Ministerie van Economische Zaken
en Klimaat

Covid-19-phishing

Criminelen misbruiken de coronacrisis voor phishing aanvallen

Een nieuwe trend in phishing e-mails

De enorme toename van nieuwsberichten over covid-19 en de bijbehorende veranderingen in de samenleving hebben een nieuwe impuls van cyber criminele activiteiten tot gevolg. Criminelen grijpen de coronacrisis aan om hun frauduleuze phishing campagnes aan te passen aan de huidige situatie, waarmee ze hopen hun effectiviteit te vergroten. Volgens Google is dezer dagen ongeveer 1 op de 5 phishing e-mails gerelateerd aan covid-19, zo'n 18 miljoen e-mails van de 100 miljoen die Gmail dagelijks blokkeert. (zie artikel van Google)

Veel van deze e-mails kunnen automatisch worden tegengehouden, maar niet allemaal.

Omdat het openen van zo'n e-mail schade kan opleveren voor Nederlandse bedrijven, is het van belang een succesvolle phishing poging zo veel mogelijk te voorkomen door die op tijd te herkennen. Onderzoeksinstituut TNO ziet dat het doel van deze criminelen grotendeels hetzelfde is gebleven, maar dat voornamelijk de lokmiddelen en tactieken zijn aangepast aan de huidige situatie en de bijbehorende maatregelen en gevoelens. In deze factsheet zetten we de verschillende soorten van deze covid-19-phishing uiteen, zodat deze makkelijker te herkennen zijn.

TNO innovation for life

digital trust center.

Wat is phishing?

Een cybercrimineel heeft als doel om ervoor te zorgen dat de ontvanger van een phishing email:

- Op een link klikt of bijlagen opent, waardoor kwaadaardige software kan worden gedownload en geïnstalleerd.
- Zijn of haar inloggegevens weggeeft, door deze bijvoorbeeld in te vullen in een hiervoor ontworpen phishing website, of door deze te versturen via een email.

De motieven van een dergelijke crimineel zijn vaak financieel gewin of het stelen van persoonsgegevens. Meer informatie over wat phishing precies is vind je op de website van het Digital Trust Center[1].

Tactieken covid-19-phishing

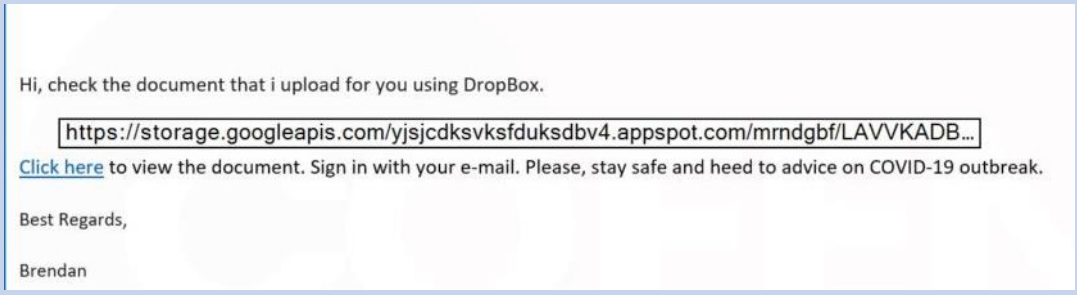
Cybercriminelen gebruiken social engineering tactieken om lezers van hun e-mails ervan te overtuigen ergens op te klikken. Deze tactieken bestaan vaak uit het losmaken van een negatieve emotie, zoals het benadrukken van urgentie of het opwekken van angst. We zien ook e-mails die inspelen op positieve emoties, zoals collegialiteit. Beiden tactieken worden ook veel gebruikt bij het uitvoeren van covid-19-phishing aanvallen.

Cybercriminelen wekken vertrouwen door zich voor te doen als iemand anders, door middel van spoofing kunnen zij zelfs het afzender emailadres veranderen in een vertrouwd adres. Door zich voor te doen als een bekende of een autoriteit, vergroten zij de kans dat het slachtoffer ergens op klikt. We zetten drie soorten mogelijke afzenders van covid-19-phishing voor je op een rij, samen met een aantal voorbeelden.

1. Iemand van binnen het bedrijf

Een crimineel kan zich voordoen als iemand die binnen hetzelfde bedrijf werkt, bijvoorbeeld als een directe collega die een bijlage doorstuurt (zie voorbeeld 1), de IT-service desk die een update of wijziging aankondigt (zie voorbeeld 2), een hooggeplaatste collega (bijv. de CEO) of de financiële afdeling.

Voorbeeld 1: Bericht van een directe collega


Hi, check the document that i upload for you using DropBox.

https://storage.googleapis.com/yjsjcdksvksfduksdbv4.appspot.com/mrndgbf/LAVVKADB...

Click here to view the document. Sign in with your e-mail. Please, stay safe and heed to advice on COVID-19 outbreak.

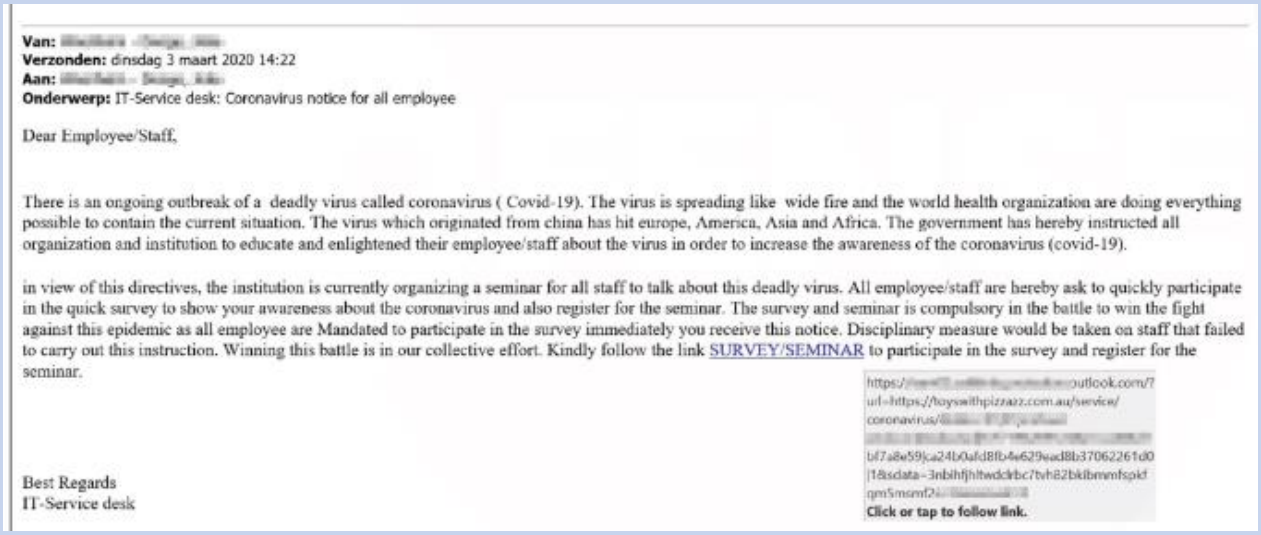
Best Regards,

Brendan

Phishing e-mail waarin een crimineel zich voordoet als een collega die een Dropbox document deelt, maar eigenlijk probeert gegevens te stelen. (www.coronavirusphishing.com)

[1] https://digitaltrustcenter.nl/phishing

Voorbeeld 2: Bericht van de IT-service desk



Van: [redacted]
Verzonden: dinsdag 3 maart 2020 14:22
Aan: [redacted]
Onderwerp: IT-Service desk: Coronavirus notice for all employee

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link SURVEY/SEMINAR to participate in the survey and register for the seminar.

Best Regards
IT-Service desk

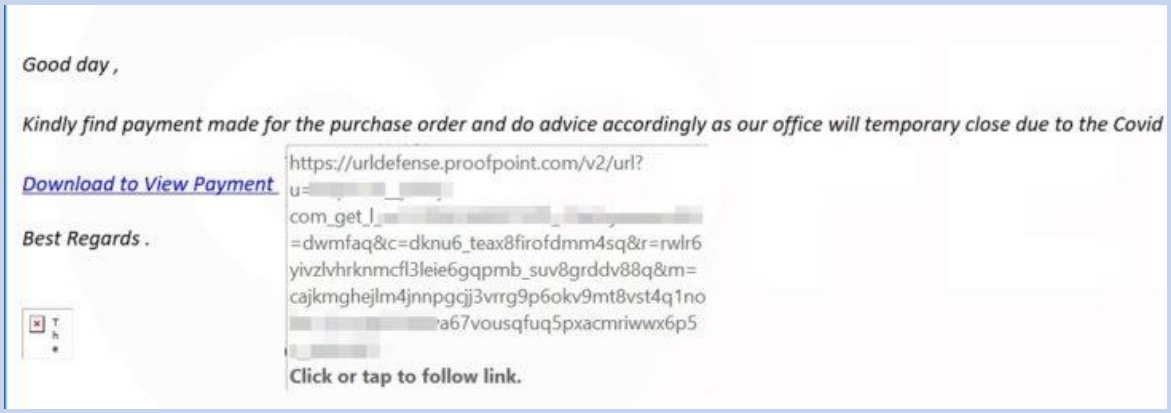
Click or tap to follow link.

Phishing e-mail waarin een crimineel zich voordoet als de IT-Service desk en probeert je op een kwaadaardige link te laten klikken (www.coronavirusphishing.com)

2. Externe contacten

Criminelen kunnen zich ook voordoen als iemand buiten het bedrijf om medewerkers te overtuigen in te gaan op phishing pogingen. Zo kan er een verzoek komen om een rekening (op een andere manier) te betalen omdat een bedrijf zal gaan sluiten (zie voorbeeld 3). Of er wordt gevraagd om hulp vanuit onverwachte hoek, bijvoorbeeld met het verzoek om mondkapjes te leveren.

Voorbeeld 3: Verzoek om rekeningen te betalen



Good day ,

Kindly find payment made for the purchase order and do advice accordingly as our office will temporary close due to the Covid

Download to View Payment

https://urldefense.proofpoint.com/v2/url?
u=[redacted]
com_get_l_[redacted]
=dwmfaq&c=dknu6_teax8firofdmm4sq&r=rwlr6
yivzlvhrknmcfl3leie6gqpmb_suv8grddv88q&m=
cajkmghejlm4jnnpgcjj3vrrg9p6okv9mt8vst4q1no
[redacted]a67vousqfuq5pxacmriwwx6p5
[redacted]

Best Regards .

Click or tap to follow link.

Phishing e-mail waarin wordt gevraagd om snel een rekening te betalen omdat het bedrijf gaat sluiten. (www.coronavirusphishing.com)

3. Autoriteiten

We zien internationaal veel e-mails waarin een crimineel zich voordoet als een autoriteit, bijvoorbeeld als de World Health Organisation (WHO) of het RIVM. In Nederland is de naam van het Ministerie van Sociale Zaken onlangs nog misbruikt door criminelen om een grootschalige phishing aanval uit te voeren (zie voorbeeld 4). In deze campagne werden bedrijven gewaarschuwd voor een sanctie omdat zij zich niet aan de nieuwe maatregelen zouden houden. Dat hier wordt ingespeeld op de snel veranderende wet- en regelgeving, laat duidelijk de relatie tussen de actualiteiten en phishing activiteiten zien.

Voorbeeld 4: Bericht van een autoriteit

een mogelijk onderzoek

Inspectie SZW
Ministerie van Sociale Zaken en Werkgelegenheid

Klachtnummer: 738467
12:20

Dit is een officiële kennisgeving met betrekking tot een mogelijk onderzoek (**Inspectie SZW**).

Wij hebben een klacht ontvangen tegen uw bedrijf met betrekking tot mogelijke inbreuken.

De belangrijkste reden die in de klacht wordt omschreven is het feit dat uw bedrijf in deze periode niet in staat is zich aan te passen en de huidige wetgeving te respecteren.

Wij zullen ons onderzoek aanvatten met het oog op een periode van de afgelopen twee maanden.

De klager zal anoniem blijven tot een eventueel proces begint.

Klik hier om de klacht online te bekijken.

Sancties:

- mogelijke sancties kunnen bestaan uit het opschorten van de activiteit van uw bedrijf;
- een klacht bij de plaatselijke openbare aanklager;

Voor wij verder gaan verwachten wij een antwoord van u. Een telefoongesprek zal ook worden ingepland om de situatie verder te bespreken.

Phishing e-mail waarin bedrijven wordt verteld dat zij zich niet aan de nieuwe maatregelen houden.(https://www.inspectieszw.nl/actueel/nieuws/2020/04/09/let-op-pfishing-mails)

Wat kunnen bedrijven nu extra doen?

In deze tijd zijn er een aantal maatregelen die bedrijven kunnen treffen om covid-19-phishing te voorkomen:

- Wees als bedrijf duidelijk en consistent naar medewerkers in hoe (IT-)veranderingen worden gecommuniceerd. Gebruik geen massa e-mails, maar in plaats daarvan het intranet. Dit leert medewerkers om alleen officiële aankondigingen op het intranet te volgen en niet te klikken op e-mails van een gefingeerde 'IT-afdeling'.
- Update kwetsbare eigen websites en controleer verouderde configuraties, want cybercriminelen misbruiken fout geconfigureerde of slecht onderhouden websites om een phishing website op te zetten.
- Er zijn publieke initiatieven die covid-19-blacklists publiceren, deze kunnen worden gebruikt om de blacklists van jouw bedrijf te updaten, bijvoorbeeld met de informatie van de Cyber Threat Coalition[2]. Dergelijke blacklists voorkomen dat medewerkers terecht komen op deze malafide websites.
- Als bedrijf kun je voorkomen dat cybercriminelen uit jouw naam phishing e-mails sturen (naar klanten, andere bedrijven of eigen medewerkers) door email authenticatie in te schakelen en gebruik te maken van SPF, DKIM en DMARC. Kijk voor meer informatie hierover op de website van het NCSC[3] en test je huidige instellingen op https://www.internet.nl.

Wat kunnen medewerkers nu extra doen?

Er is een duidelijke connectie tussen covid-19-phishing en de snel veranderende samenleving. Ter illustratie; wanneer de overheid extra maatregelen of versoepelingen aankondigt, zijn de bedrijven die deze maatregelen aangaan een extra aantrekkelijk doelwit zijn voor cybercriminelen. Wees hier waakzaam op. Nog een aantal tips:

- Wees je ervan bewust dat bedrijven en instanties een standaard manier van communiceren hebben. Een afwijking hiervan zou kunnen duiden op phishing:
  - Als het goed is zal jouw werkgever altijd communiceren via intranet of ander vast kanaal.
  - De overheid communiceert niet over maatregelen middels een persoonlijke of bedrijfs-email. Zij gebruikt hiervoor altijd persconferenties of publicaties op de eigen website.
  - Ongevraagde e-mails met bijvoorbeeld covid-19-overzichtskaarten zullen nooit worden verspreid door officiële instanties zoals de overheid of zorginstanties. Deze worden gedeeld op de eigen website, naast een persbericht of officiële aankondiging.
- Als je een email ontvangt van iemand die om hulp, samenwerking of geld vraagt, bedenk je dan:
  - Of je de bron hiervan kent en vertrouwt.
  - Of je bewijs kan vinden dat het geld op de juiste plek terecht komt.
  - Of het een logisch verzoek is (bijvoorbeeld; als er een tekort is aan mondkapjes, waarom zou iemand jouw bedrijf opeens mondkapjes aanbieden?).
- Klik nooit zomaar op een link in een e-mail. Je kunt met je muis over de link schuiven om te kijken waar deze naar verwijst, zoals in het voorbeeld van de email van IT-servicedesk. Je kan ook altijd de link checken op https://www.checkjelinkje.nl
- Let extra goed op als een email een gevoel van urgentie of angst opwekt.

Kijk voor meer informatie over hoe je een phishing email in het algemeen kunt herkennen op de DTC website[4].

[2] http://www.cyberthreatcoalition.org/
[3] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing
[4] https://digitaltrustcenter.nl/hoe-herken-ik-een-phishing-e-mail

Contactgegevens

Egmond, M.A.N.E. van (Marie Beth)
marie_beth.vanegmond@tno.nl

Kolk, J.F. van der (Jacco)
J.F.vanderKolk@minezk.nl