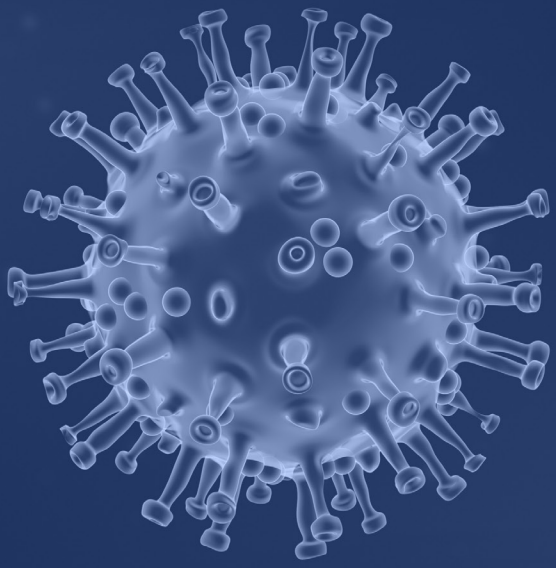
2021 Phishing Intelligence Report

rapport door PHISHED

Inhoudstafel

1. Key Learnings

Zonder grondige, voorafgaande opleiding is **1 op de 2** werknemers vatbaar voor phishing.



COVID-19- gerelateerde communicatie is het meest beruchte onderwerp in een succesvolle phishingcampagne.

23%

van de gephishte werknemers **voert gegevens in** op vervalste landingspagina's.

7% van alle werknemers opent mogelijk **gevaarlijke e-mailbijlagen**.

2. Inleiding: Algemene bevindingen voor 2021

De gezondheidscrisis van 2020, beter gekend als de **coronaviruspandemie**, vormde het startpunt van een aanzienlijke toename van de populariteit - of beruchtheid - van phishingaanvallen. Als fenomeen bleef de pandemie gedurende heel 2021 elk onderdeel van ons dagelijks leven beïnvloeden. Ondertussen hebben hackers en andere kwaadwillende actoren hun werkwijze op **efficiënte wijze aangepast** om nog beter aan te sluiten bij onze nieuwe en voorheen ongebruikelijke **manier van leven en werken**.

Deze aanpassingen werden onder meer ingegeven door:

- Verhoogde **angst, onzekerheid en emoties** als gevolg van COVID-19.
- **Onervarenheid** met thuiswerken, zowel vanuit het oogpunt van werknemers als van werkgevers.
  - Inclusief de noodzaak om snel nieuwe softwaretools en protocollen in te voeren en gebruikers op te leiden.
- Sterke stijging van:
  - Online winkelen.
  - Online dienstverlening (overheid, banken, leveranciers,...).
  - Nepnieuws (COVID-maatregelen, vaccinatie-informatie,...).

Naarmate het publiek geconfronteerd werd met plotse veranderingen in zowel hun persoonlijke als professionele omgeving, werd het voor hackers veel gemakkelijker om het terrein van de cybercriminaliteit te betreden:

- **Phishing-kits** zijn verkrijgbaar tegen steeds lagere prijzen. Ze zijn out-of-the-box gemakkelijk te gebruiken en verlagen de moeilijkheidsdrempel voor iedereen die bereid is het risico te nemen.
- **Databanken** worden steeds beter beschikbaar, deels omdat gebruikers door gegevensverzamelaars, zoals socialemediaplatformen, onvoldoende worden beschermd. Alleen al in 2021 maakten media melding van het ***scrapen* van gegevens van meer dan 1 miljard gebruikers** op twee van de grootste platforms ter wereld.
- **Diversificatie van kanalen:** het wordt steeds gemakkelijker om phishingaanvallen te diversifiëren. De kosten per sms (smishing) dalen elk jaar, terwijl de software om deze te exploiteren ook steeds goedkoper wordt en gemakkelijker te gebruiken. Voice phishing (vishing) wordt lastiger te herkennen, omdat aanvallers een meer **gelokaliseerde aanpak hanteren**.

Wist je dat?

'Mensen denken niet, ze klikken', vooral wanneer:

- De phishing boodschap kort en bondig is.
- Het bericht bevat een verzoek om hulp.
- De afzender lijkt bekend te zijn bij de ontvanger (de kans op een klik stijgt met 30%!)
- Het phishingbericht bevat een verwijzing naar een hot topic.

De coronapandemie heeft de deur definitief opengezet voor een voortdurende toename van het aantal phishingdreigingen. Aangezien phishing aan de basis liggen van het overgrote deel van alle cyberinbreuken, is het belangrijk dat mensen beseffen wat de gevaren zijn, hoe zij deze kunnen herkennen en hoe ermee om te gaan.

Om meer aandacht te vragen voor de phishingproblematiek, presenteert Phished zijn **'Phishing Intelligence Report'** voor 2021.

Veel leesplezier,
Arnout Van de Meulebroucke
CEO Phished

3. Over Phished en de database

3.1. Wie is Phished?

Phished zet in op de **menselijke kant van cyberveiligheid.** De AI-gedreven trainingssoftware koppelt gepersonaliseerde en realistische phishingsimulaties aan het opleidingstraject van de Phished Academy. Op deze manier leren medewerkers correct omgaan met online gevaren. Zo zijn werknemers voorbereid op cyberaanvallen, waardoor gegevens, activa en de reputatie van organisaties beter beschermd zijn.

3.2. De Phished-software en -database

90% van alle datalekken begint met een menselijke fout. Fouten die kunnen leiden tot virussen, ransomware, diefstal van geld en gegevens, en reputatieverlies. Phished traint uw medewerkers om efficiënt, effectief en binnen een veilige en gecontroleerde omgeving om te gaan met cyberbedreigingen.

De gegevens in dit verslag zijn verzameld door miljoenen phishingsimulaties te versturen naar **honderdduizenden ontvangers wereldwijd**.

Wij bouwen de human firewall bij PHISHED

4. Phishing wereldwijd

Iedereen, in elke uithoek van de wereld, in elke industrie of sector, in elke functie is kwetsbaar voor phishing. Dat is eens te meer bewezen als we kijken naar de wereldwijde Phished-statistieken voor 2021. Een overzicht van de belangrijkste statistieken voor Phished-ontvangers op wereldwijde schaal.

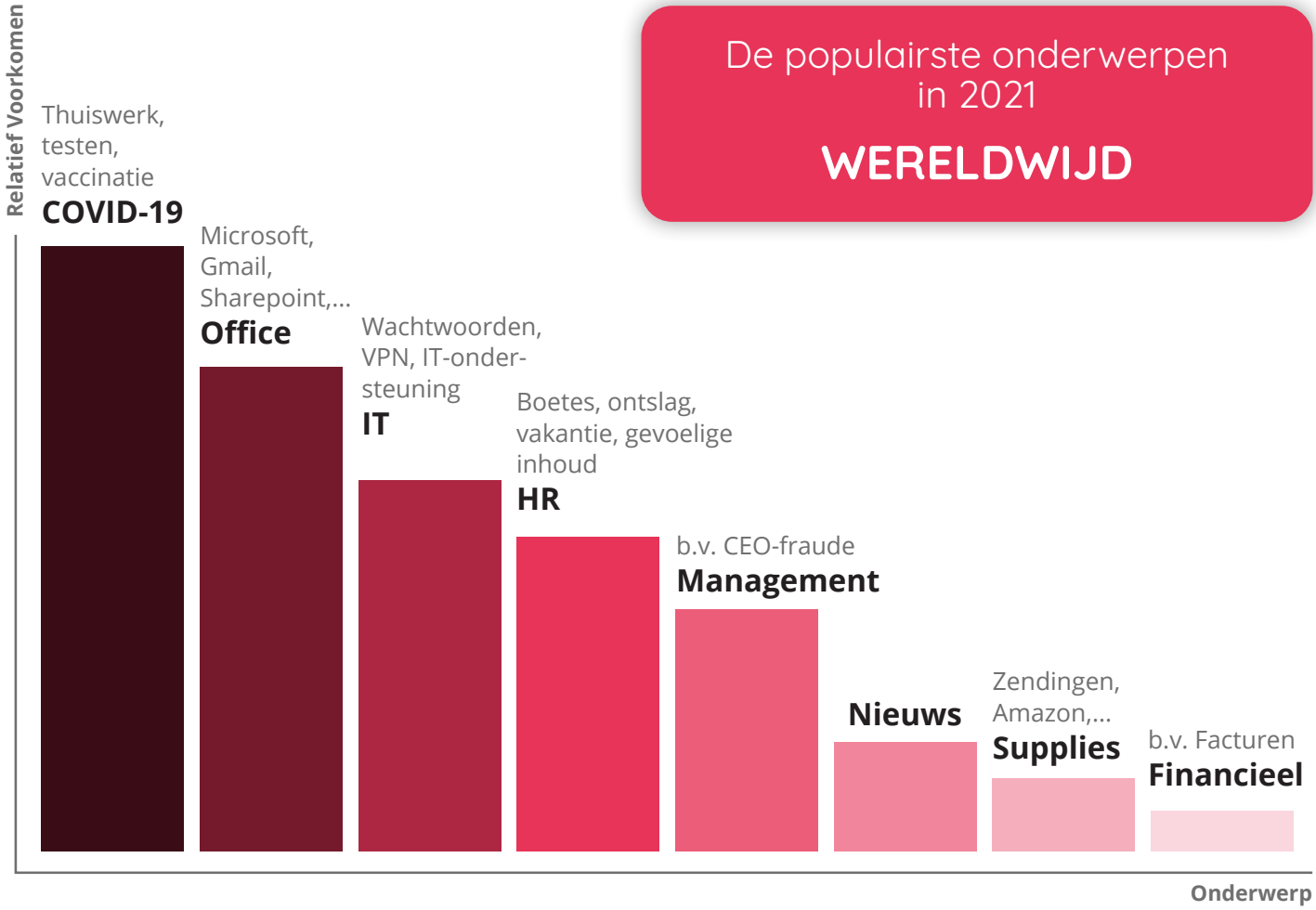
4.1. Meest populaire onderwerpen

In navolging van de trend van vorig jaar staat **COVID-19** opnieuw bovenaan de wereldranglijst. Dat is niet verwonderlijk, gezien de brede voorlichtings- en vaccinatiecampagne die burgers in de meeste landen heeft bereikt. De vele nepnieuws- en desinformatiecampagnes moedigden hackers aan om bijvoorbeeld in te spelen op de algemene ongerustheid over de risico's van vaccins en de bijwerkingen ervan.

Corona wordt op de voet gevolgd door **kantoorgerelateerde** e-mails ('Office'), variërend van problemen met Microsoft Office-tools tot inlogprompts van Gmail en bredere IT-gerelateerde phishingberichten met vragen over wachtwoorden, **IT-ondersteuning** en VPN-verbindingen.

HR-gerelateerde berichten vormen een opvallende categorie. In veel van deze berichten wordt verwezen naar de vakantie van werknemers, terwijl ook Not Safe For Work (NSFW)-berichten in deze categorie vallen: zij gaan over boetes, ontslagen of vermelden pornografische aspecten.

Financiële berichten (bv. over onbetaalde facturen) krijgen een bijzondere vermelding: zij vormen een belangrijk aandeel van alle succesvolle phishingberichten, maar **minder dan algemeen wordt aangenomen**.



4.2. Hoe kwetsbaar is de gemiddelde werknemer?

Phished verstuurt miljoenen phishingsimulaties per jaar. Organisaties kunnen de intervallen tussen simulaties zelf instellen, maar gemiddeld ontvangt een ontvanger één simulatie per tien dagen.

Wereldwijd is **22%** van alle simulaties succesvol. Als alleen rekening wordt gehouden met geopende phishingberichten, loopt dit op tot **53%**.

Als een simulatie de mogelijkheid biedt om gegevens in te voeren (bv. op een vervalste inlogpagina), voert **23%** van alle slachtoffers zijn gegevens in.

Als een bericht een bijlage bevat, downloadt en opent **7%** van alle ontvangers deze bijlage.

Op phishingberichten wordt niet vaak gereageerd: slechts **0,55%** van alle ontvangers gaf antwoord op een simulatie.

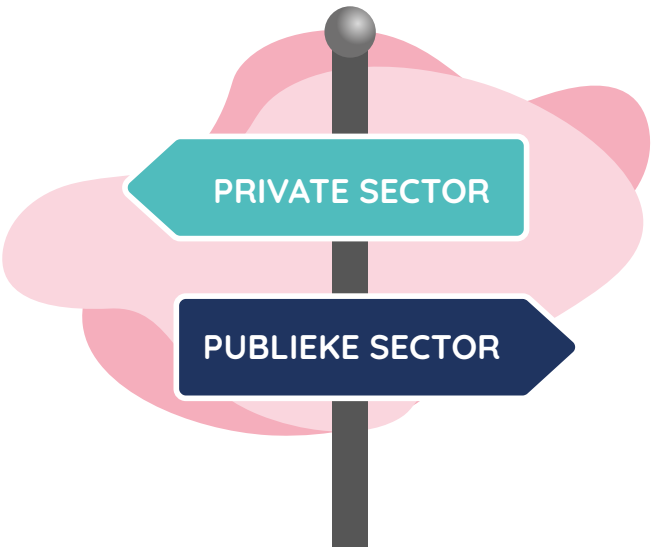
7% meldde de simulatie met succes.

Phished (van verzonden)	Phished (van geopend)	DataEntry (van geopend)	DataEntry (na gefrau-deerd te zijn)	Antwoordde	Bijlage	Gerapporteerd
21,63%	52,90%	5,11%	23,33%	0,55%	7,15%	6,85%

4.3. Publieke vs. private sectoren

Er is een duidelijk verschil in de manier waarop de publieke sector met cyberbeveiliging om (moet) gaan in vergelijking met de private sector. Aangezien openbare instellingen vaak met overheidsgeld worden gefinancierd, zijn zij bijvoorbeeld gebonden aan strenge en rigoureuze selectiecriteria bij de selectie van hun bewustmakingsprogramma's op het gebied van cyberbeveiliging.

Hoewel het moeilijk is te bepalen of dat een onderscheidende factor is wanneer beide gebieden worden vergeleken, blijft het een feit dat werknemers in de publieke sector over het algemeen **3% vaker** in de phishingval trappen dan werknemers in organisaties uit de privésector.



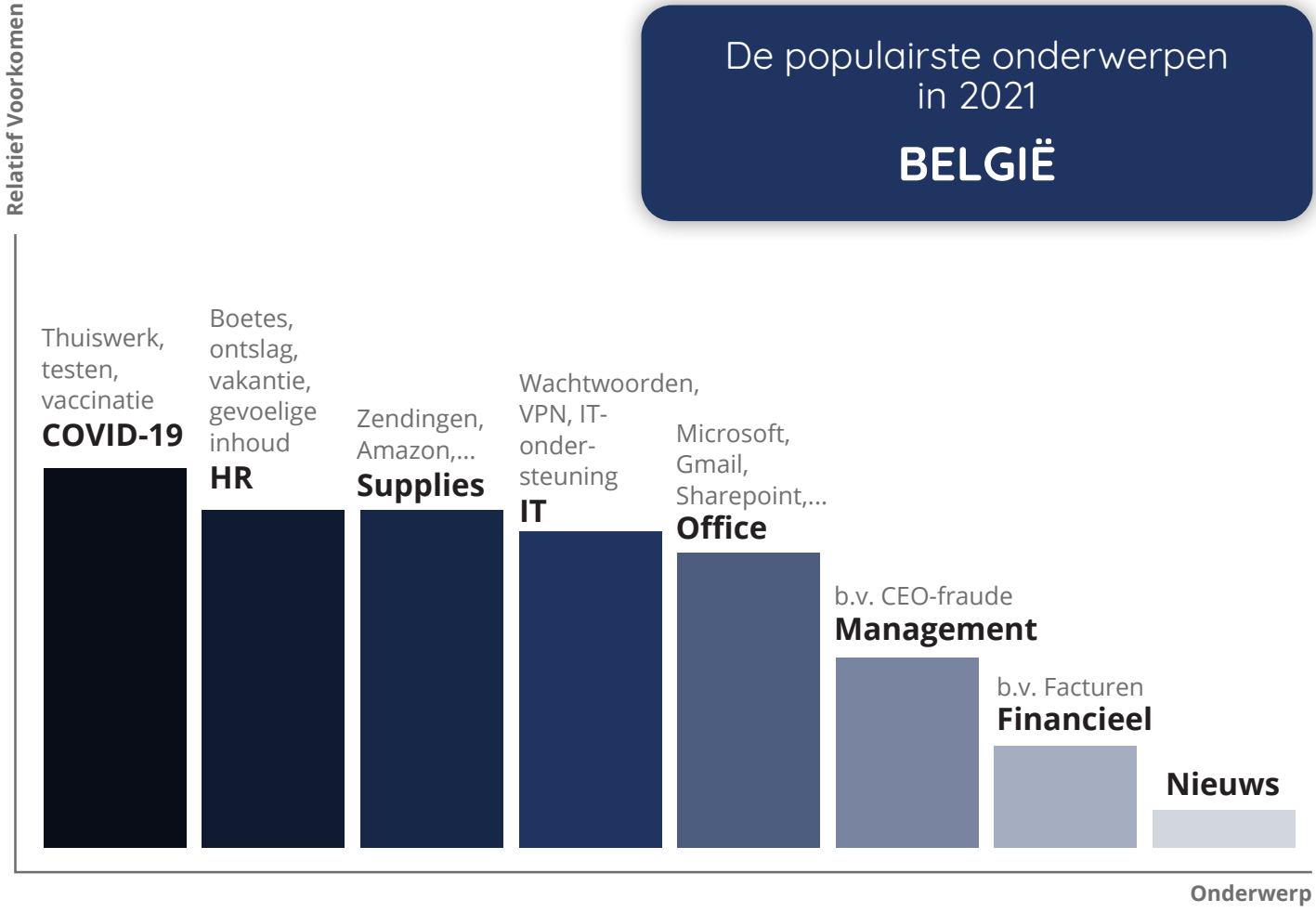
5. Phishing in België

5.1. Meest populaire onderwerpen

België volgt de wereldwijde trend en toont een gevoeligheid voor COVID-19-gerelateerde phishingberichten. Daarachter zijn de plaatsen twee tot en met vijf echter bijna gelijk aan elkaar, met een gelijkspel voor de tweede plaats: **HR**- en **Supply-gerelateerde** berichten zijn (ongeveer) even verleidelijk voor Belgische werknemers.

Wat de toeleveringsketen betreft, is er een merkbaar **lokaal tintje** aan de meest 'populaire' simulaties. Waar Amazon-simulaties wereldwijd tot de meest verraderlijke gespoofte afzenders behoren, worden zij vervangen door simulaties van bol.com en Coolblue in België.

Financiële berichten nemen de zevende plaats in; zij maken in België **aanzienlijk meer slachtoffers** dan het wereldwijde gemiddelde. Nieuwsgerelateerde berichten vervolledigen de Belgische lijst, maar met een beduidend lager percentage dan het globale gemiddelde.



5.2. Hoe kwetsbaar zijn Belgische werknemers?

In vergelijking met de wereldwijde resultaten, zitten de Belgische werknemers over het algemeen op hetzelfde niveau als hun collega's.

Belgische werknemers presteren merkbaar bovengemiddeld wanneer rekening wordt gehouden met de geopende phishing-simulaties: **47%** van de geopende berichten leidt tot een phishing-event, tegenover **53%** wereldwijd.

De verschillen zijn minder duidelijk wanneer naar de andere gegevens wordt gekeken: als een simulatie de mogelijkheid bevat om gegevens in te voeren (bijvoorbeeld op een gespoofte inlogpagina), voert **23%** van alle slachtoffers hun gegevens in. Als een bericht een bijlage bevat, downloadt en opent bijna **7%** van alle ontvangers deze bijlage.

Op phishingberichten wordt niet vaak gereageerd: slechts **0,42%** van alle ontvangers gaf antwoord op een simulatie.

7% meldde de simulatie met succes, iets minder dan het wereldwijde gemiddelde.

Phished (van verzonden)	Phished (van geopend)	DataEntry (van geopend)	DataEntry (na gefraudeerd te zijn)	Antwoordde	Bijlage	**Gerapporteerd**
22,67%	46,63%	4,96%	22,99%	0,42%	6,58%	**6,82%**

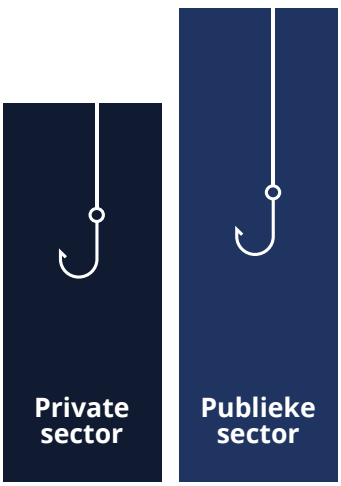
5.3. Publieke vs. private sectoren

De globale trend voortzettend, scoren Belgische overheidsinstellingen iets slechter dan organisaties in de private sector – maar het verschil is hier aanzienlijk groter:

Het verschil tussen beide sectoren bedraagt **5%**.

Dat is voor België een identiek resultaat ten opzichte van het jaar voordien.

5% meer kwetsbaar dan private sector



6. Prestaties met Phished

Wanneer nieuwe klanten het Phished-platform gaan gebruiken om hun medewerkers te trainen, zal de eerste simulatie die ontvangers bereikt meestal een algemene test zijn, vaak de 'nulmeting' genoemd. In het afgelopen jaar concludeerde Phished dat gemiddeld **45%** van alle ontvangers werd gephisht tijdens die eerste test. Indien de test een deel gegevensinvoer bevatte, voerde **27%** persoonlijke informatie in (logingegevens, unieke ID's,...).

In één geval behaalde Phished een succesratio van **100%**: dit was een nulmeting waarbij de klant voorkennis verstrekte die op dat moment een populair intern gespreksonderwerp uitmaakte. Dit resultaat benadrukt het gevaar van insider threats. Een gehackte mailbox van een werknemer zou mogelijk tot een vergelijkbaar resultaat kunnen leiden.

7. Trends voor 2022

Hoewel er regelmatig nieuwe trends opduiken, zijn de meeste succesvolle phishingaanvallen varianten op oudere campagnes of terugkerende campagnes die in het verleden succesvol zijn gebleken. Daarom is het van het grootste belang dat bedrijven beginnen met hun werknemers de basis bij te brengen:

De fundamentele problemen met phishing en hoe deze te herkennen.

Bij anti-phishingtraining gaat het om het aanleren van algemene principes die mensen helpen beschermen tegen meer specifieke bedreigingen.

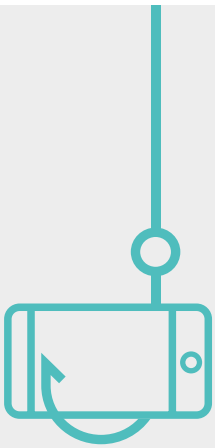
In 2022 zal de meest populaire trend van dit moment worden voortgezet: **COVID-19**-gerelateerde communicatie. Toch liggen er ook enkele nieuwe en 'opnieuw uitgevonden' phishingstrategieën in het verschiet.

Deepfakes

Deepfakes kunnen steeds gemakkelijker **in luttele seconden worden gecreëerd**, op elk smart device. Het zijn handige hulpmiddelen om iemands stem en gezicht na te bootsen als je over genoeg gegevens beschikt; momenteel zien we ze het vaakst gebruikt in Hollywoodproducties. In 2022 zullen we ze echter veel vaker zien opduiken op onze kleine schermen, in combinatie met phishingaanvallen.

Smishing

COVID-19 zorgde voor de definitieve doorbraak van SMS-phishing (smishing, waarbij ook rekening wordt gehouden met sms-diensten via webapplicaties). Omdat veel overheidscommunicatie gebruikmaakte van SMS, bijvoorbeeld om mensen te informeren over hun vaccinatiecodes, begonnen hackers deze berichten en inhoud te kopiëren. Zij koppelden deze aan overtuigend **nagebootste webpagina's**, wat tot veel fraude leidde. 2022 zal phishing nieuwe en onverwachte mogelijkheden zien gebruiken voor een communicatiemiddel dat an sich helemaal niet nieuw is.



Vishing

Wanneer mensen te maken krijgen met voice phishing (vishing), verwachten ze dat het een callcenter van Microsoft is dat hen vertelt dat er een probleem is met hun computer. Moderne vishing maakt echter gebruik van lokale mensen, l**okale onderwerpen en lokale gevoeligheden**. Het wordt een stuk moeilijker om echte bellers te onderscheiden van oplichters die om bankgegevens vragen.

QR-code fraude

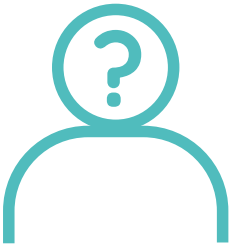
QR codes werden uitgevonden om de mogelijkheden van de traditionele streepjescode te verruimen. Ze zijn een populaire manier geworden om online transacties uit te voeren, maar voorzichtigheid is geboden. Een QR-code laat niet meteen zien wat ze bevat, wat betekent dat het scannen ervan de deur openzet voor mogelijke bedreigingen. Hackers kunnen er bijvoorbeeld extra mogelijkheden aan koppelen bij het verifiëren van betalingen, zodat ze toegang krijgen tot een bankrekening. Een ander gevaar doet zich voor bij 'man-in-the-middle'-aanvallen, waarbij een hacker kan proberen **een legitieme QR-code** te vervangen door zijn eigen frauduleuze alternatief.

Kalenderuitnodigingen-fraude

Er bestaan twee versies van deze vernieuwde zwendel: in de eerste versie verstuurt een gehackte entiteit van een betrouwbare bron uitnodigingen voor agenda's die spamfilters omzeilen en, om te kunnen worden geopend, inloggegevens voor zakelijke 'e-mail'-accounts vereisen. De ingevoerde gegevens worden vervolgens doorgestuurd naar de hackers.

In een tweede versie beginnen agenda-uitnodigingen uw agenda te vullen nadat u op een kwaadaardige link, pop-up of webbanner hebt geklikt. Hackers nemen vervolgens contact met u op om u te helpen 'het virus te verwijderen', waarbij ze zich voordoen als een professioneel cyberbeveiligingsbedrijf. In beide gevallen van deze zwendel is het raadzaam om zeer voorzichtig om te gaan met agenda-uitnodigingen.

Anonimisering



Het wordt voor aanvallers steeds makkelijker om online anoniem te blijven. Dit is deels te danken aan de opkomst en popularisering van cryptocurrencies. Omdat het een gedecentraliseerde methode is om rekeningen te vereffenen, is het steeds moeilijker om financieringsstromen van punt 'A' naar punt 'B' te volgen. Criminelen springen op de kar en werpen zo nieuwe barrières op tussen henzelf en de rechtshandhaving.

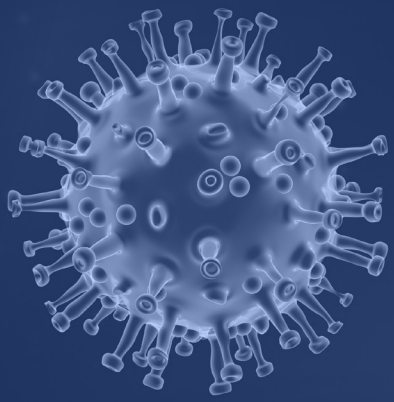
Een uiting van dit fenomeen is de doorbraak van **'Bitcoin mules'**: mensen die denken te werken voor legitieme cryptocurrency-agentschappen, belast met het creëren, aanwijzen en vereffenen van rekeningen, terwijl ze in werkelijkheid geld witwassen dat afkomstig is van criminele activiteiten.

8. Conclusies

Meer dan 1 op de 5 werknemers loopt het risico om gephisht te worden. Wanneer een phishingsimulatie gegevensinvoermogelijkheden bevat, zal 23% van alle slachtoffers zijn persoonlijke gegevens verder prijsgeven. 7% van alle ontvangers zal mogelijk kwaadaardige bijlagen openen. Wanneer Phished echter nieuwe klanten begint op te leiden, merken we vaak dat tot de helft van alle werknemers binnen een bepaalde organisatie in de phishingval zal lopen. Gemiddeld wordt 45% gephisht.

De **coronacrisis** staat bovenaan de lijst van populairste onderwerpen en het is duidelijk dat dit ook in 2022 het geval zal zijn.

De **Omikron-variant**, de lopende vaccinatiecampagnes en het vermoeden van gezondheidsdeskundigen dat de huidige crisis wel eens tot minstens 2025 zou kunnen duren, creëren een grote verantwoordelijkheid voor werkgevers: mensen opleiden in het herkennen van phishing en hen helpen er veilig mee om te gaan.



Natuurlijk mogen ook de andere onderwerpen niet worden vergeten. Pakketbezorging, HR en IT-gerelateerde onderwerpen blijven de werknemers bezighouden, evenals Office-gerelateerde berichten: de invloed van **thuiswerkinstrumenten** speelt duidelijk een rol.

In **2022** zal de trend van de afgelopen jaren zich waarschijnlijk **voortzetten**: phishing zal exponentieel in populariteit blijven toenemen onder criminelen, wat betekent dat aanbieders van cyberawarenessopleidingen waakzaam moeten blijven.

PHISHED

phished.io

hello@phished.io

+ 32 53 31 97 55