Leah Thys en Thomas Vanderveken lenen gezicht aan phishingcampagne. Of toch niet?

Campagne van Febelfin, 2dehands, het Centrum voor Cybersecurity België, de Cyber Security Coalition, de federale politie en de FOD Financiën speelt in op onveiligheidsgevoel en stijging phishingmails door coronacrisis

IN HET KORT:

- Ongeveer 20% van de phishingmails spelen momenteel in op het coronavirus.
- Uit een bevraging van Indiville in opdracht van Febelfin blijkt dat:
    - het onveiligheidsgevoel online toeneemt;
    - meer dan één op drie Belgen de laatste maand een phishingbericht heeft ontvangen. Bij de 35- tot 49-jarigen is dat zelfs de helft;
    - één op vier spijt heeft van informatie die hij online heeft doorgegeven;
    - de 18- tot 34-jarigen het minst voorzichtig zijn online.
- Bedrijven blijven niet gespaard. Medewerkers uit de departementen management, financiën en sales klikken het vaakst door op phishingmails.
- Dit is een campagne van Febelfin in samenwerking met 2dehands, het Centrum voor Cybersecurity België, de Cyber Security Coalition, de federale politie en de FOD Financiën. Met deze nieuwste phishingcampagne willen ze sensibiliseren om nooit persoonlijke bankcodes te delen via een link. Een bank of een ander betrouwbaar bedrijf vraagt dat nooit.
- Vier bekende Belgen “lenen” hun gezicht aan de campagne dankzij deepfaketechnologie.
- Alle informatie over phishing is terug te vinden op het nieuwe platform www.beschermjezelfonline.be.

Door de coronacrisis hebben mensen heel wat zorgen aan hun hoofd. 1,3 miljoen Belgen zitten thuis in een systeem van tijdelijke werkloosheid. Voor veel anderen is thuiswerk – gecombineerd met de zorg en het onderwijs van de kinderen – het nieuwe normaal. Mensen zijn bezorgd over de gezondheid van familie en vrienden. En dan zijn er nog eventuele financiële zorgen. Fraudeurs profiteren daar volop van. Een phishingmail krijgen, gauw doornemen en op de link klikken, is – nu meer dan ooit – snel gebeurd.

Fraudeurs spelen bovendien gretig in op de actualiteit. Het hoeft dan ook niet te verwonderen dat Google momenteel wereldwijd per dag 18 miljoen phishing- en malwaremails detecteert over corona. Met andere woorden: ongeveer 20% van alle phishingmails zinspeelt op het coronavirus.

Miguel De Bruycker, directeur van het Centrum voor Cybersecurity België: “Cybercriminelen spelen in op de actualiteit en weten welke thema's ons interesseren. Wees daarom steeds op je hoede wanneer je verdachte berichten krijgt met links over een actueel onderwerp.”

Vandaag zijn we met z’n allen ook digitaler dan ooit. Doordat veel winkels gesloten zijn, bestellen mensen vaker online. Ook als het om bankieren gaat, wordt er aangeraden voor

digitaal te kiezen. Wie vandaag pas de stap zet naar het digitale leven dat we momenteel aanhouden, is mogelijks een stuk gevoeliger voor de phishingpogingen van fraudeurs.

Bevraging Indiville & Febelfin: online onveiligheidsgevoel neemt toe

In een bevraging van onderzoeksbureau Indiville in opdracht van Febelfin (afgenomen tussen 7 en 10 april bij 1.183 respondenten, foutenmarge 2,3%) geven Belgen aan dat ze effectief meer zaken online regelen (64% van de respondenten) en een aanzienlijke groep zegt ook vaker digitaal bankieren (35%) dan voor de coronacrisis.

Vier op tien Belgen voelen zich online minder veilig sinds het uitbreken van corona.

39% verklaart afgelopen maand een phishingbericht te hebben ontvangen. Bij de 35- tot 49-jarigen loopt dat op tot 48%.

Het bewustzijn dat fraudeurs op het internet erop uit zijn om ons geld te stelen is groot (97% van de respondenten is zich daarvan bewust).

95% noemt zichzelf voorzichtig om niet ten prooi te vallen aan cybercriminelen. 39% van de respondenten doet zelfs extra inspanningen om het online veilig te houden.

Zijn deze cijfers realistisch? Professor Tim Smits van het Instituut voor Mediastudies (KU Leuven) formuleert zijn visie: “Een eerste kanttekening bij de cijfers uit deze bevraging is dat het hier uitsluitend om perceptie gaat. Wat mensen zelf denken over hun gedrag, klopt niet noodzakelijk met de werkelijkheid. Uit onderzoek weten we dat mensen zich vaak slimmer voelen dan anderen. De kans dat mensen in werkelijkheid minder voorzichtig en alert zijn voor phishing is reëel. In dat opzicht is het opvallend dat één op de vier Belgen al eens online gegevens heeft doorgegeven waar hij of zij zich achteraf ongemakkelijk over voelde. Dat geeft stof tot nadenken.”

Uit de bevraging blijkt effectief dat 23% van de Belgen ooit informatie online heeft doorgegeven waar hij of zij zich achteraf ongemakkelijk over voelde. Dat is een verontrustend hoog aantal, zeker omdat we merken dat deze groep meer risico blijft lopen op phishing én niet geneigd lijkt om zijn of haar gedrag aan te passen:

- Deze groep zegt vaker phishingberichten te ontvangen
  en
- Deze groep gaat ook meer dan dubbel zo vaak in op een phishingbericht (7% in plaats van 3%).

Bevraging Indiville & Febelfin: onvoorzichtigheid het grootst onder 18- tot 34-jarigen

Opvallend in de cijfers is ook de relatieve onbezorgdheid van een aantal 18- tot 34-jarigen. 9% van die leeftijdscategorie geeft aan niet voorzichtig genoeg te zijn om uit de handen te blijven van cybercriminelen. Het is ook de leeftijdsgroep die de laatste weken de minste inspanningen heeft gedaan om online veilig te zijn (27% tegenover het gemiddelde van 39%).

Fraudeurs worden steeds professioneler

Wat het de mensen natuurlijk niet gemakkelijker maakt: de tijd dat phishingberichten in een oogopslag te herkennen waren en vol taalfouten stonden, ligt achter ons. Ook Tim Smits merkt een toenemende professionalisering van phishingboodschappen. “Cybercriminelen leveren goede imitaties van effectieve bedrijfscommunicatie. De onderwerpsregels van hun berichten mikken op relevantie en maken mensen nieuwsgierig. De fraudeurs geven zich uit voor officiële instellingen zoals banken of ze slaan juist een heel vertrouwelijke toon aan zoals je van collega’s zou verwachten.”

Dat laatste is niet zonder belang want er belanden ook heel wat phishingmails in de mailboxen van werknemers. Dat weten ze ook bij Phished, een bedrijf dat gespecialiseerd is in phishing en social engineering. Phished helpt bedrijven door hun medewerkers te leren phishingaanvallen te herkennen.

Dit zijn volgens Phished de onderwerpregels van phishingberichten waarop in tijden van corona het vaakst wordt geklikt:

- IT: Hoe verbinden met hoofdkantoor.
- Microsoft: X heeft een bestand met u gedeeld.
- Office 365: Your administrator has updated your account.
- Uw pakje is onderweg!

Tijdens de coronacrisis blijken sommige afdelingen van een bedrijf makkelijker in de phishingval te lopen dan gebruikelijk, zegt COO Arnout Van de Meulebroucke van Phished. “Terwijl anders algemene kantoormedewerkers het vaakst ingaan op phishingberichten (22,9%), gevolgd door Sales (20,81%) en Finance (19,4%) ziet de top-3 van doorklikkende diensten er in coronatijden anders uit, met Finance (29,43%) op één, Sales (27,03%) op twee en Management (24,59%) op drie.”

Phishing herkennen doe je zo…

Aan de taalfouten herken je een phishingbericht dus vaak niet meer en ook (de onderwerpregel van) het bericht klinkt vaak plausibel. Hoe moet je dan phishing wel herkennen?

Wel, 1 ding hebben alle phishingberichten gemeen: ze vragen naar je persoonlijke bankcodes (meestal je codes om te internetbankieren) via een link.

Ontvang je zo’n bericht, dan moet er meteen een lichtje gaan branden: dit is vals! Je bank vraagt je nooit naar je codes via een link. Niet voor een veiligheidsupdate, niet om je bankkaart te vernieuwen of te (de)blokkeren, … Ook andere betrouwbare bedrijven en organisaties zullen dat nooit doen.

Dat is meteen ook het centrale idee van de nieuwste phishingcampagne van Febelfin die vandaag gelanceerd wordt.

“Phishingpogingen gaan het hele jaar door en het is typerend dat fraudeurs zich telkens weer aanpassen aan de omstandigheden,” zegt Karel Baert, CEO van Febelfin. “We merken

ook dat de mails, sms'en en andere berichten steeds professioneler ogen en dat het moeilijker wordt om fake van echt te onderscheiden. Daarom focussen we ons in deze campagne niet op hoe je fake berichten kunt onderscheiden. Onze boodschap is: wees alert voor vreemd gedrag. Je bank zal je nooit vragen om je persoonlijke codes door te geven. Doe het dus ook nooit."

Nieuwe awarenesscampagne over phishing gebruikt deepfake

4 bekende Belgen "leenden" hun gezicht aan de phishingcampagne. Aan Nederlandstalige zijde zijn dat Leah Thys (Marianne van Thuis) en Thomas Vanderveken. Aan Franstalige zijde Julie Taton en Christophe Deborsu.

Het woord "lenen" is op zijn plaats want de vier hebben geen moment zelf op onze shootingset gestaan. Febelfin deed daarvoor een beroep op deepfaketechnologie waarbij menselijke beelden samengesteld worden op basis van artificiële intelligentie. Met andere woorden: we plakten de hoofden van onze vier hoofdspelers op het lichaam van een nobele onbekende. Het resultaat is dan ook compleet fake, net zoals de vraag van een bank om je codes te delen via een link.

De campagne zal via filmpjes en bannering te zien zijn op alle digitale dragers van de financiële sector (Febelfin en de banken): websites, mobiele apps, ATM's, digitale schermen in kantoren, social-mediakanalen, e-newsletters, …

Vanaf vandaag 4 mei loopt de campagne ook als een boodschap van algemeen nut op de TV-kanalen van VRT en RTL.

Leah Thys: "Het filmpje is zo goed gemaakt dat de mogelijkheid van twijfel nog bestaat. En dat is net wat waar deze campagne mensen voor wilt waarschuwen: je kan online onware dingen heel echt laten lijken. Dus als je een klein vermoeden hebt dat iets niet echt is, ga er dan vooral niet op in. Ik ben echt gedegouteerd dat criminelen ook in deze moeilijke tijden nog altijd nieuwe manieren vinden om mensen van hun centjes te beroven. Iets nemen dat van jou is, dat doe je niet."

Thomas Vanderveken: "Tja, ik weet natuurlijk dat ik het niet ben in de video van Febelfin maar ik kan me heel hard voorstellen dat mensen zich laten vangen. Het is een dubbel gevoel: in tijden van corona worden we eraan herinnerd hoe fantastisch technologie is. Door onze apps kunnen we alle bankverrichtingen doen en online kopen. Dat is een grote luxe. Tegelijk moet je altijd heel alert blijven en het onderscheid blijven maken tussen wat aannemelijk is en wat niet. Eén ding weet ik zeker: mijn bank zal me nooit mijn codes vragen via de telefoon, per mail, sms of hoe dan ook."

De campagne van Febelfin geniet de steun van heel wat bedrijven en van de overheid, onder meer via het Centrum voor Cybersecurity België, de Cyber Security Coalition, de federale politie en de FOD Financiën. Allen zullen zij via hun eigen kanalen de campagne mee uitdragen.

2dehands is partner van de campagne en sensibiliseert mee met een eigen boodschap

Aleksandra Vidanovski, woordvoerster van 2dehands: “Cybercriminelen zijn vindingrijk en creatief. Toen de coronacrisis uitbrak, waren we er daarom al snel bij om alle zoekertjes van mondmaskers en desinfecterende handgels van ons platform te bannen. Niet alleen omdat we het afkeuren dat er in veel gevallen woekerprijzen werden aangerekend voor deze schaarse producten, maar ook omdat we weten dat dit net de producten zijn die misbruikt worden voor frauduleuze of fictieve zoekertjes.”

Ook blijft 2dehands verder werken aan tools om het platform nog veiliger te maken en om fraudeurs te weren.

“Toch blijft het informeren en sensibiliseren van onze bezoekers de belangrijkste tool. Zo roepen we op om steeds voorzichtig en waakzaam te zijn. De manier van werken van fraudeurs is namelijk veelal dezelfde: ze proberen je weg te leiden van ons platform en vragen je om je bankgegevens achter te laten op een valse betaalsite of een valse site van een koerierbedrijf die er vaak betrouwbaar uitziet. Eens je bent ‘ingelogd’, gaan de oplichters met je centen aan de haal. Daarom raden we aan om nooit een betaling uit te voeren via een site die je gewoonlijk niet gebruikt. Ook zijn we hard aan het werk om binnenkort tools te kunnen aanbieden waardoor gebruikers tijdens het hele verkoop- of aankoopproces op ons platform kunnen blijven,” besluit Aleksandra Vidanovski.

2dehands verzamelde alle tips om gebruikers veilig te laten handelen op deze pagina: https://www.2dehands.be/i/veilig-handelen/.

Slachtoffer vertelt over phishingervaring: “Mijn rekening werd helemaal leeggehaald”

Inge (45) werd onlangs het slachtoffer van phishing. Ze herinnert zich nog precies hoe de fraude in zijn werk ging. “Het was in het begin van de lockdown, op zondag 22 maart rond de middag. Ik was met van alles tegelijk bezig: eten maken, de tafel dekken, mijn zoon had me nodig, ... Net op dat moment ontving ik een sms van een onbekend gsm-nummer. Het bericht meldde dat mijn bankkaart op dat moment werd gebruikt om in te loggen in de app van mijn bank. Als ik het niet was, moest ik onmiddellijk de verdachte handeling verifiëren via een link in de sms. Pas achteraf besefte ik dat allerlei dingen niet klopten: dat ik mijn kaart gewoon bij me had, dat mijn bank me nooit op die manier zou benaderen en dat de domeinnaam achter de link verdacht was. Maar op het moment zelf klikte ik op de link, kwam ik terecht op een goed nagebouwde site van mijn bank en logde ik in met mijn kaartlezer. Ik kreeg een foutmelding, ontving een nieuwe sms en logde nogmaals in.”

Inge ging verder met haar eten en checkte even daarna haar rekening via de app van haar bank. “Ik schrok met rot. Er was twee keer 2.000 euro verdwenen via overschrijving en vervolgens nog eens 500 euro. Op 9 euro na was mijn rekening helemaal leeg.”

Inge deed meteen aangifte bij de politie, blokkeerde haar bankkaart en opende een fraudedossier bij haar bank. “Via de politie heb ik achteraf gehoord ik dat het geld meteen na overschrijving is afgehaald door een zogenaamde muilezel. Dat is dus weg naar een onbekende bestemming. Ik ben een alleenstaande ouder met een beperkt inkomen en het leven is duur. De bank liet me intussen gelukkig weten dat ik vergoed word. Ik vind het

belangrijk dat dit soort fraude onder de aandacht komt, want een paar dagen geleden ontving een vriendin van me exact dezelfde sms. De criminelen hierachter blijven dus gewoon doorgaan."

Alle info over phishing op een rijtje

In de campagne verwijst Febelfin altijd naar het online platform www.beschermjezelfonline.be. Daar vinden mensen alle praktische informatie over phishing terug. Wat is het? Waar moet je op letten? Wat moet je wel of niet doen? En waar kan je terecht als je in de val bent getrapt?

En wat met andere fraudevormen?

Uiteraard spelen fraudeurs niet enkel in op de coronacrisis door phishingmails uit te sturen. Ze proberen mensen via allerlei manieren op te lichten: door mensen hun pc te blokkeren en losgeld te vragen, of simpelweg door hen dingen te verkopen die niet bestaan.

Commissaris Olivier Bogaert van de Federale Politie: "Cybercriminelen spelen gretig in op de ongerustheid over corona. Mensen krijgen bijvoorbeeld fake berichten dat het virus bij een van hun familieleden is vastgesteld. De bedoeling is dat je impulsief klikt op een link die een programma op je computer of smartphone installeert en het toestel onbruikbaar maakt tenzij je losgeld betaalt. Dit is een variatie op de klassieke ransomware waarmee criminelen je computer of smartphone vergrendelen. Bij dergelijke berichten geldt ons standaardadvies: hou het hoofd koel, reageer niet onmiddellijk maar kijk na wat de bron is van het bericht. Zoek bijvoorbeeld de herkomst van het bericht op in de zoekmachine van Google. Omdat dit pogingen tot fraude zijn die internationaal circuleren, is de kans groot dat Google je er al voor kan waarschuwen. We zien ook frauduleuze berichten via mail, sms en sociale media over valse geneesmiddelen, mondmaskers, handschoenen… Zelfs over giften voor ziekenhuizen. Als je op deze aanbiedingen of vragen ingaat, ben je je geld kwijt en deel je privégegevens met fraudeurs. Ons advies: klik niet op verdachte berichten, koop alleen bij vertrouwde (web)shops en ga na of de afzender van een bericht authentiek is voor je erop ingaat."

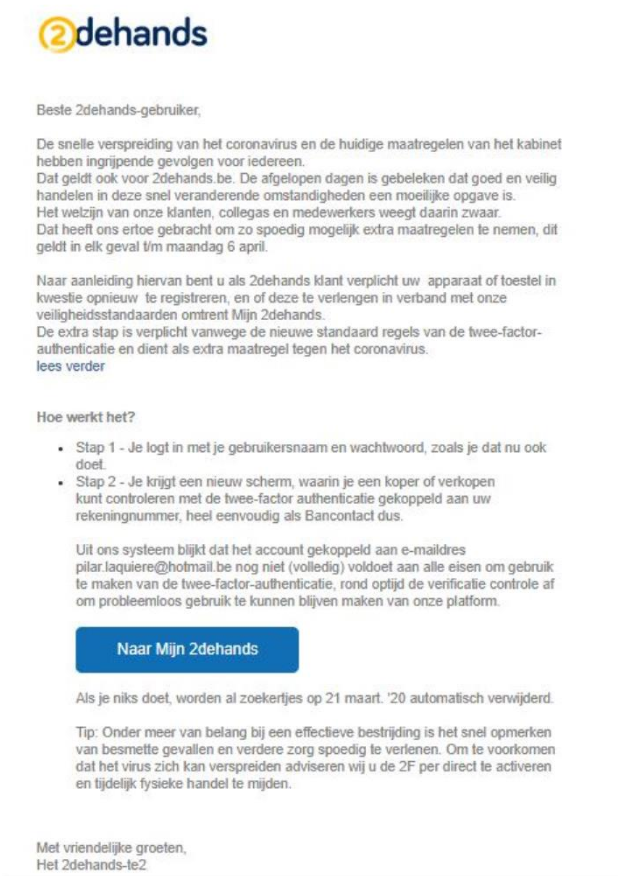
Bijlagen

Video's

De video's kunnen jullie op onderstaande linken terugvinden:

Thomas: https://youtu.be/i-yH_L0GAcE
Christophe: https://youtu.be/dh0J2JxMHwg
Julie: https://youtu.be/mY6-bzb9Tao
Leah: https://youtu.be/auJ3Np-YkXg

Voorbeelden van corona phishing berichten



2dehands

Beste 2dehands-gebruiker,

De snelle verspreiding van het coronavirus en de huidige maatregelen van het kabinet hebben ingrijpende gevolgen voor iedereen.
Dat geldt ook voor 2dehands.be. De afgelopen dagen is gebeleken dat goed en veilig handelen in deze snel veranderende omstandigheden een moeilijke opgave is.
Het welzijn van onze klanten, collegas en medewerkers weegt daarin zwaar.
Dat heeft ons ertoe gebracht om zo spoedig mogelijk extra maatregelen te nemen, dit geldt in elk geval t/m maandag 6 april.

Naar aanleiding hiervan bent u als 2dehands klant verplicht uw apparaat of toestel in kwestie opnieuw te registreren, en of deze te verlengen in verband met onze veiligheidsstandaarden omtrent Mijn 2dehands.
De extra stap is verplicht vanwege de nieuwe standaard regels van de twee-factor-authenticatie en dient als extra maatregel tegen het coronavirus.
lees verder

Hoe werkt het?

- Stap 1 - Je logt in met je gebruikersnaam en wachtwoord, zoals je dat nu ook doet.
- Stap 2 - Je krijgt een nieuw scherm, waarin je een koper of verkopen kunt controleren met de twee-factor authenticatie gekoppeld aan uw rekeningnummer, heel eenvoudig als Bancontact dus.

Uit ons systeem blijkt dat het account gekoppeld aan e-maildres pilar.laquiere@hotmail.be nog niet (volledig) voldoet aan alle eisen om gebruik te maken van de twee-factor-authenticatie, rond optijd de verificatie controle af om probleemloos gebruik te kunnen blijven maken van onze platform.

Naar Mijn 2dehands

Als je niks doet, worden al zoekertjes op 21 maart. '20 automatisch verwijderd.

Tip: Onder meer van belang bij een effectieve bestrijding is het snel opmerken van besmette gevallen en verdere zorg spoedig te verlenen. Om te voorkomen dat het virus zich kan verspreiden adviseren wij u de 2F per direct te activeren en tijdelijk fysieke handel te mijden.

Met vriendelijke groeten,
Het 2dehands-te2

Volledige resultaten onderzoek Phished

Q: Type onderwerp (welke onderwerpen zijn populair?)
A: In een normale, willekeurige periode bestaat de top 10 uit volgende onderwerpregels:

- SharePoint: Your files are being deleted soon.
- Microsoft: {{ SpearPhishingFirstName }} {{ SpearPhishingLastName }} heeft een bestand met u gedeeld.
- Office 365: Your administrator has expired your password.
- Uw pakje is onderweg!
- Reset uw wachtwoord (ter info: LinkedIn)
- LinkedIn: {{ SpearPhishingFirstName }} has invited you
- Er is een nieuw document beschikbaar voor u (ter info: van myworkandme)
- BOETE [#644733573] – Proces verbaal
- Waarom post je dit online??
- Kan jij deze offerte goedkeuren?

Q: Tijdens de coronacrisis, zijn de volgende onderwerpen onze spreekwoordelijke toppers:

- IT: Hoe verbinden met hoofdkantoor.
- Microsoft: {{ SpearPhishingFirstName }} {{ SpearPhishingLastName }} heeft een bestand met u gedeeld.
- Office 365: Your administrator has updated your account.
- Uw pakje is onderweg!
- Uw pakje is vertraagd!
- LinkedIn: {{ SpearPhishingFirstName }} has invited you
- Er is een nieuw document beschikbaar voor u (ter info: van myworkandme)
- BOETE [#644733573] – Proces verbaal
- Corona maatregelen: Update
- Kan jij me dit uitleggen?

Q: Op welk tijdstip van de dag en op welke dag wordt het meest geklikt?
A: Extra informatie vind je in de folder 'tijden', hierin is ook het onderscheid gemaakt tussen een normale situatie en de crisissituatie.
Als we in absolute aantallen spreken, dan is maandag de phishing-dag bij uitstek. Hierop doen vooral spear-phishing mails het goed, wat dus wil zeggen dat ze gerichte mails krijgen van de (zogezegde) baas of collega's.
Het gemiddelde phishing-percentage ligt dan weer hoger op dinsdag. Hierbij zijn de uitschieters die het goed doen mails die met allerhande transacties te maken hebben (denk aan: 'wij hebben uw bestelling ontvangen' of 'uw betaling is gevalideerd'). Daarom doen ook mails van postdiensten zoals PostNL of bpost het goed.

Q: Zijn BE werknemers meer vatbaar voor phishing dan hun collega's in de landen opgesomd in het artikel?
A: De Belgische werknemers zijn inderdaad iets vatbaarder voor phishing tegenover medewerkers in de andere landen. In België is bewustzijn nog veel minder een begrip als in die landen, en hieraan linken we het verschil.

Q: Welke afdelingen binnen het bedrijf zijn meer vatbaar?
Normale periode:

1. Office – 22.90%
   (hiermee bedoelen we algemene kantoormedewerkers)
2. Sales – 20.81%
3. Finance – 19.40%
4. Management – 19.32%

5. Marketing – 16.57%

Coronacrisis:

1. Finance – 29.43%
2. Sales – 27.03%
3. Management – 24.59%
4. HR – 22.56%
5. Operations – 17.86%

Het is opvallend dat net medewerkers uit de finance-afdeling tijdens deze crisis zich meer in de val laten lokken.

Q: Heeft coronacrisis een impact?

A: Over het algemeen blijft de gemiddelde phishing-ratio rond de 20% hangen, zowel in een normale periode als tijdens de Coronacrisis. Het gemiddelde klikgedrag blijft dus ruwweg gelijk. Er is echter wel een duidelijke verschuiving te merken in welke departementen klikken op de simulaties. Je kan hiervan een overzichtje en analyse vinden onder de sub-map “Departementen”.

Echter merken wij wel een verhoging in het aantal phishing-aanvallen, waardoor je dus inderdaad kan zeggen dat er het risico op een destructieve phishing-aanval significant hoger is.
Samengevat: gemiddeld trappen er niet meer medewerkers in dan normaal, maar op wereldwijde schaal schiet het aantal phishing-mails de hoogte in: dus ja er is een impact voelbaar.