

Veilig Mailen



Nog nooit was het zo makkelijk in digitale communicatie te voorkomen dat menselijke fouten tot datalekken leiden.

ZIVVER controleert het mailadres van de ontvanger, het bericht en de inhoud van de bijlage.

ZIVVER is een platform voor veilig mailen dat helpt datalekken door menselijke fouten te voorkomen. Hiermee beschermt het organisaties tegen de zware gevolgen van datalekken, zoals imagoschade en AVG-boetes. ZIVVER beschermt daarmee ook je klanten, door ongewenste toegang tot hun privé-informatie te voorkomen.

Met Veilig Mailen biedt ZIVVER de meest uitgebreide en toekomstbestendige oplossing op de markt. Het platform controleert het mailadres van de ontvanger, het bericht en de inhoud van de bijlage. Als er iets dreigt mis te gaan, waarschuwt ZIVVER de gebruiker met een melding die moet worden opgelost voordat de mail verzonden kan worden. Zelfs als er toch iets mis gaat na deze waarschuwing, biedt het platform de optie om een bericht in te trekken. Zo hebben ontvangers, en geadresseerden aan wie zij het bericht hebben doorgestuurd, geen toegang meer tot het bericht. Het is ook mogelijk om een vervaldatum in te stellen voor een bericht. Dit is handig voor informatiebeveiliging, maar is ook voor andere (zakelijke) toepassingen zeer nuttig.

Wat ZIVVER jouw organisatie kan bieden



Realtime controle van ontvangers, e-mail en bijlagen



E-mails intrekken



2FA om berichten te openen



Asymmetrische encryptie



Ondersteuning voor gastgebruikers



Outlook Plug-in



WebApp en Mobile App



Corporate Guest Branding



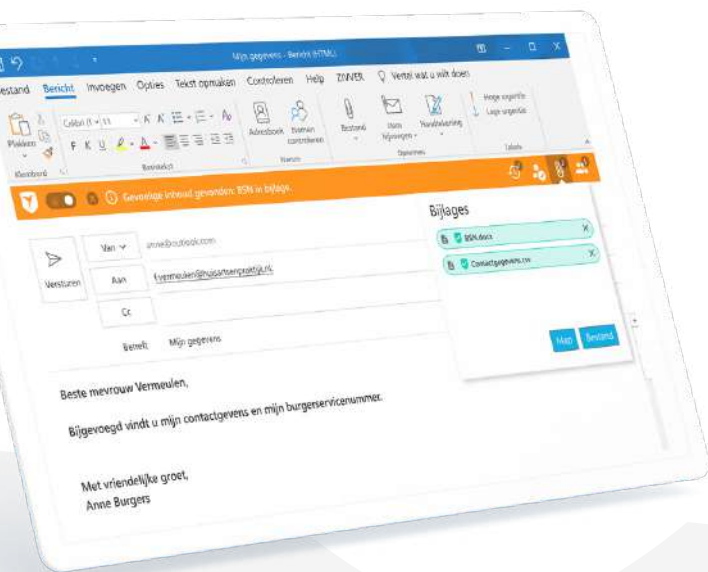
Veilige Conversatiestarters

1 De speerpunten van ZIVVERs platform voor Veilig Mailen:

Je kunt ZIVVERs Conversatiestarter direct koppelen aan een persoonlijk account. Wanneer je een link voor veilig mailen in je e-mailhandtekening zet, kan iedereen zonder ZIVVER-account een veilig gesprek beginnen met een specifieke contactpersoon binnen jouw organisatie. Zo kunnen contacten van buiten je organisatie veilig privé-informatie versturen vanuit dezelfde veilige mailomgeving van ZIVVER.

2 Tweede factor authenticatie (2FA) voor ontvangers

Iedere mail die via ZIVVER wordt verstuurd kan alleen maar worden geopend als de ontvanger gebruik maakt van tweede factor authenticatie (2FA). Op die manier weet je altijd zeker dat je bericht alleen bij de juiste ontvanger(s) terecht komt. ZIVVER biedt 2FA door middel van een SMS-code, een e-mail of 2FA apps (zoals Google Authenticator).



3 De veiligste manier van e-mailencryptie

ZIVVER gebruikt asymmetrische e-mail-encryptie, wat betekent dat er twee sleutels worden gebruikt om een bericht te versleutelen. Deze sleutels worden via het internet of intranet uitgewisseld. Dit zorgt ervoor dat kwaadwillenden geen toegang krijgen tot het bericht. Wie zo'n geheime sleutel heeft, kan het bericht ontsleutelen. Daarom gebruikt asymmetrische encryptie twee sleutels, die met elkaar verbonden zijn. De openbare sleutel is, zoals de naam al zegt, openbaar en beschikbaar voor iedereen die jou een privésleutel, houd je geheim zodat alleen jij en de ontvanger(s) de mail kunnen lezen.

4 Bestanden delen tot 5 TB

Wat uniek is aan ZIVVER, is dat het mogelijk is om tot 5 TB aan data als e-mailbijlage te versturen. Geen enkele andere dienst ter wereld biedt zo'n grote mogelijkheid voor het delen van bestanden via e-mail. Nude capaciteit voor dataopslag toeneemt, en de data zelf uitvoeriger wordt, ontstaat de vraag naar de mogelijkheid om grotere bestanden te kunnen delen. Als je in de toekomst dagelijks 5 TB aan data moet delen, ben je met ZIVVER al voorbereid hierop.

Heb je vragen over Veilig Mailen of andere ZIVVER-diensten?

Neem contact op met ons team.

+31 (0) 85 01 60 555

contact@zivver.com

www.zivver.com

linkedin.com/company/zivver

@ZIVVER_NL

facebook.com/zivver