marketing fizz

MSP-Marketing

Starterskit

INTRODUCTIE

Hé daar!

MSP's leveren sterk werk, maar online klinkt dat nog te vaak zoals de rest. 24/7 support, security, Microsoft 365... allemaal belangrijk, maar niet genoeg om meteen het verschil te maken.

Daarom maakten we deze starterkit: een praktische basis om je marketing sneller scherper te zetten, zonder telkens van nul te moeten beginnen.

Wat zit er in deze #starterskit?

1. How to MSP-landingspagina om leads aan te trekken
2. Ready-to-use MSP-blog, ja gewoon copy-paste!
3. #SocialMedia post die je direct kan inzetten

'Why oh why' horen we je denken ...

Omdat sterke service niet vanzelf leidt tot sterke marketing. Veel MSP's weten perfect wat ze doen, maar krijgen dat online niet altijd helder vertaald. En net daar wringt het vaak: de expertise is er, het verhaal staat nog niet scherp genoeg. Met deze starterkit geven we je een sterk vertrekpunt om daar sneller werk van te maken.

Succes!

#TeamFizz

MSP-LANDINGSPAGINA

Toelichting
Je landingspagina is je beste verkoper: ze moet in één oogopslag herkenning creëren, vertrouwen opbouwen en duidelijk maken waarom jij de juiste MSP bent; nog vóór je eerste gesprek. Met de blokken hieronder bouw je een pagina die niet “mooi klinkt”, maar effectief aanzet tot actie.

Ready? Met deze blokken creëer je de ideale landingspagina rond jouw MSP-diensten:

H2 Titel Lorem ipsum

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus lacinia odio vitae vestibulum vestibulum.

Cras quis nulla at velit laoreet dapibus. Morbi id felis dignissim, aliquam libero eu, consequat mauris.

‹ Afbeelding ›

Dienst 1

Dienst 2

Dienst 3

Dienst 4

H2 MSP-diensten

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus lacinia odio vitae vestibulum vestibulum.

Cras quis nulla at velit laoreet dapibus. Morbi id felis dignissim, aliquam libero eu, consequat mauris.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium.

CTA ›

H2 Titel Waarom ...

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

- Lorem ipsum dolor
- Lorem ipsum dolor
- Lorem ipsum dolor

Cras quis nulla at velit laoreet dapibus. Morbi id felis dignissim.

‹ Afbeelding ›

Deze klanten gingen je voor

Case

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus lacinia odio vitae vestibulum vestibulum.

CTA ›

“Cras quis nulla at velit laoreet dapibus. Morbi id felis dignissim, aliquam libero eu, consequat mauris.“

Naam
Functie | Bedrijf

Closing CTA

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus lacinia odio vitae vestibulum vestibulum.

CTA ›

Gelukt?

Dan staat de basis van je landingspagina er. Je verhaal is helder, je aanbod staat scherp en je CTA zit op zijn plaats. Tijd voor de volgende stap: content die extra vertrouwen opbouwt en prospects nog beter laat voelen dat ze bij jou aan het juiste adres zijn.

2. BLOG BLOG BLOOOOOG

Toelichting

Deze blog is je slimme “trust-opener”: je geeft waarde weg, toont dat je vooruitdenkt en bouwt geloofwaardigheid op nog vóór iemand contact opneemt. Zet ’m live, deel ’m op socials en link ’m vanaf je landingspagina; zo wordt je CTA geen sprong in het donker, maar een **logische volgende stap.**

Email bombing + vishing: de aanval die je mailfilters omzeilt in 2026

Een volle inbox is niet altijd een “drukke dag”

Je inbox ontploft: honderden tot duizenden mails in korte tijd. Terwijl je probeert te filteren wat belangrijk is, belt “IT support” met een behulpzame toon: “We zien een incident. We lossen het meteen op. Kun je even …”

Dit is geen toeval. Het is een bewuste tactiek: email bombing als rookgordijn, gevolgd door vishing (voice phishing) om je mensen onder druk te zetten en procedures te laten overslaan. Microsoft beschreef recent expliciet aanvallen die email bombing combineren met vishing en zelfs impersonatie via Microsoft Teams, om overtuigend als IT-support over te komen en remote access te krijgen.

In 2026 is het risico niet (altijd) dat mensen “verdachte links” klikken. Het risico is dat ze onder stress een uitzondering maken.

Wat is email bombing?

Email bombing is het overspoelen van een mailbox met een enorme hoeveelheid berichten, vaak via geautomatiseerde inschrijvingen op nieuwsbrieven of formulieren.

Het doel: je inbox onbruikbaar maken, en belangrijke meldingen verbergen in de ruis. MITRE beschrijft het als een techniek waarbij aanvallers een adres massaal registreren, wat leidt tot een golf aan e-mails die je inbox overlaadt. Belangrijk: email bombing is vaak geen “einddoel”, maar een voorfase.

Wat is vishing (en waarom werkt het zo goed)?

Vishing is phishing via telefoon: iemand doet zich voor als een betrouwbare partij (IT, bank, leverancier, collega) en probeert je informatie of acties te ontlokken.

Waar klassieke phishing vaak botst op filters en training, speelt vishing op iets anders: autoriteit, urgentie, schaamte ("ik heb iets verkeerd gedaan"), en behulpzaamheid. En in combinatie met email bombing wordt het nog sterker: de inbox-chaos maakt het verhaal geloofwaardig.

Waarom die combinatie zo gevaarlijk is

De combinatie van mail bombing en vishing werkt omdat het drie dingen tegelijk doet:

1. Het creëert chaos
2. Mensen zien de situatie als "incident" in plaats van "scam".
3. Het dwingt snelheid af
4. Hoe langer je wacht, hoe meer het "probleem" lijkt te escaleren.
5. Het verlegt het kanaal
6. Je e-mailbeveiliging kan top zijn, maar telefoon (en Teams) is vaak minder strak afgedekt met verificatieregels.

Microsoft signaleert dat aanvallers deze tactiek gebruiken om geloofwaardig IT-support te spelen en toegang te krijgen.

Hoe zo'n aanval er in de praktijk uitziet

Je hoeft geen exact script te kennen om je te beschermen. Dit zijn de typische patronen:

- Inbox "stormt" vol met subscription e-mails of meldingen.
- Kort daarna volgt een call: "We zien verdachte activiteit", "Je mailbox staat onder aanval", "We moeten je account veiligstellen."
- De beller stuurt je naar een "snelle fix":
  - software installeren / remote tool openen
  - MFA resetten of een goedkeuring "even" toestaan
  - een link openen "om het probleem te stoppen"
- Er wordt geduwd op uitzonderingen: "Normaal doen we dit via ticket, maar dit is dringend."

Microsoft beschrijft ook dat email bombing gebruikt kan worden om kritieke alerts (zoals MFA prompts of password resets) te verbergen in de massa.

7 signalen waar je op moet letten

Deze signalen zijn herkenbaar, ook voor niet-technische collega's:

- Onverwachte urgentie ("nu meteen" / "je account wordt afgesloten")
- Kanaalwissel (e-mailchaos → "los het op via call")
- Verzoek om uitzonderingen ("normaal niet, maar vandaag wel")
- Druk om remote access te geven
- Verificatie wordt ontmoedigd ("niet nodig, ik ben IT")
- Vage identiteit (geen ticketnummer, geen interne referentie)
- Je voelt je opgejaagd (dat gevoel is een signaal, geen detail)

Wat je vandaag al kan doen (zonder tooling)

De beste verdediging is een combinatie van proces + techniek + training. Begin met deze basis:

1) Maak "call-back" een vaste regel

Geen discussie, geen uitzonderingen: Bij IT-support calls bel jij terug via een bekend nummer (intern directory, officiële vendor contact, helpdesk portaal).

2) Werk met verificatie-stappen

Een simpele standaard helpt enorm, bv.:

- ticketnummer + naam + afdeling
- wat is het probleem, op welk toestel, welke gebruiker
- "ik bel terug via ons officiële kanaal"

3) Leg escalatie vast

Wie mag remote access toestaan? Wie mag MFA resetten?
Maak dat expliciet, zodat "de meest behulpzame persoon" niet automatisch de zwakste schakel wordt.

4) Zet alerts slim (en zichtbaar) buiten e-mail

Als cruciale security alerts enkel via mail komen, verdwijnen ze sneller in de ruis. Overweeg redundantie via security portals/teams-kanalen/notifications (afhankelijk van je stack).

5) Oefen het één keer per kwartaal

Geen grote awareness-show. Gewoon een 15 minuten scenario: inbox-chaos + "support call". Doel: pauzeren, verifiëren, loggen.

Conclusie

Email bombing + vishing is geen technisch wonderwapen. Het is een stress-aanval op je mensen en processen. Wie duidelijke verificatie-afspraken heeft, haalt de angel eruit. Wil je weten of jullie verificatie- en incidentflow hiertegen bestand is? Vraag een korte social engineering readiness check aan.

3. #SOCIALMEDIA

Toelichting

Gebruik deze post om je blog een vliegende start te geven. Kopieer, plak, voeg je bloglink toe en publiceer. Zo creëer je snel een extra touchpoint dat herkenning en vertrouwen opbouwt.

Ready? Met deze post zet je je blog in één klik op LinkedIn:

1

2

Cyberaanvallen worden steeds vaker multi-channel: e-mail → telefoon → (soms) Teams.

Een sterk voorbeeld dat we steeds vaker zien: email bombing als rookgordijn, gevolgd door vishing om verificatiestappen te omzeilen.

Geen sensatie, wél realiteit. En net daarom loont het om hier vooraf afspraken rond te maken: call-back regels, verificatie, escalatie en logging. Simpel. Werkbaar. En vooral: toepasbaar op een drukke werkdag.

In deze blog leggen we uit hoe de aanvalsketen werkt én geven we een mini-checklist om je incidentflow scherper te zetten.

Lees de blog: [LINK]

#Cybersecurity #MSP #Vishing #Phishing #SecurityAwareness

#MAAS

MARKETING FIZZ AS A SERVICE

Marketing FiZZ is a no-nonsense agency that assists IT and software companies in strategically and successfully implementing marketing.

We provide proactive advice and help our clients to take many steps forward!

CONTACT US!

M: hello@marketingfizz.be
T: 0492 72 61 91

Komiteistraat 46-52, 2170 Antwerp
Belgium