

Sender Policy Framework (SPF)

Vad SPF är

Sender Policy Framework, eller SPF som förkortning, är en teknik för att minska mängden skräppost på internet. Tekniskt så publicerar man en lista över vilka servrar som får skicka e-post för en viss domän. Den listan innehåller normalt ens egna e-post server, men också olika tredjeparts tjänster som kan skicka e-post. I fallet med Kodmyran Commerce så behöver våra servrar ligga med för att kunna skicka ut kundernas orderbekräftelser, produkttips, med mera.

Det fungerar genom att mottagande e-post server kontrollerar i DNS för den aktuella avsändande e-post domänen. Om det finns en speciell TXT post som börjar med den magiska texten "v=spf1", och sedan fortsätter med en lista över tillåtna och otillåtna adresser så används SPF. Ni hanterar alltså denna post via er DNS leverantör, och inte hos oss.

Inställningar

Det exakta formatet kan skilja sig lite åt beroende på vilka tjänster ni använder, vilken DNS leverantör ni har och så vidare. Men en bra start för hur det kan se ut hittar ni nedan:

- <erdomän> TXT "v=spf1 mx:<erdomän> include:kodmyran.se -all"

- Där <erdomän> skall ersättas med er egen domän, om vi antar att ni har e-post adressen "kalle.anka@exempel.com" t.ex. så skulle den färdiga posten se ut enligt nedan:

```
exempel.com TXT "v=spf1 mx:exempel.com include:kodmyran.se -all"
```

- Man kan läsa denna post enligt listan nedan, läses alltid ifrån vänster till höger och varje regel skiljs ifrån föregående med ett mellanslag. Så fort mottagande e-post server hittat en regel som träffar så slutar den läsa listan.

Entiteternas betydelse

1. v=spf1 - Indikerar att detta är en SPF post, DNS typen 'TXT' är en generell post och kan innehålla annat data än SPF - därför måste denna speciella text finnas med.
2. mx:exempel.com - Indikerar att alla (inkommande) e-post servrar som finns i DNS för domänen exempel.com också är betrodda att skicka e-post utåt.
3. include:kodmyran.se - Indikerar att alla SPF poster för domänen kodmyran.se också gäller för denna domän.
4. -all - Indikerar att alla andra varianter INTE är tillåtna (notera inledande minustecken)

Glöm inte bort att det kan finnas andra tjänster som det också behöver öppnas för, ett vanligt fall är ditt nyhetsbrevs program/leverantör - kontakta dessa för att veta hur de rekommenderar att man ställer in SPF. Normalt infogar man det mellan sina egna öppningar ("mx:exempel.com") ovan och "-all" på slutet.

Ibland räcker det tyvärr inte heller med att endast ha en SPF upplagd för att se till att ni blir white-listade, utan man kan även behöva sätta upp någonting som heter DKIM. Mer information om detta kan ni läsa i guiden 'Domain Key Identified Mail (DKIM)'.