



I denne manualen vil man se litt nærmere på epost-oppsettet i MAB. Hvordan man setter opp, og hva man skal se etter hvis det (plutselig) ikke virker lenger.

Her vil man også se på tilfeller hvor epost kommer frem til kunde, men går rett i kunden sin søppelpost/spam-mappe.

## Hvorfor skal man feilsøke selv, hvorfor ikke ta kontakt med support med en gang?

Fordi detaljene som gjør at epost plutselig ikke virker etc, er detaljer som ofte har med egne innstillinger å gjøre.

F.eks. har noen glemt å informere om at det har kommet ny leverandør av internett-tjenester etc.

Alternativt at man har byttet passord ett sted, uten at man har tenkt at endringen påvirker dette her – nemlig epost.

Samt at feilmeldingene man får i MAB *når ting som dette feiler* ofte vil fortelle mer om *hva* det er som er feil.

Hvis ditt firma har en person som er ansvarlig for nettverk, server, mailserver eller domene, så er det denne personen som bør få tilgang til denne manualen.

## Innhold

<b>Viktig</b> .....	<b>1</b>
<b>Spam og signering - Hva er SPF, DKIM og DMARC?</b> .....	<b>2</b>
SPF (Sender Policy Framework).....	2
DKIM (DomainKeys Identified Mail) .....	2
DMARC (Domain-based Message Authentication, Reporting and Conformance) .....	2
<b>Epost-oppsettet i MAB - Feltforklaring</b> .....	<b>3</b>
Eksempel oppsett for bruk av Microsoft 365 sin epostserver.....	4
<b>Feilsøking – OBS! Feilmeldingen man får vil ofte fortelle hva det er som er feil!</b> .....	<b>5</b>
Epost blir ikke sendt fra MAB.....	5
Epost blir sendt, men den kommer ikke frem til mottaker .....	5
SPF - Epost blir sendt fra MAB, men den går rett i kunden sin søppelpost – eller kommer ikke frem.....	6
SPF - hvordan ser man at det er dette som er årsaken? .....	6

## Viktig

Inkludere `_spf.mab.no` i ditt SPF-oppsett. Mer om dette lenger ned.

## Spam og signering - Hva er SPF, DKIM og DMARC?

Går din epost i spamfilter hos mottaker eller kommer eposten ikke frem?

De fleste epostservere har løsninger for å sortere søpleepost (spam). Disse arbeider på forskjellige måter, men noe av det de sjekker er SPF, DKIM og DMARC. Les mer teknisk om SPF her: [https://en.wikipedia.org/wiki/Sender\\_Policy\\_Framework](https://en.wikipedia.org/wiki/Sender_Policy_Framework)  
Det er derfor viktig at dette er satt opp riktig om det er i bruk (anbefaler å bruke dette).

Om dere ikke bruker SPF/DKIM/DMARC vil det åpne for at eksterne aktører (svindlere etc) kan sende epost på vegne av deg. Det vil også resultere i at reell epost fra dere kan havne i spamfilteret hos mottaker.  
Om SPF/DKIM/DMARC er satt opp feil eller du bruker feil epostserver vil det også kunne resultere i at epost havner i spamfilteret hos mottaker.

### SPF (Sender Policy Framework)

NB! Du må inkludere `_spf.mab.no`.

Dette er en DNS TXT-record på domene (f.eks *mittdomene.no*) som definerer hvilke epostservere som skal få lov til å sende på vegne av deres domene (f.eks *post@mittdomene.no*, *dagligleder@mittdomene.no* etc), samt hva som skal skje med epost som sendes fra andre servere.

Dersom SPF ikke er satt opp kan hvem som helst sende på vegne av dere.

Dersom SPF er satt opp, men du bruker feil epostserver vil epost trolig markeres som spam hos mottaker.

Eksempel på gyldig SPF-record dersom du bruker Office 365 og MAB:

TXT-record på ditt domene med følgende verdi: `"v=spf1 include:spf.protection.outlook.com include:_spf.mab.no -all"`

### DKIM (DomainKeys Identified Mail)

Dette er en signering av epost som skjer ved bruk av en privat nøkkel. Tilhørende offentlig nøkkel settes opp i DNS.

Mottakers epostserver sjekker så signaturen i eposten opp mot public key som ligger på avsenders domene for å verifisere om epost er kommet fra gyldig epostserver/domene. Les mer teknisk om DKIM her:

[https://en.wikipedia.org/wiki/DomainKeys\\_Identified\\_Mail](https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail)

#### Oppsett av DKIM kan gjøres på 2 måter:

Oppsett på epostserver.

Man trenger da bare å passe på å sende via denne epostserveren. Den har da normal verifisering som f.eks. brukernavn og passord, IP-filter etc.

Oppsett direkte i MAB.

MAB har da egne private nøkler samt en offentlig nøkkel som er registrering på `mab._domainkey.mab.no`.

Aktiveres i epostoppsettet i MAB (se eget punkt).

Ditt domene må ha et `mab._domainkey.mittdomene.no` CNAME som peker mot `mab._domainkey.mab.no`.

For å benytte DKIM- signering på epost:

- All epost? Alternativer, Administrasjon, Generelt, Epost og masseutsendelse, i "SMTP DKIM" Velg "All epost fra MAB skal signeres".
- Kun fra enkelte brukere/maskiner? Alternativer, Generelt, i "SMTP DKIM" velger du "Signere utgående epost med DKIM".

### DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC er et `_dmarc` TXT-record på deres domene, f.eks `_dmarc.mittdomene.no`.

Les mer teknisk om DMARC her: <https://dmarc.org/>

I denne recorden setter man hva som skjer om SPF/DKIM feiler og om mottakers epostserver skal varsle en gitt epostadresse med feil eller rapporter.

Eksempel på gyldig DMARC-record:

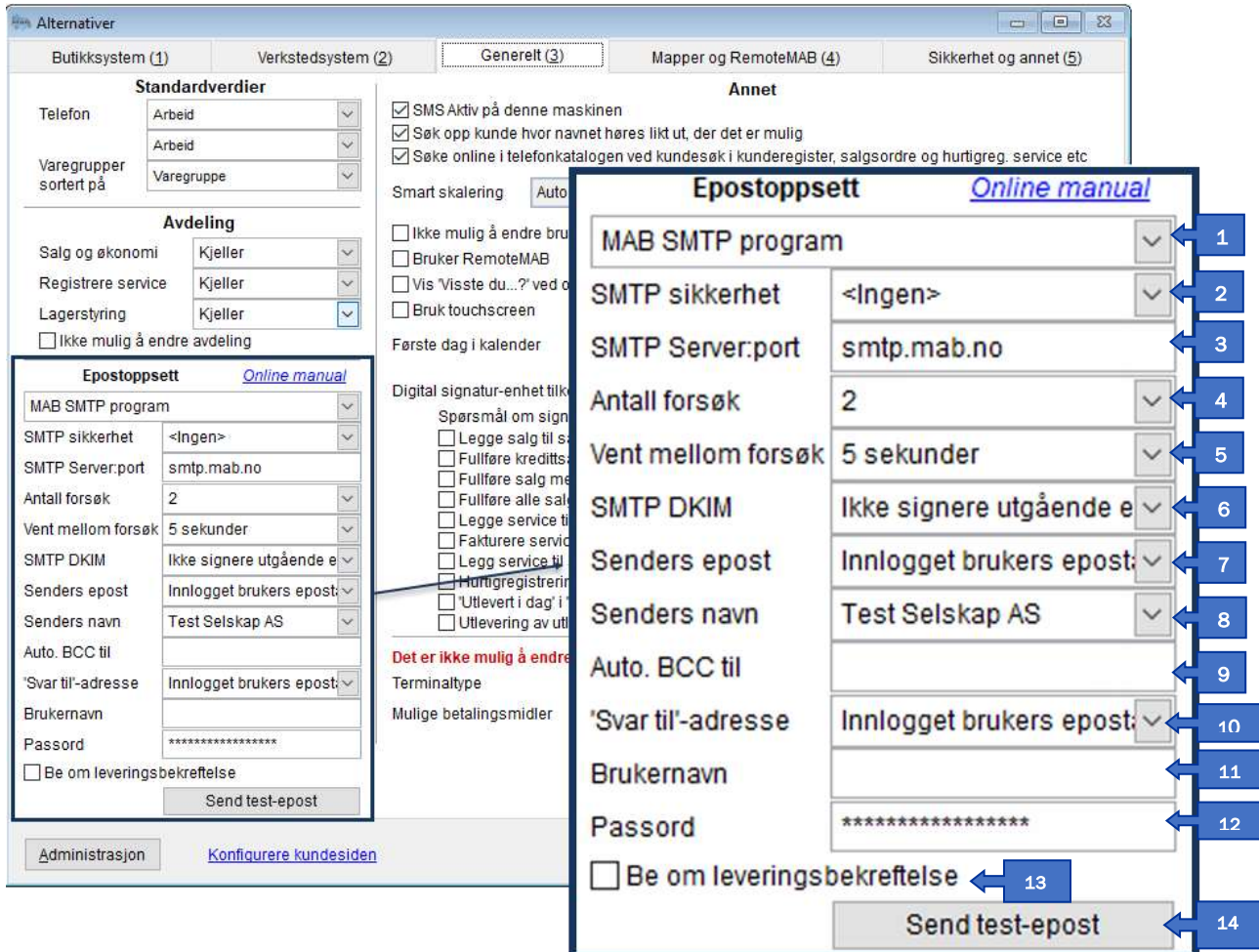
TXT-record `_dmarc.mittdomene.no` med følgende verdi: `"v=DMARC1; p=quarantine; ruf=mailto:post@mittdomene.no"`

## Epostoppsettet i MAB - Feltforklaring

Oppsettet finner man ved å gå inn følgende sted:

**Butikksystem:** Alternativer → Generelt → Nede til venstre

**Verkstedssystem:** Alternativer → Endre oppsett → Generelt → Nede til venstre



1. I nedtrekkmenyen øverst velger man program MAB skal sende epost via. Det anbefales her MAB SMTP, dette fordi det Outlook-valget er laget knyttet mot en eldre versjon av Outlook. I tillegg så er MAB SMTP-valget bedre til å takle terminalserver, Remote Desktop / RemoteAPP etc.
2. SMTP-sikkerhet har med kryptering å gjøre, her bør en nettverksansvarlig, domeneleverandør eller nettleverandør vite hva som skal velges.
3. Hva som skal stå utfyllt i feltet SMTP-server bør en nettverksansvarlig, domeneleverandør eller nettleverandør ha kontroll på.
4. Antall forsøk på å sende epost dersom tilkobling mot server feiler.
5. Antall sekunder mellom hvert forsøk på å sende.
6. Valg om hvorvidt eposten skal signeres med DKIM eller ikke (Les eget avsnitt om DKIM og krav rundt dette lengre oppe i manualen).
7. Fyll ut epost som man vil skal stå som avsender på eposter sendt fra denne PC-en. Dersom man sender epost fra MAB på «denne PC-en», så er eposten utfyllt her den som kunde vil se som avsender.
8. Navnet som vil stå som avsender på epost sendt fra denne PC-en.
9. Fordi man via MAB sitt epost-program ikke har 'sendte elementer', så har man her mulighet til å velge at for hver epost som sendes, så går det en «anonym kopi» til den adressen man fyller ut her. På denne måten har man mulighet til å dobbeltsjekke at epost har blitt sendt ved at den kommer til Outlook\* - eller hvis man bare vil ha en kopi selv av hva som faktisk er sendt.

10. Felt for utfylling av adresse som kunde skal svare til – hvis det er en annen adresse enn «Senders email». Skal normalt sett ikke være utfylt.
11. Felt for utfylling av brukernavn for pålogging til SMTP-server. Ikke alle krever dette.
12. Felt for utfylling av passord for pålogging til SMTP-server. Ikke alle krever dette.
13. Kryss i dette feltet gjør at mottaker av epost får opp et valg hvor vedkommende kan markere/bekreftede at epost er mottatt.
14. For å sende en test-epost.

\* Dersom man er bekymret for dette med at for hver eneste epost sendt fra MAB, så går det en kopi til denne adressen, så kan man i Outlook lage egne regler.

For eksempel, så kan man bestemme at disse kopiene man her får, automatisk skal gå til en egen mappe som f.eks. heter «Sendt fra MAB».

## Eksempel oppsett for bruk av Microsoft 365 sin epostserver

**Epostoppsett** [Online manual](#)

MAB SMTP program	▼
SMTP Server:port	smtp.office365.com
SMTP sikkerhet	TLS ▼
Brukernavn	post@mab.no
Passord	*****
SMTP DKIM	Ikke signere utgående e ▼
Senders epost	post@mab.no ▼
Senders navn	Bleken Data AS ▼
Auto. BCC til	noreply@bleken.no
'Svar til'-adresse	Innlogget brukers epost: ▼
Antall forsøk	2 ▼
Vent mellom forsøk	5 sekunder ▼
<input type="checkbox"/> Be om leveringsbekreftelse	
Send test-epost	

NB! Det kan være vanskelig å sette opp bruk av Microsoft 365 sin SMTP-server så det anbefales å bruke epostserveren til din internettleverandør eller sette opp en egen epostserver. Ta kontakt med IT-ansvarlig for hjelp med dette. Eventuell support fra Bleken Data AS på dette inngår ikke i normal supportavtale. Må mulig settes opp med trusted IP eller annet som går utenom MFA.

## Feilsøking – OBS! Feilmeldingen man får vil ofte fortelle hva det er som er feil!

### Epost blir ikke sendt fra MAB

Dersom man sender en test-epost fra MAB, så vil man faktisk kunne få en indikasjon på hva det er som er grunnen til at det feiler.

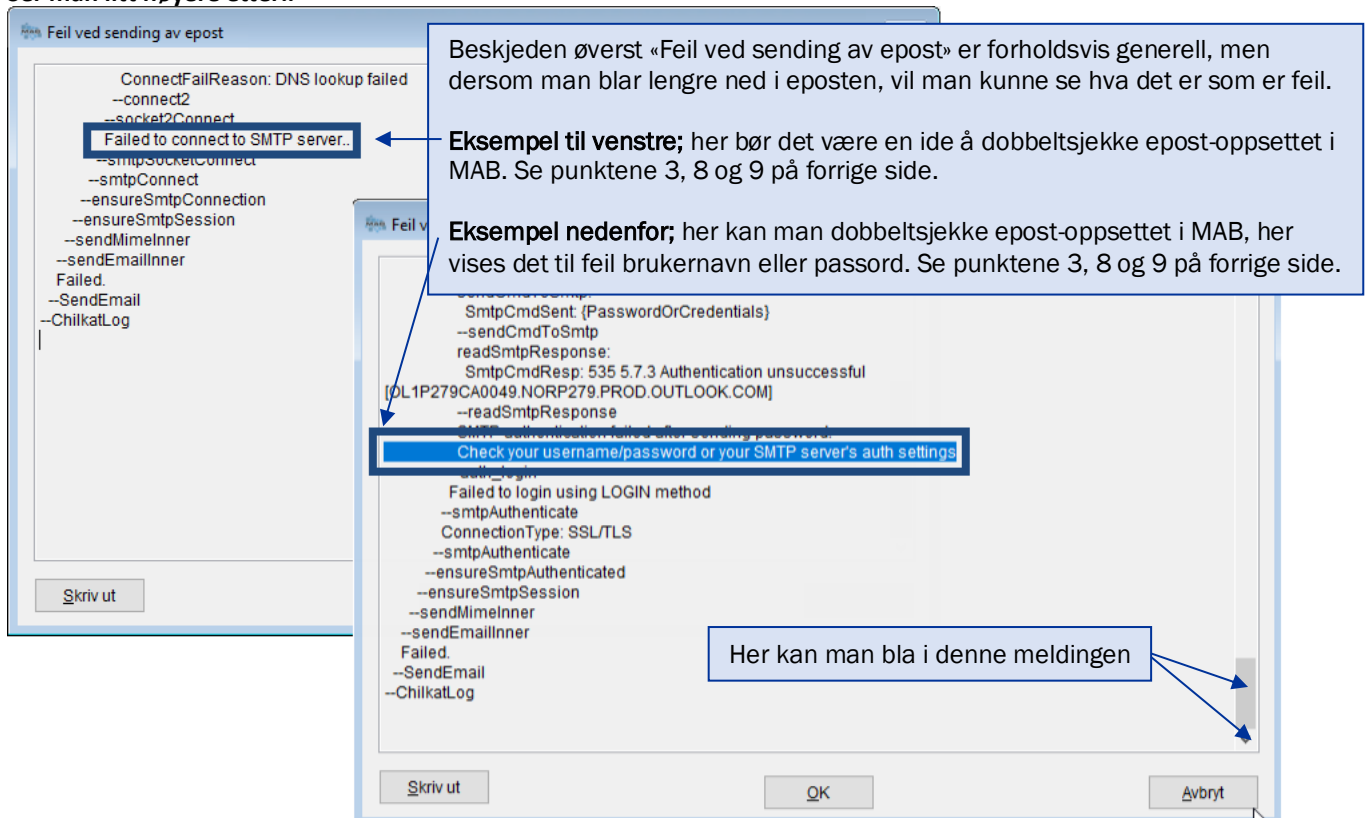
Har det seg slik at dersom epost-sending fra MAB har fungert tidligere, men ikke gjør det nå lengre, kan man stille seg selv spørsmålet «hva er forandret». Eksempler på hva som kan være forandre, og som er relevant her for feilsøkingen.

Har vi siden sist;

- fått ny internettleverandør
- fått ny domeneleverandør
- har blitt bedt om av Microsoft om å bytte passord

Dersom svaret er «Ja» på ett av disse spørsmålene, så må man forhøre seg med nettverksansvarlig, internettleverandør eller domeneleverandør om SMTP-adresse, brukernavn eller passord skal byttes i MAB. Se punktene 3, 8 og 9 på forrige side.

### Ser man litt nærmere etter..



Beskjeden øverst «Feil ved sending av epost» er forholdsvis generell, men dersom man blar lengre ned i eposten, vil man kunne se hva det er som er feil.

**Eksempel til venstre;** her bør det være en ide å dobbeltsjekke epost-oppsettet i MAB. Se punktene 3, 8 og 9 på forrige side.

**Eksempel nedenfor;** her kan man dobbeltsjekke epost-oppsettet i MAB, her vises det til feil brukernavn eller passord. Se punktene 3, 8 og 9 på forrige side.

Her kan man bla i denne meldingen

### Epost blir sendt, men den kommer ikke frem til mottaker

En åpenbar årsak er dersom man får skrevet feil i en epost-adresse.

Dette vil ikke MAB oppdage. Det MAB derimot kan oppdage er dersom epost-adressen er bygd opp feil.

Eksempel på en feil oppbygd epost-adresse kan være *post@@mab.no* eller *post.bleken.no* etc.

Et alternativ dersom epost ser ut til å ha blitt sendt fra MAB, men ikke komme frem; be kunden dobbeltsjekke i søppelpost-mappe. Se evt. også neste punkt; hva kan man gjøre dersom epost går rett til søppelpost hos kunde.

Hvis det sendes epost til en ikke-eksisterende (men «korrekt oppbygd») adresse, vil man i de fleste tilfeller få svar tilbake fra SMTP-serveren eller mottaker-domenet sin epost-server om at mottakers epost-adresse er ugyldig.

## SPF - Epost blir sendt fra MAB, men den går rett i kunden sin søppelpost – eller kommer ikke frem.

Dersom oppsett i MAB stemmer og epost-adresse til kunde stemmer – men epost går rett til kundens søppel/spam-mappe (eller ikke kommer frem), så kan man se på en «innstilling» som heter «SPF».

All epost som blir sendt fra MAB blir sendt med en avsender-adresse som «tilhører» dere. Denne domene-adressen har man skaffet fra en domene-leverandør. F.eks. er domenet til epost-adressen «post@mab.no» - «mab.no».

På domenet «mab.no», ligger det DNS-oppføringer hos domene-leverandører – som kort forklart fungerer som en adressebok for internett.

Innunder dette finnes det en epost-valideringsrutine som kalles «SPF» - som ligger som en «TXT-oppføring» på domenet. Denne skal sikre at avsender av eposten er korrekt – og har lov til å sende «fra» denne epost-adressen. Dette for å forhindre spam/phishing.

Moderne epost-lesere og epost-servere blir stadig strengere og strengere rundt dette – og dette er ofte hovedårsaken til havner i søppelkassen – eller i verste fall ikke kommer frem.

Det fungerer slik, at hvis mottaker ser at eposten kommer fra en epost-server som ikke ligger i «SPF-listen», så blir den (avhengig av regler satt opp hos mottaker) enten markert som spam, lagt i søppelpost-kasten, eller rett og slett ikke blir levert.

Dere kan se deres nåværende SPF-oppsett f.eks. her – ved å søke opp deres domenenavn. F.eks. «mab.no».

<https://mxtoolbox.com/SuperTool.aspx?action=spf:>

F.eks. for «mab.no» står det per i dag følgende;

Prefix	Type	Value	PrefixDesc	Description
	v	spf		The SPF record version
+	include	_spf.bleken.no	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

Pass på at deres domene inkluderer Bleken Data sin SPF-oppføring:

```
include:_spf.mab.no
```

Slik at hvis dere fra før f.eks. har:

```
v=spf1 include:_custspf.one.com ~all
```

Skal den nå være:

```
v=spf1 include:_spf.mab.no include:_custspf.one.com ~all
```

Hvis dere IKKE har SPF-oppføring fra før, anbefales dette på det sterkeste. Men det er da viktig at alle «servere» dere sender epost fra, legges inn. F.eks. utgående epost-server til Outlook (eller andre mailprogrammer), regnskapsprogrammer, etc.

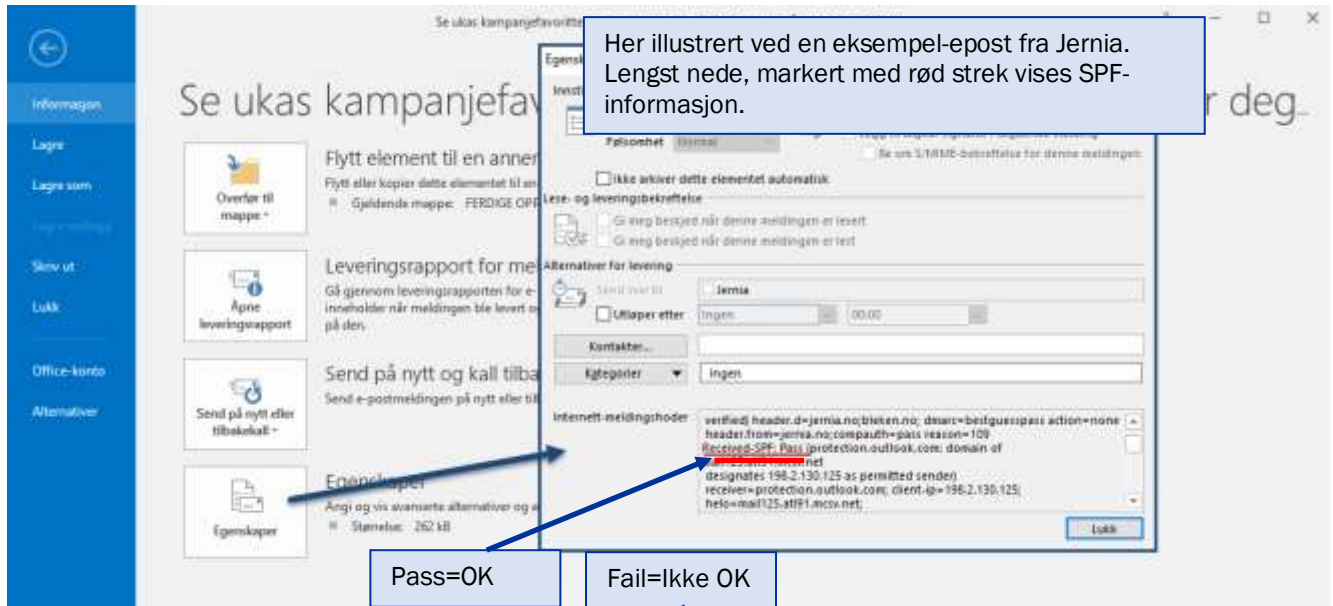
Support kan hjelpe til med oppsett her, men dette krever at dere har innlogging til deres domeneleverandør for hånden.

Hvis dere ikke har en SPF-oppføring fra før, så må det opplyses om hvilke andre tjenester/servere som skal legges inn. Det kan være at «deres» SPF-oppføring må hentes inn, hvis den ikke ligger tilgjengelig på internett (hvilket den gjør for de fleste internettleverandører.)

## SPF - hvordan ser man at det er dette som er årsaken?

Dersom man dobbeltklikker på en epost i Outlook, kan man gå til *Fil* oppe til venstre.

Trykk deretter på *Egenskaper*. Her kan man deretter bli i feltet som heter *Internett-meldingshoder (Internet headers)* og bla til man ser teksten SPF; etterfulgt av enten *Pass*, *SoftFail*, *Fail* eller *None*. Alt annet enn «**Pass**» bør sees nærmere på og muligens korrigeres.



Anonymisert, men fail.

