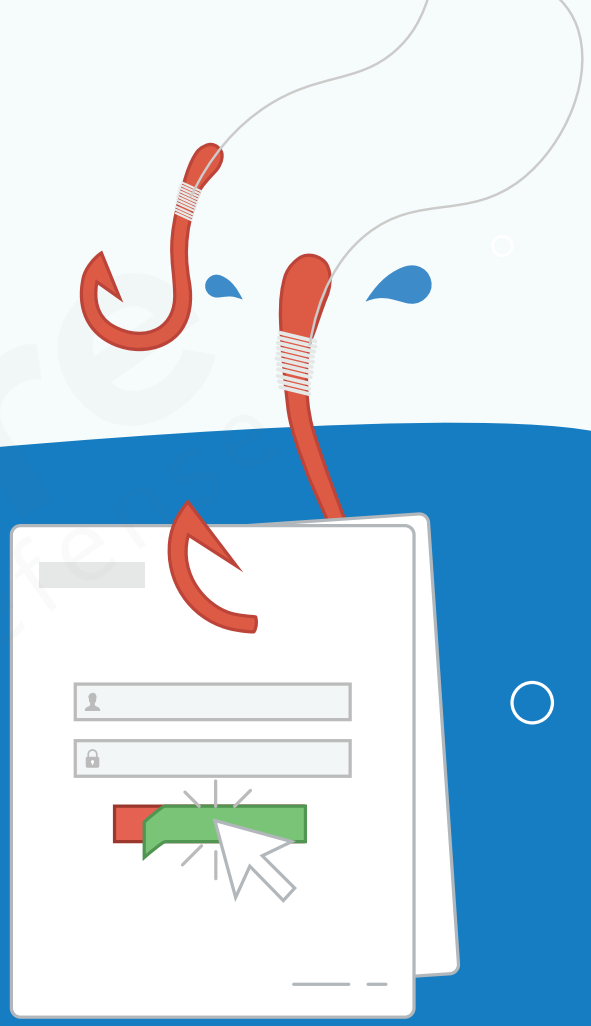
Phishers' favorieten

2020 jaaroverzicht



VadeSecure
Predictive Email Defense

OFFICE~IT

INHOUD

Phishers' favorieten 2020 jaaroverzicht 3

Microsoft blijft meest geïmiteerde merk 3

De 20 meest gebruikte merken voor phishing-aanvallen 4

Phishers' Favorites 2020 20 meest geïmiteerde merken 5

Microsoft 365 blijft het belangrijkste doelwit voor phishing-aanvallen 6

Sociale media blijven op koers 7

Cloud haalt financiële markt in als meest geïmiteerde sector 9

De actuele gebeurtenissen hebben geleid tot trends in phishing-aanvallen 11

Een late zomer deed phishing bij Microsoft explosief toenemen 13

Geavanceerde phishing-aanvallen vereisen een geavanceerde verdediging 16

Over Vade Secure 17

Vade Secure
Predictive Email Defense

PHISHERS' FAVORIETEN 2020 JAAROVERZICHT

Microsoft blijft meest geïmiteerde merk

Phishers' Favorites is het driemaandelijkse rapport van Vade Secure waarin de top 20 van de meest geïmiteerde merken in phishing-aanvallen wordt belicht. In ons jaaroverzicht kijken we naar de top 20 en bespreken we ook de belangrijkste trends binnen phishing. We zien onder meer de aanhoudende dominantie van Microsoft 365 phishing en de opkomst van nieuwe merken op de lijst van Phishers' Favorites.

Elk kwartaal detecteert en analyseert het filtersysteem van Vade Secure tienduizenden unieke phishing-URL's. *Unieke phishing-URL's* verwijzen alleen naar het aantal URL's en niet naar het aantal ontvangen phishingmails. Hackers sturen vaak tientallen, soms honderden of duizenden phishingmails met dezelfde URL.

De 20 meest gebruikte merken voor phishing-aanvallen

Microsoft is voor het derde jaar op rij het meest geïmiteerde merk van 2020. Vade Secure detecteerde 39.621 unieke Microsoft phishing URL's in 2020. Facebook staat op nummer 2 in de lijst, komende van nummer 4 in 2019, met 14.876 unieke phishing-URL's.

De top drie wordt afgerond met PayPal, dat in 2019 op nummer 2 stond. Vade Secure detecteerde 11.841 unieke phishing URL's van PayPal in 2020. Het aantal unieke phishing-URL's is in 2020 gedaald, terwijl het aantal ontdekte phishingmails gelijk is gebleven. De belangrijkste aanvalsdoelen en de toenemende complexiteit bleven ongewijzigd.

39,621
unieke phishing-URL's

Microsoft

14,876
unieke phishing-URL's

facebook

Phishers' Favorites 2020
20 meest geïmiteerde merken

#		Merk	unieke phishing-URL's
1	-	Microsoft Categorie: Cloud	39,621
2	↑2	Facebook Categorie: Sociale media	14,876
3	↓1	PayPal Categorie: Financiële Diensten	11,841
4	↑4	Chase Categorie: Financiële Diensten	8,832
5	↑28	eBay Categorie: E-Commerce/logistiek	6,918
6	-	Rakuten Categorie: E-Commerce/logistiek	6,452
7	↓4	Netflix Categorie: Cloud	6,417
8	↑2	Amazon Categorie: E-Commerce/logistiek	6,063
9	↑5	WhatsApp Categorie: Sociale media	5,322
10	↓1	DHL Categorie: E-Commerce/logistiek	4,403
11	-	Credit Agricole Categorie: Financiële Diensten	4,317
12	↑6	Wells Fargo Categorie: Financiële Diensten	4,265
13	↑3	Adobe Categorie: Cloud	4,171
14	↓9	Bank of America Categorie: Financiële Diensten	4,042
15	↑2	Google Categorie: Cloud	3,317
16	↑8	Comcast Categorie: Internet/Telco	3,297
17	↓11	Apple Categorie: E-Commerce/logistiek	3,131
18	↑22	La Banque Postale Categorie: Financiële Diensten	2,932
19	↑9	LinkedIn Categorie: Sociale media	2,548
20	↓8	Dropbox Categorie: Cloud	2,427

Vade Secure
Predictive Email Defense

Microsoft 365 blijft het belangrijkste doelwit voor phishing-aanvallen

Het gebruikersbestand van Microsoft 365 is in 2020 gegroeid tot 258 miljoen. Dit cijfer ligt hoger dan verwacht en geeft een verdere marktdominantie weer op vlak van zakelijke productiviteitssoftware. Deze groei werd voor een groot deel aangedreven door de COVID-19 pandemie die begin 2020 de wereld overspoelde. Microsoft zag met 75 miljoen actieve gebruikers van Microsoft Teams in april 2020 een forse stijging ten opzichte van 44 miljoen in maart 2020.

Microsoft staat al zeven kwartalen bovenaan de lijst van onze Phishers' Favorites kwartaalrapporten. Met een aandeel van meer dan 90 procent in de e-mailmarkt en de auteursmarkt bevat het pakket applicaties van Microsoft 365 een rijke bron van gegevens voor cybercriminelen om te exploiteren.

De phishing-aanvallen variëren van gewone wachtwoordresets en waarschuwingen tot meer gepersonaliseerde e-mails waarin gebruikers worden gevraagd om OneDrive- en SharePoint-bestanden te openen. Zoals we verder in dit e-book zullen zien, doen veel Microsoft phishingmails zich helemaal niet voor als Microsoft. Deze e-mails doen zich voor als een ander bedrijf en bevatten links naar Microsoft 365 phishingpagina's, waarbij misbruik wordt gemaakt van het vertrouwen van gebruikers in het merk Microsoft.

Microsoft 365

258 miljoen
actieve gebruikers

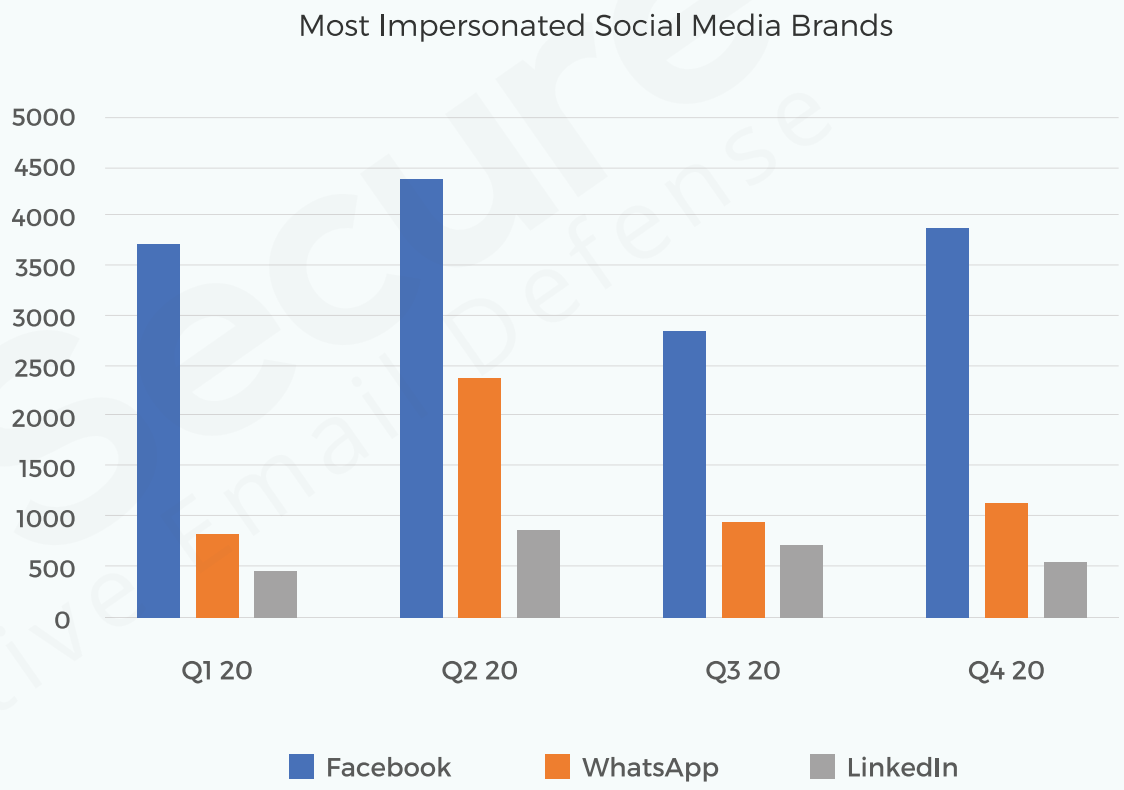
1 miljoen
zakelijke klanten

90%
marktaandeel voor e-mail

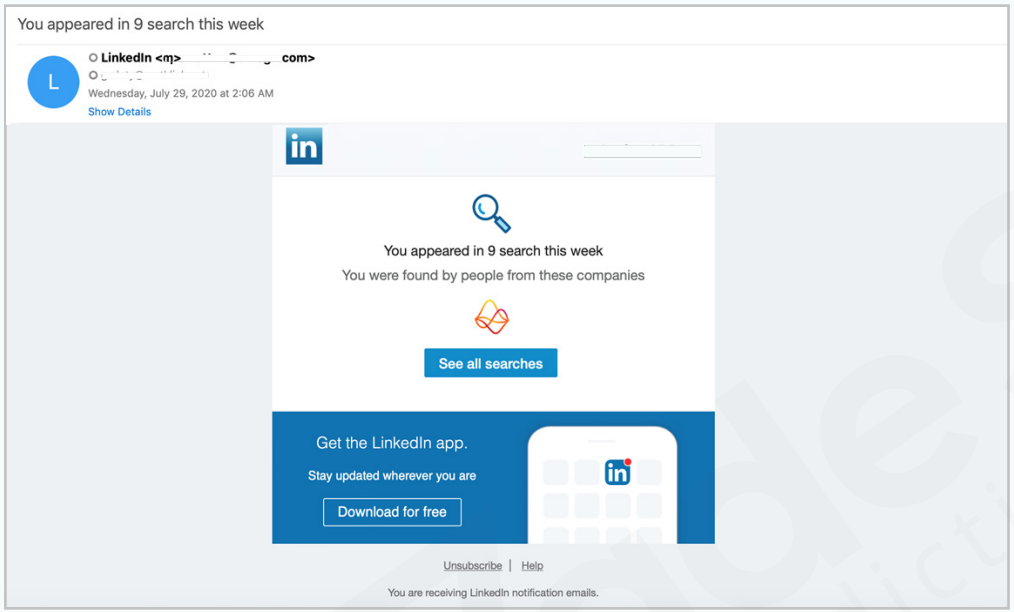
Sociale media blijven op koers

Vade Secure is in 2018 gestart met het monitoren van unieke Facebook-URL's. Sindsdien zagen ze het aantal aanvallen steeds verder toenemen met een eerste grote piek in het tweede kwartaal van 2019, waar het aantal unieke phishing URL's van Facebook met meer dan 155 procent de hoogte in ging. Dit niveau bleef min of meer stabiel doorheen 2020. Enkel in het tweede kwartaal was er een toename merkbaar met 4.373 ontdekte unieke URL's op een totaal van 14.876 voor het hele jaar.

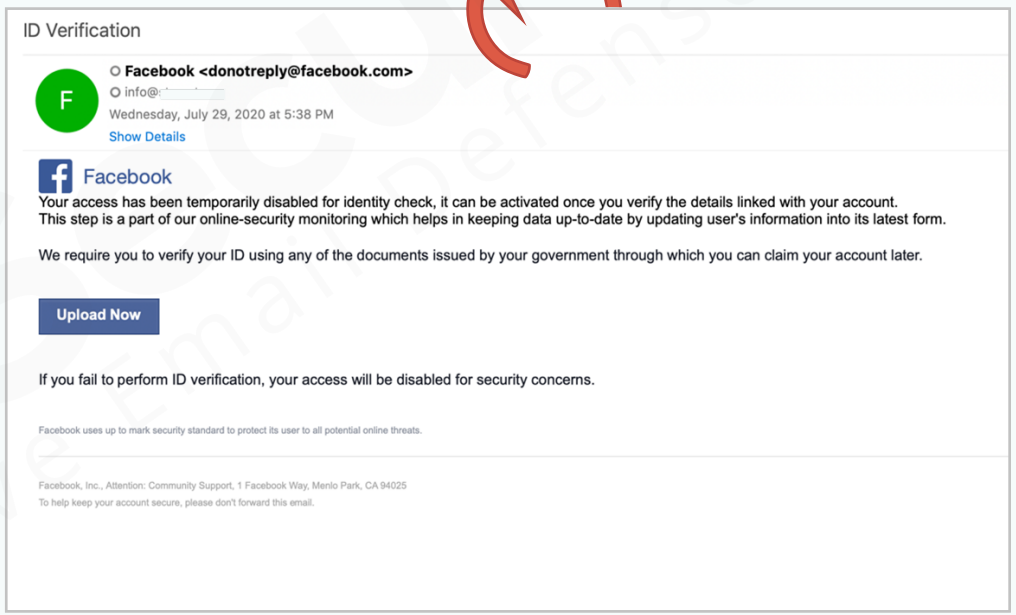
WhatsApp verscheen in het eerste kwartaal van 2019 voor het eerst op de lijst met favorieten van phishers, met een klein aantal gedetecteerde phishing-URL's. Dat veranderde drastisch in het vierde kwartaal van 2019, toen Vade Secure 5.029 unieke WhatsApp phishing URL's ontdekte. WhatsApp deed het terug wat beter bij de start van 2020, maar de cijfers gingen in het tweede kwartaal fors omhoog. De piek viel samen met de COVID-19 pandemie, toen sociale mediabedrijven in het algemeen een toename van phishing kenden.



Facebook en WhatsApp tellen samen 4,7 miljard gebruikers. Ze staan bovenaan de lijst van meest geïmiteerde sociale mediamerken. En ook al beschikken ze niet over bankrekening- en kredietkaartnummers van grote banken of financiële instellingen, ze hebben wel een schat aan persoonsgegevens die kunnen worden verzameld, verkocht en geëxploiteerd.



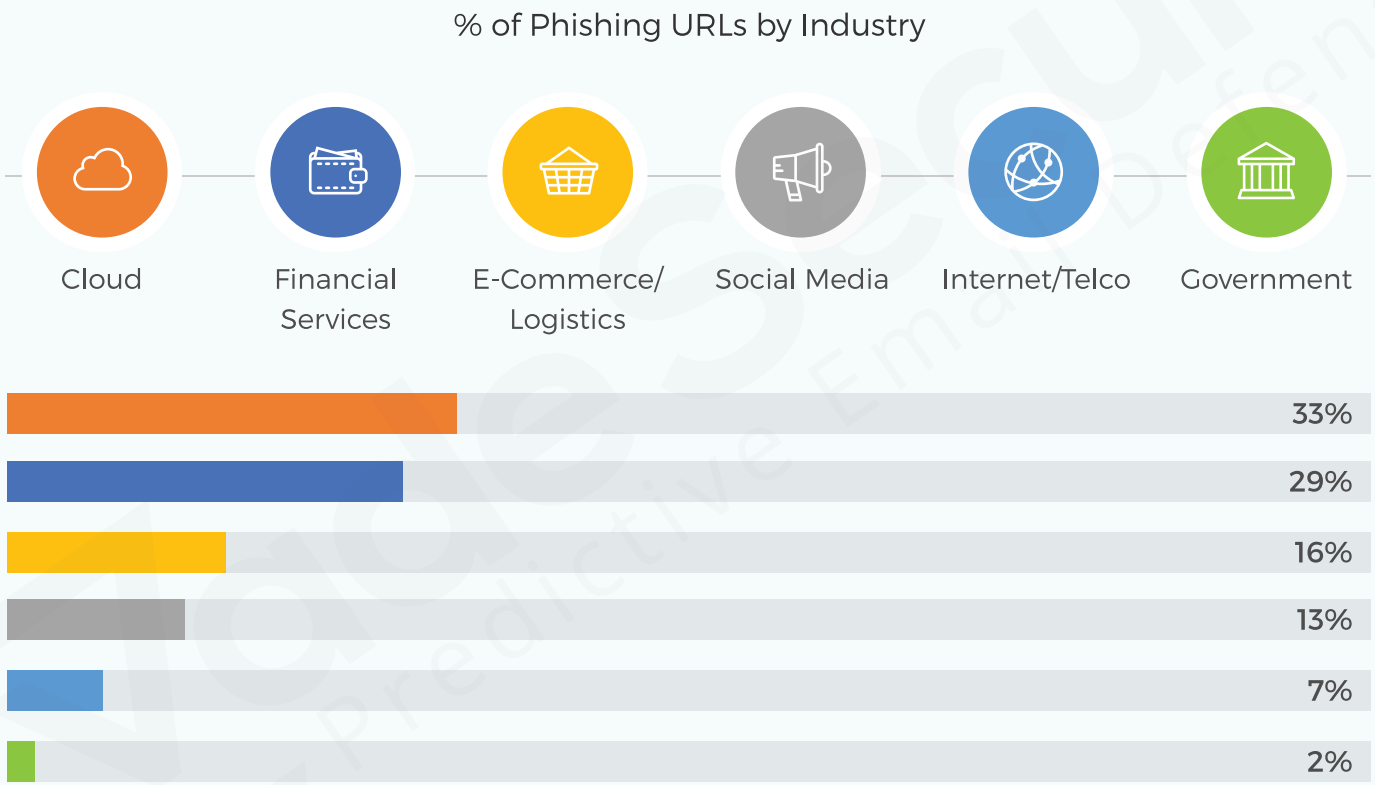
LinkedIn phishing e-mail, juli 2020



Facebook phishing e-mail, juli 2020

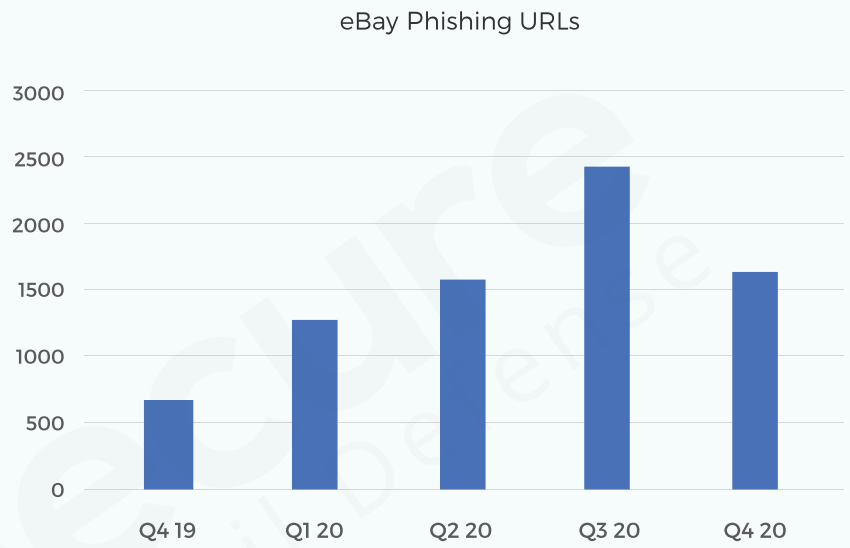
Cloud haalt financiële markt in als meest geïmiteerde sector

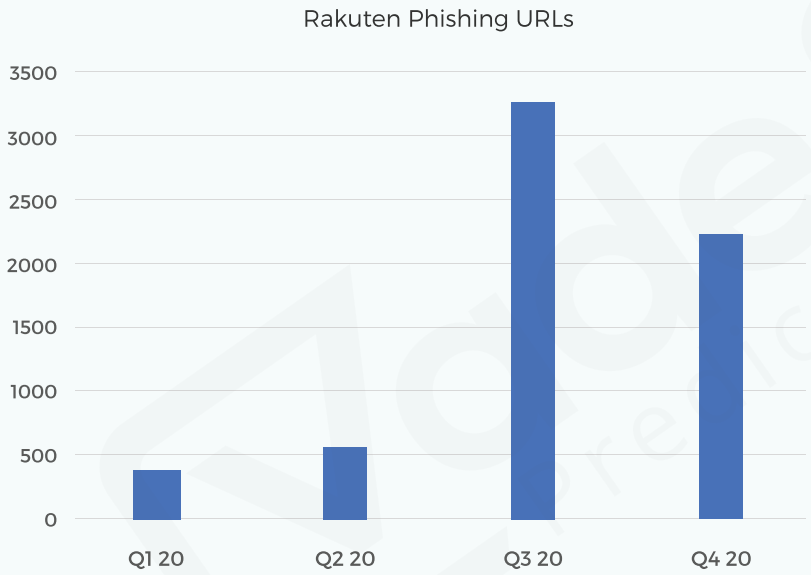
De financiële dienstenleveranciers stonden bij de start van het jaar nog bovenaan met een aandeel van 36,7 procent aan unieke phishing-URL's. PayPal, dat in 2019 op nummer 2 stond, zakte naar de derde plaats. Chase, dat eerst op nummer 8 stond, steeg in 2020 naar de vierde plaats, met 8.832 phishing-URL's. Credit Agricole behield zijn positie op nummer 11 in 2020 met 4.317 phishing-URL's, gevolgd door Wells Fargo, dat zes plaatsen steeg naar nummer 12 met 4.265 phishing-URL's.



In het tweede kwaartaal van 2020 deed er zich een plotse verschuiving voor. Het aantal phishing-aanvallen die zich voordeden als financiële diensten daalde van 37 procent naar 33 procent, terwijl de aanvallen op cloud-dienstverleners toenamen. In het derde kwartaal steeg het percentage cloud phishing naar 40,5 procent, t.o.v. 33 procent in het tweede kwartaal. Cloud bleef in het vizier van de hackers en eindigde met 33 procent van alle unieke phishing-URL's die in 2020 werden gedetecteerd op een onfortuinlijke eerste plaats. Microsoft, Netflix, Adobe, Apple en Dropbox vertegenwoordigden de meest geïmiteerde cloud-dienstverleners in de top 20. Zowel Google als Adobe zagen het aantal phishing-URL's toenemen en stegen respectievelijk twee en drie plaatsen.

Ten opzichte van 2019 heeft e-commerce de sociale media ingehaald als de derde meest geïmiteerde sector. Net als bij clouddiensten bereikte het aantal phishingaanvallen binnen het e-commercesegment nieuwe hoogten in 2020. De stijging is het gevolg van zowel het massaal telewerken als de quarantaine. eBay, dat in 2019 de top 20-lijst niet haalde, sprong 28 plekken omhoog naar nummer 5. De stijging van eBay begon in Q1 met een toename van 89 procent in phishing-URL's ten opzichte van Q4 2019. eBay phishing piekte in Q3 met 2.424 URL's en 143 procent jaar-op-jaar (YoY) groei.



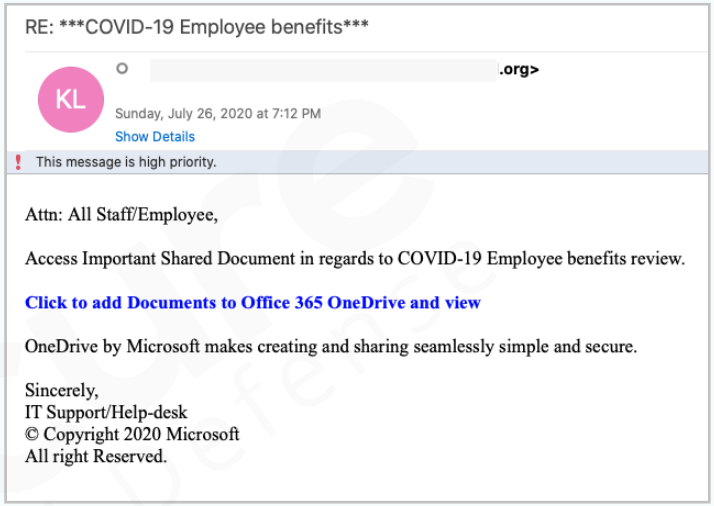


Rakuten, een Japans e-commercebedrijf dat in 1997 werd opgericht, verscheen voor het eerst op de lijst in Q3 2020, toen unieke Rakuten phishing-URL's explodeerden met 485 procent, van 559 URL's in Q2 tot 3.272 URL's in Q3. In het vierde kwartaal werd het rustiger voor Rakuten, waarbij het aantal Rakuten phishing URL's met 32 procent afnam.

De actuele gebeurtenissen hebben geleid tot trends in phishing-aanvallen

De plotse verschuiving van phishing bij financiële diensten naar phishing bij clouddiensten kwam op het moment dat COVID-19 de manier waarop wij over de hele wereld werken veranderde. Het aantal actieve gebruikers van Microsoft Teams is in het derde kwartaal explosief gestegen. De omzet van Amazon Web Services (AWS) is zowel in het tweede als in het derde kwartaal met 29 procent gestegen en de omzet van Google Cloud is in het derde kwartaal met 45 procent gestegen. Rond dezelfde periode bereikte eBay phishing een hoogtepunt en schoot het aantal Rakuten phishingaanvallen ook de hoogte in.

Toen COVID-19 bedrijven ertoe verplichtte over te schakelen op telewerken, gingen cybercriminelen onmiddellijk aan de slag. Dit leidde tot een massale golf van phishing- en spam e-mails met COVID-19 als onderwerp. Inspelend op het angstgevoel varieerden de COVID-19 e-mails van advertenties voor gezichtsmaskers en andere persoonlijke beschermingsmiddelen, tot nep e-mails van personeelszaken waarin de voordelen van COVID-19 werden aangeprezen en zelfs tot phishing e-mails die zich voordeden als gezondheidsorganisaties, waaronder de Wereldgezondheidsorganisatie (WHO) en de nationale gezondheidsdiensten.


RE: ***COVID-19 Employee benefits***

KL .org>

Sunday, July 26, 2020 at 7:12 PM

Show Details

This message is high priority.

Attn: All Staff/Employee,

Access Important Shared Document in regards to COVID-19 Employee benefits review.

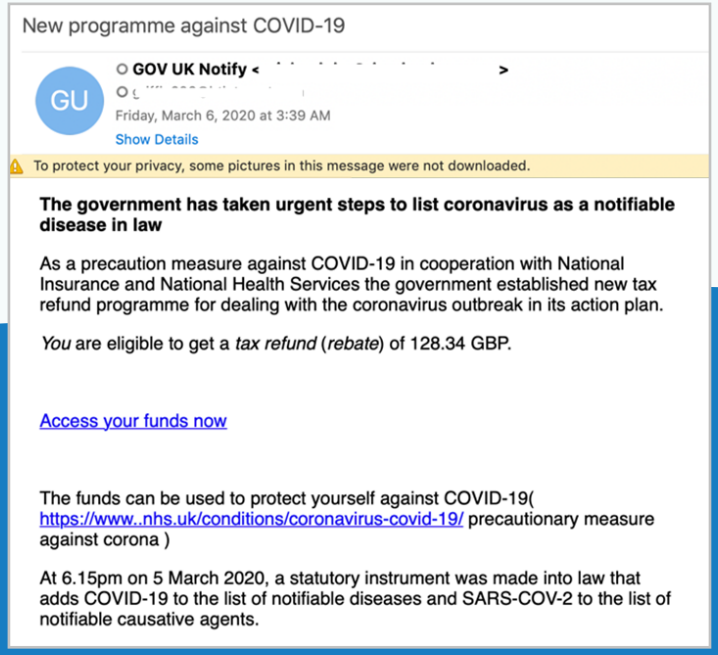
Click to add Documents to Office 365 OneDrive and view

OneDrive by Microsoft makes creating and sharing seamlessly simple and secure.

Sincerely,
IT Support/Help-desk
© Copyright 2020 Microsoft
All right Reserved.

COVID-19 HR phishing e-mail

WHO phishing-pagina


New programme against COVID-19

GU GOV UK Notify <

Friday, March 6, 2020 at 3:39 AM

Show Details

To protect your privacy, some pictures in this message were not downloaded.

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

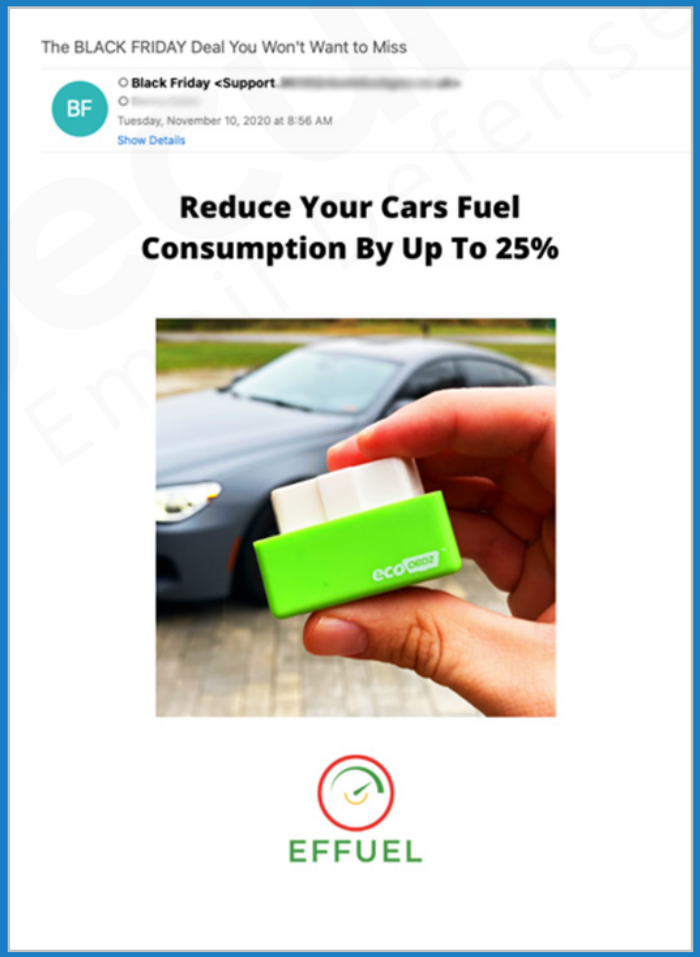
The funds can be used to protect yourself against COVID-19(https://www..nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

COVID-19 phishing e-mail over belastingteruggave

Black Friday is een ander jaarlijks gebeuren dat tot een massale toevloed van kwaadwillende e-mails heeft geleid. In 2020 werd 10 tot 15 procent van de door Vade Secure geanalyseerde e-mails over Black Friday herkend als onveilig. Amazon-spam en phishing e-mails kwamen veel voor tijdens de periode van Black Friday. Black Friday is een wereldwijd initiatief en heeft geleid tot phishingaanvallen, variërend van nep-prijsvragen en -beloningen tot e-mails die in de onderwerpregel inspelen op het enthousiasme van Black Friday, maar een aanbod bevatten dat er niets mee te maken heeft.

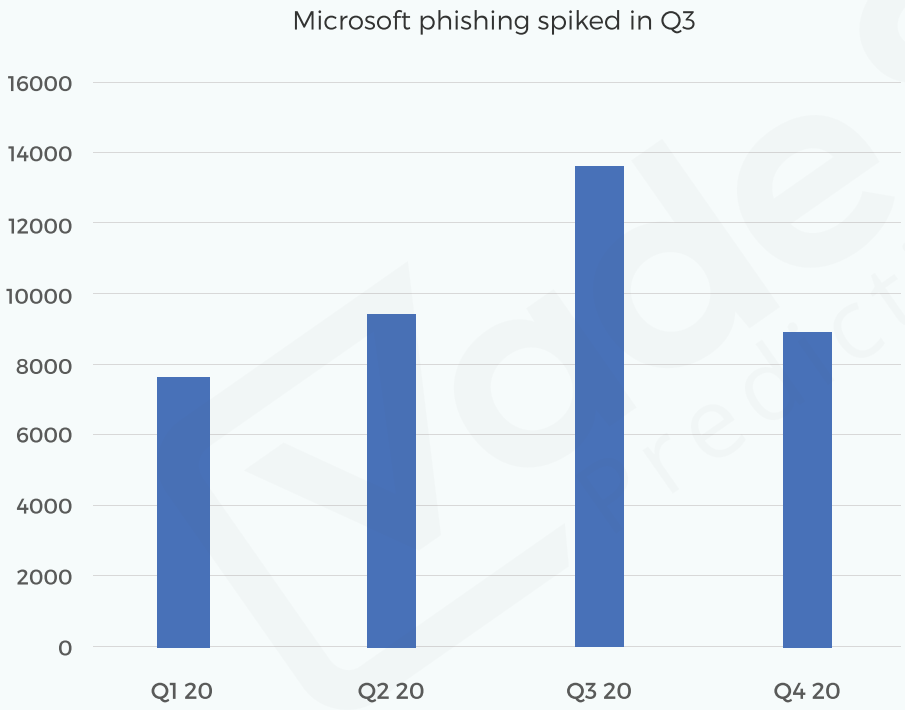
Amazon phishing e-mail (Italiaans)



Effuel spam e-mail

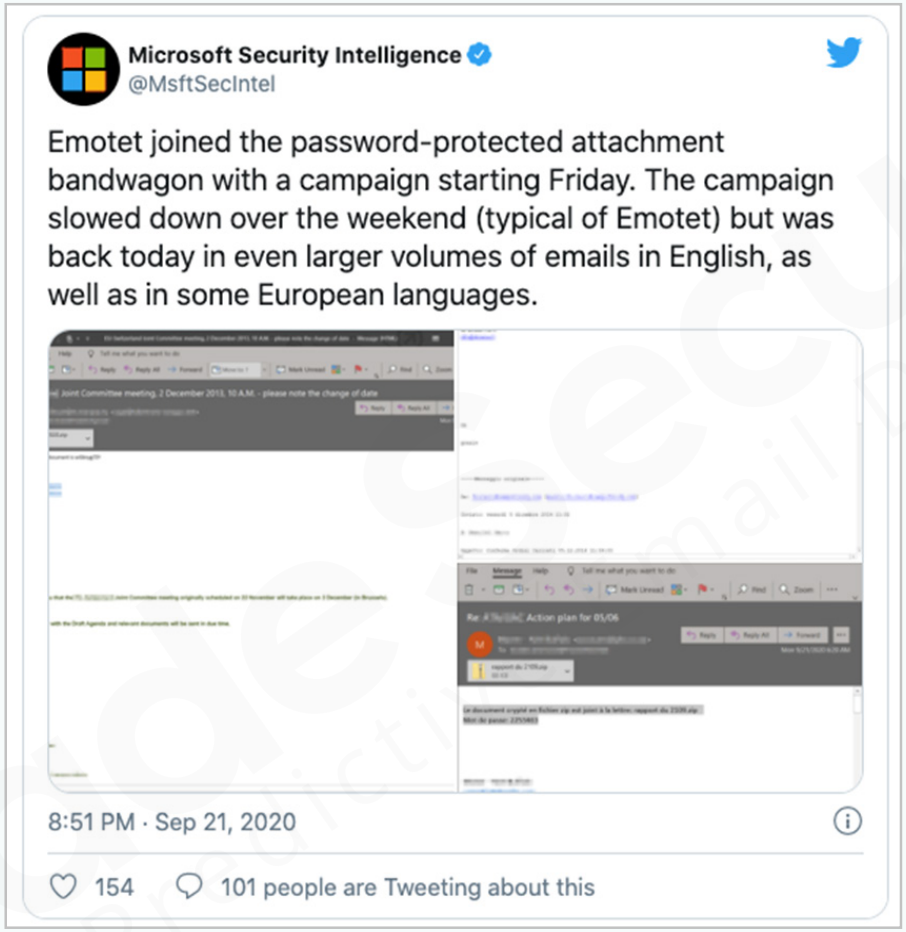
Een late zomer deed phishing bij Microsoft explosief toenemen

Microsoft zag in de eerste helft van het jaar stabiele niveaus van phishing-URL's, met 7.581 URL's in Q1 en 9.410 URL's in Q2. In het begin van het derde kwartaal explodeerde Microsoft phishing tot 13.617 phishing URL's, met een kleine toename van phishing in juli gevolgd door een explosie in augustus en september. Het hoogtepunt van de golf vond plaats op 24 september, toen Vade Secure 1.151 unieke phishing-URL's van Microsoft ontdekte.



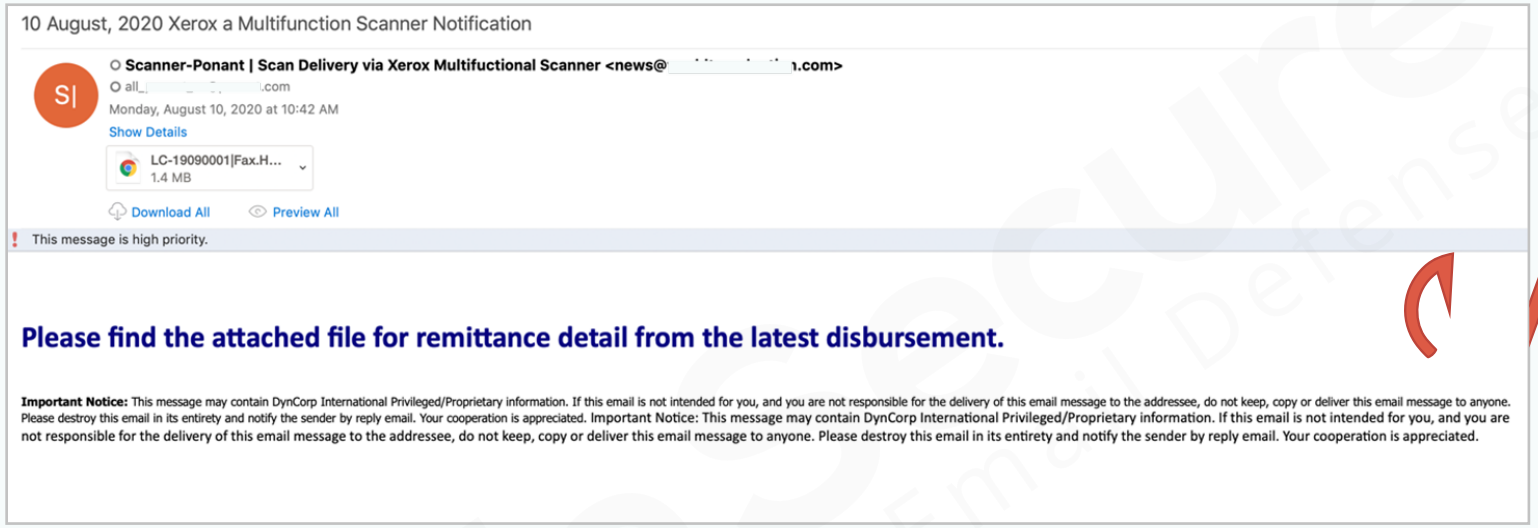
De golf viel samen met een reeks waarschuwingen over Emotet-malware, een botnet dat een voorloper is van malware-aanvallen. De Emotet-hackers hadden maandenlang een pauze ingelast voordat ze in juli weer opdoken, toen Microsoft, samen met organisaties voor cyberbeveiliging in Frankrijk, Japan en Nieuw-Zeeland , haar gebruikers waarschuwde voor Word-documenten met koppelingen en kwaadaardige macro's die Emotet activeren.

Microsoft waarschuwde zijn gebruikers in september opnieuw voor een nieuwe golf, gevolgd door waarschuwingen van beveiligingsorganisaties in Italië en Nederland. De nieuwe golf bevatte ZIP-bestanden met wachtwoordbeveiliging van Emotet.

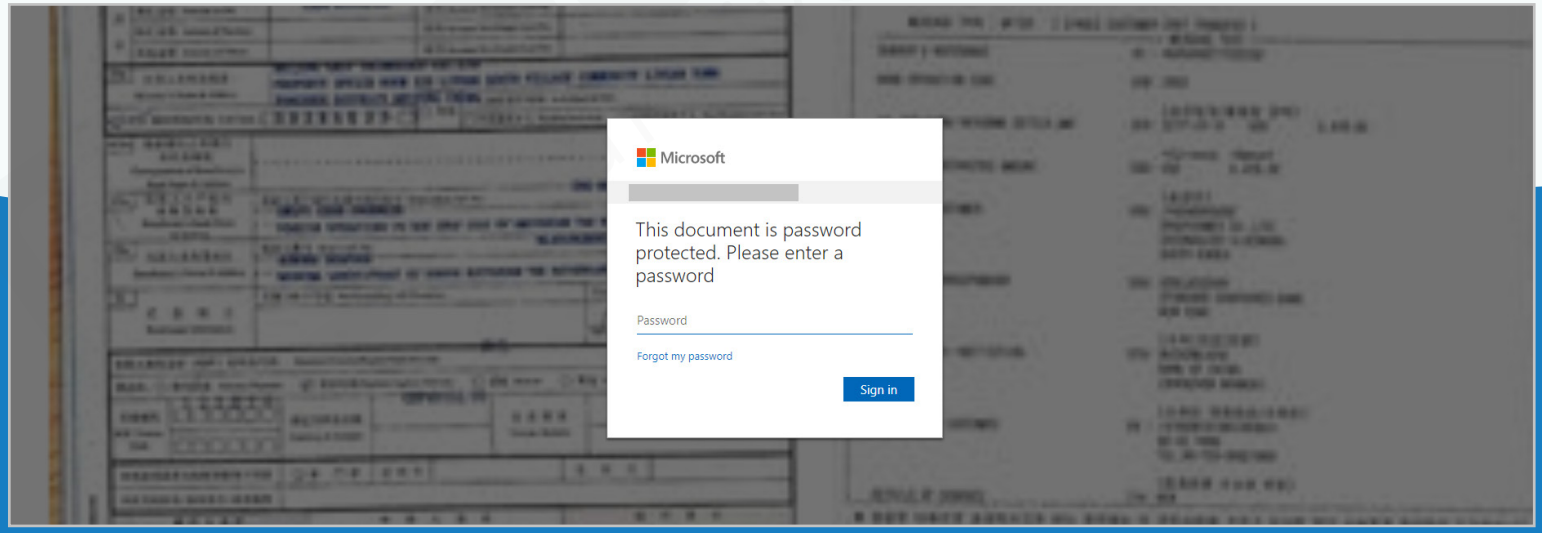


Microsoft phishing daalde in het vierde kwartaal terug tot het normale niveau, met 9.013 gedetecteerde unieke phishing-URL's. De Emotet-hackers maakten handig gebruik van het vertrouwen van de gebruikers in Microsoft. Microsoft Word is het meest gebruikte elektronische document in de wereld. Door de visuele herkenbaarheid van het logo en de daarmee gepaard gaande authenticiteit zagen cybercriminelen een uitgelezen kans om er succesvol misbruik van te maken.

We hebben dit in 2020 gezien met phishingmails die zich voordeden als andere merken dan Microsoft, maar toch links bevatten naar Microsoft-producten, waaronder Microsoft 365 en de bijbehorende toepassingen. Veel phishingmails van COVID-19 deden zich bijvoorbeeld voor als gezondheidsorganisaties, maar vroegen gebruikers in te loggen bij Microsoft 365 om bestanden en speciale meldingen op te vragen. In het onderstaande voorbeeld doet de cybercrimineel zich voor als Xerox en verwijst hij naar een vooraf ingevuld Microsoft-formulier.



Xerox phishingmail



Microsoft-formulier

GEAVANCEERDE PHISHING-AANVALLEN VEREISEN EEN GEAVANCEERDE VERDEDIGING

Phishing-aanvallen komen dagelijks voor. Of ze nu in uw map met ongewenste e-mail terechtkomen of in uw inbox, de aanvallen gaan door en worden steeds complexer. Daarnaast zijn ze ontworpen om zowel geavanceerde filters als getrainde gebruikers te omzeilen. Bescherm uw bedrijf en uw klanten tegen dynamische phishing-aanvallen met een combinatie van training, technologie en waakzaamheid:

Gebruikerstraining: Investeer in phishing-training die verder gaat dan de jaarlijkse trainingssessie. Door contextuele training aan te bieden op het moment dat de gebruiker op een phishing-link klikt, wordt de handeling aan de training gekoppeld, waardoor deze beter wordt onthouden door de gebruiker.

AI-gebaseerde anti-phishing technologie: AI-gebaseerde anti-phishing technologie overtreft verdedigingssystemen op basis van reputatie en digitale handtekening. Zelflerende leeralgoritmen proberen op basis van de oefendataset te generaliseren om zo variaties van bekende aanvallen te herkennen. Algoritmen voor Deep Learning met computervisie worden getraind om beelden te herkennen, waarbij zelfs minieme vervormingen van de beelden, ontworpen om aan detectie te ontsnappen, worden opgespoord.

Geautomatiseerde phishing-bestrijding: Phishingmails die een filter omzeilen blijven niet lang ongeopend. Geautomatiseerde phishing-bestrijding verwijdert bedreigingen na ontvangst, waardoor handmatig onderzoek en reactie worden verminderd.

Bescherming tegen meerfasige aanvallen: Spear-phishing e-mails zonder links en onbekende malware vereisen extra technologieën en mogelijkheden in één oplossing. Zelflerende leeralgoritmen detecteren zeldzame gebeurtenissen en anomalieën, terwijl natuurlijke taalverwerking schadelijk gedrag detecteert, zoals sleutelwoorden en zinsdelen die vaak voorkomen bij spear-phishing.

OVER VADE SECURE

Vade Secure biedt gebruikers bescherming tegen geavanceerde cyberdreigingen, zoals phishing, spear phishing, malware en ransomware. De software maakt hiervoor gebruik van kunstmatige intelligentie, gevoed door gegevens uit 1 miljard mailboxen, om zo gerichte bedreigingen en nieuwe aanvallen vanaf het eerste moment te blokkeren. Dankzij realtime detectie worden nieuwe bedreigingen onmiddellijk geïdentificeerd en kunnen er gecoördineerde maatregelen genomen worden.

Meer informatie

Wil je meer informatie? Neem dan contact op met onze sales afdeling via sales@office-it.be of ga naar www.office-it.be/veilig-thuiswerken

Office-IT: de betrouwbare partner voor uw ICT-beheer

Al sinds 2012 bouwen we bij Office-IT aan onze reputatie. Met meer dan 20 jaar ervaring op zak ontzorgen we onze klanten op het vlak van ICT-beheer vanuit onze 3 vestigingen in Olen, Deurne en Mortsel. Bij Office-IT vormen we een hecht team, dat gepassioneerd is door de job en waar mensen zich goed voelen. Een uitstraling die onze klanten onmiddellijk opvalt en weet te waarderen. Lokaal, in de cloud of hybride? U zegt het maar. Samen met u streven we naar de meest geschikte oplossing in functie van uw noden. Technische keuzes worden onderbouwd en omgezet in oplossingen op maat. We integreren de beste oplossingen op de markt, in samenwerking met zorgvuldig geselecteerde professionele partners. Tel daar nog onze flexibiliteit bij op en u heeft meteen een verklaring voor onze klanttevredenheid. Bij Office-IT is uw IT in goede handen. Meer informatie vind je op www.office-it.be

OFFICE~IT
CLOUD & MANAGED SERVICES PROVIDER
Armand Segerslei 118
B- 2640 Mortsel

t +32 (0)3 446 60 03
e info@office-it.be
i www.office-it.be

Copyright © 2021 Vade Secure