DMARC beleid en zijn dus kwetsbaar voor e-mailspoofing.

Onduidelijkheid over de authenticiteit van internetdomeinen ondermijnt het vertrouwen van burgers in echte overheidswebsites/-mails. Eén van de uitgangspunten van overheidscommunicatie is dat de overheid, ongeacht het kanaal of medium, herkenbaar is als afzender. Er ligt dus een uitdaging om verstandiger om te gaan met internetdomeinen om zo de herkenbaarheid van de overheid te vergroten.

Nieuwsberichten phishing en spoofing

Het onderstaande overzicht toont nieuwsberichten over recente incidenten waarbij overheden zijn gespoofd, nieuwsberichten omtrent e-mailphishing in het algemeen, en meldingen over phishing uit naam van de overheid bij fraudehelpdesk.nl.

Nieuwsberichten m.b.t. e-mailspoofing overheid

Datum	Verwijzing	Citaat
3 april 2020	Lek bij RIVM en overheid maakte gevaarlijke nepmails criminelen mogelijk	Door een lek bij het RIVM en de Rijksoverheid was het voor cybercriminelen mogelijk om uit naam van deze organisaties gevaarlijke e-mails te versturen. Deze e-mails waren niet van echt te onderscheiden.

8 april 2020	Spoofbaar RIVM had mailbeveiliging weer uitgezet	Het RIVM heeft zich snel weten te beschermen tegen het ontdekte (en verantwoord gemelde) gevaar van mailspoofing op zijn domein. Het instituut dankt deze snelheid aan het feit dat de bescherming eerder al is ingevoerd, maar toen is uitgeschakeld. Dit blijkt uit antwoorden van een woordvoerster op vragen van AG Connect.
9 april 2020	Valse mail uit naam van Inspectie SZW bevat mogelijk malware	Uit naam van de Inspectie SZW, onderdeel van het Ministerie van Sociale Zaken en Werkgelegenheid, gaat een mail rond met als onderwerp 'Officiële kennisgeving (WS2F4W6A) met betrekking tot een mogelijk onderzoek'. Deze mail is vals en verwijst mogelijk naar schadelijke, gevaarlijke malware.
13 april 2020	"Als IT'er heb ik in mijn leven vele phishing en spam e-mails gezien, maar deze!"	De e-mail is niet in mijn spam terecht gekomen. Het taalgebruik klopt. De e-mail komt vanaf een e-mailadres wat in eerste instantie niet per se verdacht is (Weet u wat de domeinnaam van Inspectie SZW is?) De kleur van de inspectie zit in de e-mail. Er zijn zogenaamd unieke identificaties opgenomen. Vertwijfeld roep ik mijn collega erbij. Het ziet er te echt uit – en het kan nou eenmaal zo zijn dat iemand een klacht tegen je bedrijf indient.
20 april 2020	Algemene Rekenkamer: Grenscontrole op Schiphol niet genoeg beveiligd	Ook konden e-mails uit naam van de Commandant der Strijdkrachten worden verzonden.

Nieuwsberichten m.b.t. e-mailphishing algemeen

Datum	Verwijzing	Citaat
17 maart 2020	Politie waarschuwt voor phishingmails over coronavirus	De Nederlandse politie heeft vandaag een waarschuwing afgegeven voor cybercriminelen die inspelen op het nieuws rondom het coronavirus om mensen op te lichten. Het gaat onder andere om phishingmails en sms'jes die ontvangers persoonsgegevens proberen te ontfutselen.
27 maart 2020	Scherpe toename phishing vanwege corona	Al aan het begin van de corona-uitbraak in Europa zagen cybercriminelen hun kans schoon om misbruik te maken van de situatie. Met het verstrijken van de tijd is dit alleen maar toegenomen, inspelend op de toenemende paniek. Beveiligingsadviseur Barracuda noteert een stijging van het aantal phishing-gevallen van maar liefst 667% over maart.
16 april 2020	Veel meer phishing en bankpasfraude in 2019	De schade als gevolg van gestolen of verloren bankpassen is in een jaar tijd bijna verdubbeld, van 3,32 miljoen euro tot 6,61 miljoen euro. Fraude met gestolen bankpassen begint vaak met een phishing mail of valse sms. Die misleidt de ontvanger om zijn of haar bankpas met de post op te sturen en de bijbehorende pincode af te geven, bijvoorbeeld op een valse website.
17 april 2020	Gmail blokkeert 240 miljoen aan covid-19 gerelateerde spammails per dag	Google meldt in een blogposting over de beschermingsmaatregelen die het met Gmail biedt, dat de webmaildienst dagelijks 100 miljoen phishingmails blokkeert, waarvan er vorige week 18 miljoen over covid-19 gingen. Gmail bestempelde vorige week per dag nog eens 240 miljoen aan covid-19 gerelateerde mails als spam.

20 april 2020	Duitse deelstaat blundert met coronawebsite: diefstal van miljoenen	Met een heel simpele phishingactie zijn cybercriminelen er in geslaagd voor zeker tien miljoen euro aan overheidssteun weg te sluizen in de Duitse deelstaat Noordrijn-Westfalen.

Meldingen phishing uit naam overheid op fraudehelpdesk.nl

Datum	Organisatie	Melding
10 maart 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/laatste-herinnering-u-heeft-nog-een-openstaande-boete/
10 maart 2020	CJIB	https://www.fraudehelpdesk.nl/valse-email/openstaande-factuur/
11 maart 2020	Rijksoverheid	https://www.fraudehelpdesk.nl/valse-email/rijksoverheid-mogelijke-fraude-misbruik-gepleegd-met-uw-identiteitskaart/
12 maart 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/betreft-belastingschuld-afgelopen-fiscale-jaar/
16 maart 2020	CJIB	https://www.fraudehelpdesk.nl/valse-email/openstaande-factuur-2/
25 maart 2020	Waternet	https://www.fraudehelpdesk.nl/valse-email/bericht-2/
30 maart 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/uw-openstaande-schuld-met-kenmerk-is-na-meerdere-herinneringen-nog-niet-voldaan/
1 april 2020	Waternet	https://www.fraudehelpdesk.nl/valse-email/bericht-3/
1 april 2020	CJIB	https://www.fraudehelpdesk.nl/valse-email/laatste-aanmaning-3/
6 april 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/belasting/
9 april 2020	Inspectie SZW	https://www.fraudehelpdesk.nl/valse-email/officiele-kennisgeving-met-betrekking-tot-een-mogelijk-onderzoek/
9 april 2020	CJIB	https://www.fraudehelpdesk.nl/valse-email/openstaande-factuur-3/
14 april 2020	CJIB	https://www.fraudehelpdesk.nl/valse-email/betaal-nu-uw-openstaand-bedrag/
14 april 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/belasting-2/
20 april 2020	Belastingdienst	https://www.fraudehelpdesk.nl/valse-email/belasting-3/