



Brugermanual 1.1
d. 1. januar 2019

Introduktion

Hosted Spamfilter ligger uden tvivl blandt markedets mest sikre og effektive løsninger til frafiltrering af spam, malware, spear phishing og lignende uønskede e-mails. Kvaliteten afhænger selvfølgelig af, at løsningen løbende bliver administreret, kontrolleret og overvåget, hvilket 100% håndteres af os.

Herudover kan der i det daglige løbende opstå behov for tilpasninger, hjælp til opsætning og anden tvivl, hvorfor vi altid vil sidde klar til at hjælpe.

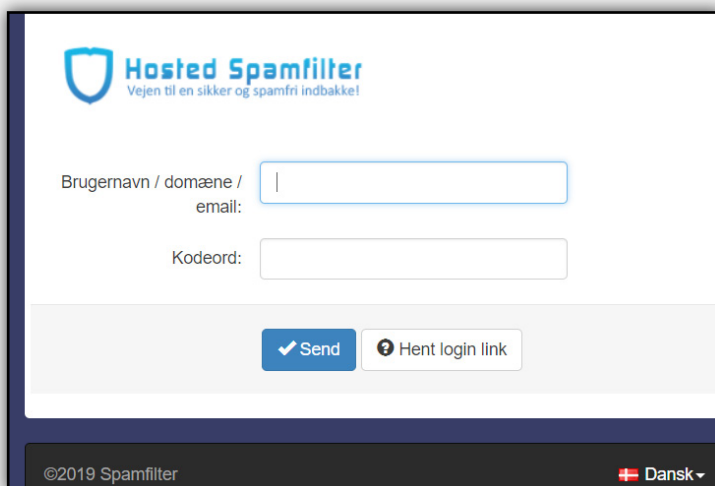
Hosted Spamfilter tilbyder dog muligheden for selv at kunne administrere løsningen, fra et online og altid tilgængeligt kontrolpanel. Denne brugermanual vil med udgangspunkt i dette, vejlede dig til hvorledes du selv, hurtigt og nemt, kan foretage langt størstedelen af de tilpasninger som måtte få brug for - ellers ringer du bare!

Indholdsfortegnelse

	Side
1. Log ind og adgang	3
1.1. Skift af kodeord / e-mail	3
1.2. Mistet kodeord	3
1.3. Opret adgang til en ny bruger	3
2. Statistik og Log søgning	4
2.1. Statistikrapport (online)	4
2.2. Statistikrapport til e-mail	4
2.3. Log søgning	4
3. Opsætning af restriktioner	5
3.1. White- og Blacklisting	5
3.2. Blokering af filtyper	5
3.3. Begrænsning på e-mail størrelser	5
4. Spam karantæne	6
4.1. Karantæne området	6
4.2. Hvilke filer ryger i karantæne	6

1. Log ind og adgang

På <https://www.spamfilter.io> kan du logge ind i dit online kontrolpanel.



Som brugernavn skal du benytte dit domænenavn. Hvis du har flere domæner tilknyttet til den samme løsning, skal du benytte det som blev oplyst ved oprettelsen af din løsning.

Som kodeord skal du første gang benytte det autogenerated kodeord, som du fik ved oprettelsen af din løsning.

1.1. Skift af kodeord / e-mail

Når du er logget ind i dit online kontrolpanel, kan du klikke på ikonet "Brugerens profil". Her kan du vælge at skifte dit kodeord og din tilknyttede e-mail adresse.

1.2. Mistet kodeord

Hvis du har mistet dit kodeord, bør du kontakte vores kundeserviceafdeling.

1.3. Opret adgang til en ny bruger

Du kan give flere brugere adgang til det online kontrolpanel, ved at klikke på knappen Administrer email-brugere. Her skal du klikke på Tilføj for at tilføje brugere enkeltvis, eller du kan uploade en liste som CSV-fil.

Bemærk!: Nye brugere har som standard kun adgang til de mest basale funktioner, såsom:

- Frigivelse af e-mails fra karantæne
- Whitelisting
- Log søgning
- m.m.

2. Statistik og Log søgning

2.1. Statistikrapport (online)

Ved at klikke på ikonet Domæne statistik, er det muligt på domænebasis at generere statistik over mængden af modtaget spam, e-mails generelt og lignende fra time til time.

2.2. Statistikrapport til e-mail

Som domæneadministrator har du adgang til at oprette 3 forskellige slags rapporter

1. En manuel spamrapport, der kan sendes til en valgfri e-mailadresse, og som viser, hvilke e-mails der er blokeret på domænet. Modtageren kan frigive de blokerede e-mails direkte fra rapporten.
2. En periodisk spamrapport (domæne), der viser, hvilke e-mails der er blokeret på domænet. Rapporten udsendes automatisk (dagligt eller ugentligt) til en specifik modtager, som kan frigive de blokerede e-mails direkte fra rapporten.
3. En periodisk spamrapport (bruger), der viser, hvilke e-mails der er blokeret. Rapporten udsendes automatisk (dagligt eller ugentligt) til den enkelte bruger, som kan frigive sine egne blokerede e-mails direkte fra rapporten.

Vi anbefaler sidstnævnte type af rapport i de tilfælde, hvor brugerne selv skal have lov til at administrere filtret.

2.3. Log søgning

Det er muligt at søge blandt alt ind- og udgående post, som er løbet igennem Spamfilter systemet. Via et af de to forskellige Log søgning ikoner, kan du tilgå en oversigt over henholdsvis alle sendte og modtagede e-mails.

Alle e-mails er tydeligt klassificeret, med henblik på om de er blevet accepteret eller blokeret.

3. Opsætning af restriktioner

3.1. White- og Blacklisting

Det er muligt at opsætte lister for, hvilke modtagere og afsendere som skal kunne omgå Spamfilteret, og som derved aldrig vil få blokeret e-mails af systemet, ved hjælp af en såkaldt whitelist. På samme måde er det muligt at opsætte lister for, hvilke modtagere og afsendere som altid vil blive blokeret, uanset indholdet af de sendte e-mails, ved hjælp af en blacklist.

For at oprette whitelists, skal du klikke på ikonerne Afsender whitelist og Modtager whitelist, og tilføje de e-mail adresser som skal på din whitelist.

For at oprette blacklists, skal du klikke på ikonerne Afsender blacklist og Modtager blacklist, og tilføje de e-mail adresser, som skal på din blacklist.

3.2. Blokering af filtyper

Via ikonet Blokerede fil-typer kan du tilføje kendte fil-endelser, som du ønsker altid skal blive opsnappet af Spamfilteret. Som standard er der listet en række kendte filtyper, som oftest er de der anvendes ved spredning af vira og lignende.

Bemærk! Ved at anvende denne funktion, er der stor risiko for at blokere for e-mails, som ikke skulle have været blokeret.

3.3. Begrænsning på e-mail størrelser

Via ikonet Maksimal e-mail størrelse er det muligt at sætte en begrænsning på hvor mange kilobyte en e-mail må fylde, for at blive sluppet igennem Spamfilteret.

Bemærk! Ved at anvende denne funktion, er der stor risiko for at blokere for e-mails, som ikke skulle have været blokeret. Specielt billeder kan risikere at fylde flere tusinde Kilobytes.

4. Spam karantæne

4.1. Karantæne området

Alle e-mails som bliver blokeret af dit Spamfilter, vil fremgå i dit karantæne område, som kan tilgås via ikonet Spam karantæne. Her er det muligt at frigive eller slette e-mails. Hvis du frigiver en e-mail, vil den blive leveret som oprindeligt planlagt til den pågældende modtager.

Da der som oftest fremgår rigtig mange e-mails på denne liste, kan du via søgefunktionen i toppen af siden, vælge at søge på f.eks. en specifik modtager eller enkelte ord fra emnefeltet.

4.2. Hvilke filer ryger i karantæne

Via ikonet Filtrerings indstillinger kan du definere en række indstillinger for dit Spamfilter, med henblik på i hvilket omfang at e-mails skal sendes i karantæne.

Hvis karantæne ikke er slået til, så vil blokerede e-mails blot blive slettet og afvist.

Karantæne filtrerings score definerer hvor mange e-mails, som skal defineres som SPAM. Hvis den står på 1.0, så blokerer Spamfilteret kun e-mails som den er 100% sikker på er SPAM. Hvis den bliver sat lavere, så vil den også på trods af usikkerhed blokere en række e-mails.

Spam score definerer hvor sikker systemet skal være på at en e-mail er SPAM, førend det tilføjer en valgfri tekst i emnefeltet. Det kunne f.eks. være ** Denne e-mail indeholder måske spam **. Teksten kan defineres i feltet der hedder Usikker notation.

Undlad et SPF checks og Undlad at tjekke på max linje-længde bør kun anvendes af øvede brugere.

Karantæne svar bestemmer hvilken notifikation afsenderen af en e-mail, som bliver klassificeret som SPAM skal have - dvs. om han skal vide, at den er blevet blokeret.