

## EN VELFUNDERENDE MAILLØSNING SKAL BÅDE VÆRE SIKKER OG TROVÆRDIG

**Mail er en forretningskritisk kommunikationsplatform – som er og forbliver vigtig for enhver virksomhed.**

Med en moderne it-løsning følger også moderne kommunikationsværktøjer, som fx Microsoft Teams. De nye værktøjer er smarte og hjælper til nemmere samarbejde. De kan dog ikke erstatte e-mail, som en forretningskritisk kommunikationsplatform. E-mail er og forbliver vigtigt for enhver virksomhed.

Mail Security Management (MSM) er en service, der komplementerer Exchange Online og tilhørende teknologier, ved at tage hånd om mailløsningen og følge best practice på området.

**Angreb via fx spam, phishing og spoofing er stigende**  
Falske e-mails, phishing efter data, spamfiltre, blacklisting og spoofing. Truslerne er mange og selvom e-mail er en ældre teknologi, så udvikles tilstedende teknologier og angrebsmønstre sig konstant. At være på forkant hermed er afgørende for en sikker og velfungerende mailløsning.

**Ikke kun de mails du modtager – også dem du sender**  
Manglende fremkommelighed af de mails du sender eller mails der sendes på vegne af dig uden dit kendskab, er også et stigende problem, der skal tages hånd om. Det er vigtigt for at beskytte dit image eller brand.



**SPF** - (Sender Policy Framework) er et simpelt system til validering af mails, og er designet til at detektere spoofing.

Modtageren af en mail kan kontrollere, at indgående mails fra et domæne kommer fra en server, der er godkendt af domæne-ejeren (afsender).

**DKIM** - (DomainKeys Identified Mail) beskriver, hvordan der kan knyttes et domænespecifikt id til en mail.

Domæne-ejeren kan signere den enkelte mail med en privat signeringsnøgle og dermed give modtageren mulighed for at verificere, om mailen er afsendt fra en troværdig server.

**DMARC** - (Domain-based Message Authentication, Reporting and Conformance) er en e-mail-autentifikations-protokol, som sætter en politik for anvendelsen af de to andre protokoller: SPF og DKIM.

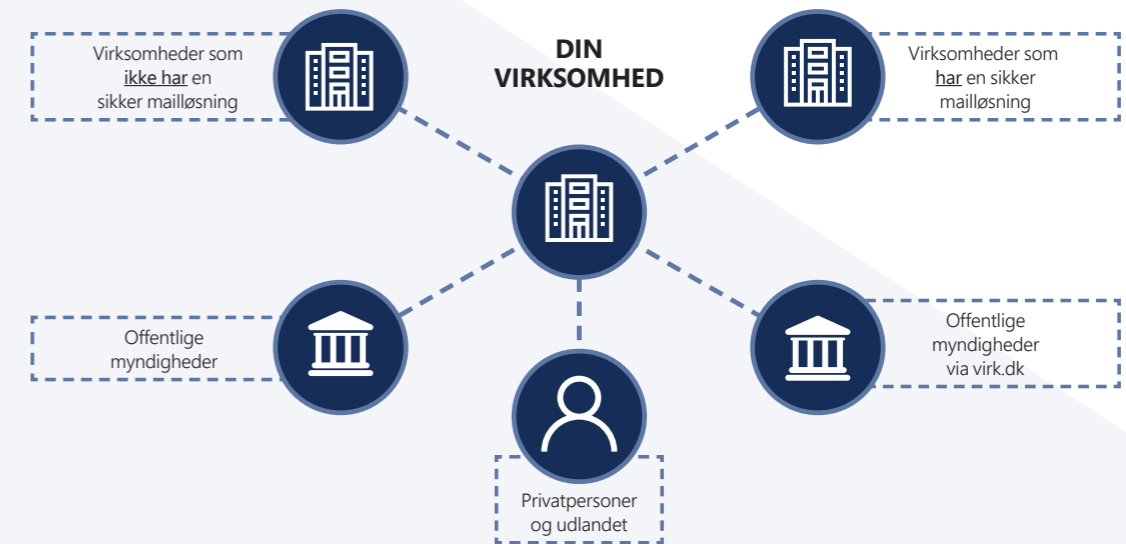
**Tilsammen giver de den bedste beskyttelse mod domænemisbrug.**

## SIKKER MAIL ER ET KRAV NÅR DU SKAL HÅNDTERE PERSONDATA - og et generelt krav når du kommunikerer med det offentlige

Ud over at følge best practice for generel mailbehandling, bør du også forholde dig til kryptering af de e-mails du sender og kan modtage.

Vi anbefaler en SIKKER@MAIL løsning hvis du modtager/sender mail med persondata fra fx ansøgninger, eller kommunikerer med offentlige myndigheder eller ønsker at modtage post direkte fra virk.dk (og dermed slipper for at logge ind i virk.dk).

Det offentlige accepterer kun krypterede e-mails og det bør du, i visse tilfælde, også gøre.



## DET FÅR DU MED MAIL SECURITY MANAGEMENT

### MSM - Basic

- **EMAIL VERIFICATION MANAGEMENT**  
Administration af SPF, DKIM og DMARC for begrænsning af forfalskede e-mails
- **THREAT PROTECTION MANAGEMENT**  
Begræns angreb via e-mail med vedhæftede filer eller links til sites med malware
- **SPAM POLICY MANAGEMENT**  
Administration af SPAM politik
- **MAILRELAY MANAGEMENT**  
Krypteret mailforsendelse fra fx printere
- **BEST PRACTICE MANAGEMENT**  
Løbende best practice tilpasning af løsningerne

### MSM - Pro

- **MAILBOX POLICY MANAGEMENT**  
Løbende kontrol og sikring af at postkasser overholder aftalte politikker
- **EMAIL ABUSE MANAGEMENT**  
Overvågning og rapportering af mængden af forfalskede e-mails, der udsendes og opfanges i forhold til misbrug af organisationens hoveddomæner
- **ANTIPHISHING MANAGEMENT**  
Begræns forfalskning af mailadresser, fx "CFO fraud"
- **SECUREMAIL MANAGEMENT**  
Administration af mailkryptering og evt. sikker post løsning (forudsætter særskilt SIKKER@MAIL aftale)

## Andre har suppleret med:

Sikker og pålidelig e-mail håndtering er blot en del af en større sammenhæng. Derfor er Mail Security Management-løsningen også en del af den større samlede løsning, Modern Management Suite. Desuden ser vi ofte danske virksomheder kombinere løsningen med:

**Microsoft Defender for Office 365 - Beskyttelse mod avancerede trusler som phishing og kompromittering af virksomhedsmail**  
Er inkluderet i Microsoft 365 Business Premium eller kan købes som særskilt licens. Bemærk at alle postkasser skal licenseres.

**SIKKER@MAIL - Send sikre mails, med ét enkelt klik**  
Tilføjer en knap i Outlook, hvor du ved ét enkelt klik sender mails, der er krypterede og signerede. Det betyder, at det kun er modtageren, der kan læse mailen – og modtageren er sikker på, at afsenderen er den, som vedkommende giver sig ud for at være.

**Styring af mailsignatur via cloud**  
Giv medarbejdere en ensartet signatur. Med en dynamisk signatur løsning kan du sikre at alle medarbejdere altid sender mails med signatur, der er baseret på nyeste opdaterede skabelon. Du kan både styre layout og vælge hvilke informationer, der skal fremgå af den enkelte medarbejders mailsignatur.

**Backup af Microsoft 365 og Dynamics 365 via cloud**  
Data i skyen er ikke nødvendigvis sikret så godt som du tror. En rigtig backupløsning er nødvendig for at kunne undgå tab af data ved fx menneskelige fejl (sletning eller overskrivning), hacking, ransomware eller lukning af brugerkonti.

Aktuelt for mig