

# Antispam drifting i stor skala

Gjennom et studie av norske  
utdanningsinstitusjoner

Erling O. Hauge



Masteroppgave  
Master i informasjonssikkerhet  
30 ECTS  
Institutt for informatikk og medieteknikk  
Høgskolen i Gjøvik, 2005



Masterprogrammet i informasjonssikkerhet  
har blitt kjørt i samarbeid med  
Kunliga Tekniska högskolan (KTH),  
Stockholm, Sverige

Institutt for  
informatikk og medieteknikk  
Høgskolen i Gjøvik  
Postboks 191  
2802 Gjøvik

Department of Computer Science  
and Media Technology  
Gjøvik University College  
Box 191  
N-2802 Gjøvik  
Norway

## **Forord**

Denne rapporten er skrevet som masteroppgave i forbindelse med informasjonsikkerhetsstudiet på Høgskolen i Gjøvik våren 2005. Jeg har valgt en oppgave med spam som tema siden det er et viktig tema innen informasjonsikkerhet samt at det er et betydelig problem for den allmenne databruker.

Jeg vil takke min veileder dr. Erik Hjelmås for tilbakemeldinger og veiledning underveis. Jeg vil også takke førstelektor Frode Volden for støtte med statistikk og kommentarer.

Erling Olai Hauge juni 2005.

## **Abstract**

*Unsolicited Bulk E-mail (UBE) known as spam is a growing problem. Spam became first register as a problem in 1975 and described in RFC 706[1], but have the 10 last years been a prevalent and common problem for big fragments at inhabitants. The fight against spam takes place today at a many plan, with laws, technical mechanism's and user behavior.*

*This studies show digest above possible methods to combat spam at, and I've made a digest above different spamfilter-techniques.*

*I've accordingly analyzed by interview how the fight against spam is executed against the norwegian educational establishment for higher education, to find flaws and fails with the todays system. The study demonstrate improvement potential at many ranges.*

*Keywords: Spam, Junk emails, Unsolicited commercial emails, Unsolicited bulk emails, Cyberlaw, Internet law and CAN-SPAM*

## **Sammendrag**

*Uønsket uoppfordret masseutsendelse av e-post, spam, har økt og blitt et betydelig problem de siste årene. Spam ble først registrerte som et problem i 1975 og beskrevet i RFC706[1], men har de 10 siste årene blitt et vanlig og allment problem for store deler av befolkningen. Bekjempelsen mot spam foregår i dag på mange plan, ved lover, tekniske innretninger og adferdsendring.*

*Studien viser en oversikt over mulige måter å bekjempe spam på, samt at jeg har laget en oversikt over forskjellige spamfilterløsninger.*

*Jeg har deretter undersøkt gjennom intervju hvordan spambekjempelsen er utført ved de norske utdanningsinstitusjonene for høyere utdanning, for å finne svakheter og mangler med det nåværende systemet. Studien viser forbedringspotensialer på flere områder.*

*Nøkkelord: Spam, Junk emails, Uoppfordret kommersiell e-post, Uoppfordret bulk e-post, Cyberlover, Internet lover og CAN-SPAM*



## Innholdfortegnelse

Forord.....	3
Abstract.....	4
Sammendrag.....	5
Innholdfortegnelse.....	7
Liste over figurer og tabeller.....	10
1 Innledning.....	11
1.1 Tema.....	11
1.2 Problemstilling.....	11
1.3 Begrunnelse, motivasjon og gevinstpotensial.....	12
1.4 Forskningsspørsmål.....	12
1.5 Sammendrag av antatte bidrag.....	12
1.6 Metodevalg.....	13
1.6.1 Er det behov for strengere norske spam lover?.....	14
1.6.2 Fungerer dagens spam løsninger tilfredsstillende for de store aktørene på det norske markedet ?.....	14
1.6.3 Tar dagens høgsoler og universiteter det ansvaret som de burde for å stanse spam?.....	14
1.6.4 Hvilke tiltak har mest effekt for å redusere spam for de store aktørene på det norske markedet ?.....	14
1.7 Oversikt over kapitlene.....	14
2 Spam Teori.....	17
2.1 Definisjon av spam.....	17
2.1.1 Nivå av Spam.....	17
2.2 Hvilke lover omhandler spam?.....	18
2.2.1 Lovlige e-postlister og ulovlige spammlister.....	18
2.2.2 Registrere seg på en e-postliste (Opt-In).....	18
2.2.2 Trekke seg fra en e-postliste (Opt-out).....	19
2.2.3 USA (United States of America).....	19
2.2.4 EU (European Union).....	20
2.2.5 Norge.....	20
2.2.6 Hvilke land sender ut e-postspam ?.....	21
2.3 Hvilke tiltak finnes for å redusere e-postspam?.....	22
2.3.1 Kjemp på alle områder.....	23
2.3.2 Best Practice.....	24
2.3.3 Nett-ettikette.....	24
2.3.4 Betalingsmetoder.....	25
2.4 Hvordan fungerer dagens spamfilter?.....	26
2.5 Plassering av spamfilter.....	26
2.5.1 Spam filtrering på klient.....	26

2.5.2 Spam filtrering på server.....	27
2.6 Real-time Spam Black Lister (RBL).....	27
2.7 Known spammers lister.....	28
2.8 Open relay lister.....	28
2.9 Svartelisting.....	28
2.10 Hvitlisting.....	28
2.11 Grålisting .....	28
2.12 Innholdsbaserte filtrering.....	30
2.12.1 Regelbasert filtrering.....	30
2.12.2 Statistiske filtrering.....	30
2.12.3 Bayesian.....	30
2.12.4 Markovian.....	31
2.13 Hvilke metoder bruker spammeren for å finne din e-postadresse ?.....	31
2.14 Hvilket merarbeid påfører spam brukeren ?.....	31
2.15 Spam filterenes logiske oppbygning.....	32
3 Relatert arbeid.....	33
3.1 Undersøkelser.....	33
3.2 Artikler .....	35
4 Vurdering av intervju.....	37
4.1 Overføring av kunnskap.....	37
4.2 Gjennomføring av intervjuene.....	37
4.3 Formålet/vurdering av spørsmålene:.....	37
4.3.1 Generelle spørsmål.....	37
4.3.2 Spørsmål om kompetanse.....	38
4.3.3 Spørsmål om risiko.....	39
4.3.4 Spørsmål om spamfilter.....	39
4.3.5 Spørsmål om prioritering.....	41
4.3.6 Spørsmål om lover og regler.....	42
4.3.7 Spørsmål om tiden fremover.....	43
5 Presentasjon og Vurdering av data fra Intervju.....	45
5.1 Datagrunnlaget.....	45
5.2 Presentasjon av data.....	45
5.2.1 Spørsmål nr 6:.....	46
5.2.2 Spørsmål nr 7:.....	47
5.2.3 Spørsmål nr 8:.....	48
5.2.4 Spørsmål nr 9.....	49
5.2.5 Spørsmål nr 10.....	50
5.2.6 Spørsmål nr 11.....	51
5.2.7 spørsmål nr 14.....	52
5.2.8 Spørsmål nr 15.....	53
5.2.9 Spørsmål nr 16.....	54



5.2.10 Spørsmål nr 17.....	55
5.2.11 Spørsmål nr 18.....	57
5.2.12 Spørsmål nr 19.....	58
5.2.13 Spørsmål nr 20.....	59
5.2.14 Spørsmål nr 21.....	61
5.2.15 Spørsmål nr 22.....	62
5.2.16 Spørsmål nr 23.....	63
5.2.17 Spørsmål nr 24.....	64
5.2.18 Spørsmål nr 25.....	65
5.2.19 Spørsmål nr 26.....	66
5.2.20 Spørsmål nr 27.....	67
5.2.21 Spørsmål nr 28.....	68
5.2.22 Spørsmål nr 29.....	69
5.2.23 Spørsmål nr 30.....	69
5.2.24 Spørsmål nr 31.....	72
6 Diskusjon.....	73
6.1 Risiko faktorer som fører til økt spam mengde.....	73
6.2 Vurdering av forskningsspørsmål.....	75
6.2.1 Er det behov for strenge norske spam lover?.....	75
6.2.2 Fungerer dagens spam løsninger tilfredsstillende for de store aktørene på det norske markedet ?.....	78
6.2.3 Tar dagens høgschooler og universiteter det ansvaret som de burde for å stanse spam?.....	79
6.2.4 Hvilke tiltak for å redusere spam har mest effekt for de store aktørene på det norske markedet ?.....	80
6.3 Oppsett på ideelt system.....	81
6.4 Ethiske og lovlige betraktninger.....	82
7 Konklusjon og videre arbeid.....	83
7.1 Konklusjon.....	83
7.2 Videre arbeid.....	83
Appendiks I Spam-Spørreskjema for utdanningsinstitusjonene.....	89
Appendiks II Tips for å redusere spam.....	93
Appendiks III Data fra intervju.....	95

## Liste over figurer og tabeller

Tabell 1 Metodevalg for forskningsspørsmålene	13
Tabell 2 Land som utsender spam i 2005 Kilde:Sophos Plc.	20
Tabell 3 Oversikt over tiltaks metoder delt i 2 hovedgrupper	22
Tabell 4 Undersøkelse av IKT arbeidere i forhold til spam	32
Illustrasjon 1 Oversikt over utdannelsen til de ansatte	45
Illustrasjon 2 Oversikt over erfaringen til de ansatte	46
Illustrasjon 3 Oversikt over student boliger som er tilknyttet nettverket	47
Illustrasjon 4 Oversikt over trådløse nettverk som er tilknyttet nettverket	48
Illustrasjon 5 Oversikt over hvilke spamfilter som ble brukt	49
Illustrasjon 6 Oversikt over hvilken type spamfilter som ble brukt	50
Illustrasjon 7 Oversikt over hvor mange som out-sourcet e-post driften sin	51
Illustrasjon 8 Oversikt over hvor stor prosent spam av e-post	52
Illustrasjon 9 Oversikt over hvor stor andel som har en spampolicy	53
Illustrasjon 10 Oversikt over hvem som er forpliktet til å følge spampolicyen	54
Illustrasjon 11 Oversikt over hvordan prioriteringen er hos it-avdelingen	56
Illustrasjon 12 Oversikt over falske positive	57
Illustrasjon 13 Oversikt over falske negative	58
Illustrasjon 14 Oversikt over arbeidstimer som brukes til spam drifting	60
Illustrasjon 15 Oversikt over arbeidstimer som brukes til å holde seg oppdatert	61
Illustrasjon 16 Oversikt over arbeidstimer som brukes til kompetanseheving	62
Illustrasjon 17 Oversikt over hvor stor effekt en tror internasjonale lover har	63
Illustrasjon 18 Oversikt over hvor stor effekt en tror norske lover har mot spam	65
Illustrasjon 19 Oversikt over om en har et system for å oppdage sending av spam	66
Illustrasjon 20 Oversikt over bevisst utsending av spam	67
Illustrasjon 21 Oversikt over ubevisst utsending av spam	68
Illustrasjon 22 Oversikt over tilfredshetsgraden av spamfilter løsningen	69
Illustrasjon 23 Oversikt over hvor lang tid det tar før spamsituasjonen blir bedre	72
Illustrasjon 24 Oversikt over spam mengden for Norge 1 mnd i 2005.	76

## 1 Innledning

Bekjempelse av spam krever enorme ressurser fra arbeidstakere, bedrifter, organisasjoner og privatpersoner i dag. En studie[2] som EU gjorde i år 2001 viste at internettbrukerne kaster bort 10 milliarder Euro årlig på spam. Spam fører til avbrudd i arbeidet til alle leddene ved datakommunikasjon. Dette er et stort problem og berører alle internettbrukere.

### 1.1 Tema

Jeg vil i denne oppgaven presentere informasjon om dagens aktuelle anti-spam teknologi og prøve å finne ut hvor effektiv den er ved å intervju utdanningsinstitusjoner i Norge.

Det har vært nødvendig å innhente kunnskap om informasjonssikkerhet, spam, datakommunikasjon, IKT og statistikk for denne oppgaven.

### 1.2 Problemstilling

Spamproblematikken er omfattende og de fleste som benytter seg av e-post er mer eller mindre berørte av problemet. Dette har ført til at e-post som kommunikasjonskanal har fått en betydelig «støykilde», og ikke fungerer ideelt lenger.

#### **Hvilke hovedutfordringer står universitet og høyskoler overfor i forhold til spamproblemet ?**

Utdanningsinstitusjonene for høyere utdanning håndterer spam og sikkerhet på en strengere måte en mange bedrifter og Internett tilbydere, herretter kalt ISP-er. Noe av denne forskjellen ligger i at ISP-ene tilbyr et kommersielt produkt en tjeneste, som de vil begrense minst mulig. Høgskolene og universitetene begrenser derimot brukernes muligheter og har mer effektive spamtiltak som kommer den daglige driften av nettverket tilgode.

#### **Hypotese:**

Hverken ISP'ene eller høyskolene og universitetene gjør en god nok jobb i forhold til spam i dag.

### **1.3 Begrunnelse, motivasjon og gevinstpotensial**

Denne Msc oppgaven om reduksjon av spam vil samle informasjon om de mest effektive måtene å bekjempe spam på. Ut fra media, fra bedriftsmarkedet og gjennom egne erfaringer har jeg møtt på forskjellige problemer knyttet til spam. Det krever i dag store ressurser for å holde spam mengden på et akseptabelt nivå. Dagens bedriftsledere /IT ledere må jevnlig vurdere om de skal innføre nye tiltak for å redusere spam eller jobbe videre med å utvikle allerede eksisterende tiltak. Ved at disse får økt kompetanse på området vil de kunne ta bedre beslutninger.

Motivasjonene og gevinstpotensialet ved å utnytte informasjon om effekt reduksjon/bekjempelse av spam:

- Mindre irritasjon ved bruk av e-post.
- Mulig bruk av e-post
- Større effektivitet
- Bedre utnyttelse av ressurser og båndbredde
- Lettere å finne egnede spam tiltak, eller tilleggstiltak til de eksisterende tiltakene

Gevinstpotensialet med denne studien vil være størst for personer som sitter og vurderer tiltak for bekjempelse spam, da de riktige og mest effektive valgene kan tas. Vanlige brukere av e-post vil også kunne få flere tips og anbefalinger som vil redusere belastningen med spam.

### **1.4 Forskningsspørsmål**

For å løse problemstillingen har jeg kommet frem til følgende forskningsspørsmål:

- Er det behov for strengere norske spam lover?
- Fungerer dagens spamløsninger tilfredsstillende for de store aktørene på det norske markedet ?
- Tar dagens høyskoler og universiteter det ansvaret som de burde for å stanse spam?
- Hvilke tiltak har mest effekt for å redusere spam for de store aktørene på det norske markedet ?

### **1.5 Sammendrag av antatte bidrag**

Mitt bidrag vil være å samle informasjon rundt temaet spam. Dette vil da føre til at kunnskapen som finnes blir strukturert og satt i sammenheng. På den måten vil flere få nytte av forskningen og arbeidet som er gjort for å bekjempe spam. Dette vil også øke den generelle kunnskapen om temaet.

Kunnskap om hvilke teknikker en bør bruke for å bekjempe spam på best mulig måte vil også økes. En økt forståelse av oppgavene som forventes utført av sentrale knutepunkt, som ISP-er og andre som har mange brukere (f.eks. Utdanningsinstitusjonene) vil oppnås.

Jeg vil samle høgskolers og universiteters erfaringer i spam arbeidet, for å lykkes med dette. Arbeidet vil bli samlet og strukturert, slik at andre kan dra nytte av den erfaringen og kunnskapen som har opparbeidet seg de siste årene.

Bidraget vil kunne gi ny og bearbeidet informasjon til det akademiske miljøet, og erfaringer/oversikter til nettverks og sikkerhets personell/administrasjon.

Oppgaven vil bygge på eksisterende og ny kunnskap som det hele tiden forskes videre på. Innholdet i oppgaven vil derfor ha en begrenset aktualitet, da IT bransjen er under kontinuerlig utvikling.

## 1.6 Metodevalg

Denne rapporten vil i hovedsak anvende kvalitative metoder som analyse og observasjon av datamateriale for å besvare problemstillingen. Den andre hoveddelen av prosjektarbeidet vil være litteraturstudie og dokumentanalyse for om mulig å hente erfaringer fra lignende prosjekter.

<i><b>Forskningsspørsmål</b></i>	<i><b>Metode</b></i>
Er det behov for strengere norske spam lover?	Spørreundersøkelse og litteraturstudie
Fungerer dagens spamløsninger tilfredsstillende for de store aktørene på det norske markedet ?	Spørreundersøkelse
Tar dagens høgskolers og universiteter det ansvaret som de burde for å stanse spam?	Spørreundersøkelse
Hvilke tiltak har mest effekt for å redusere spam for de store aktørene på det norske markedet ?	Spørreundersøkelse og litteraturstudie

Tabell 1 Metodevalg for forskningsspørsmålene

### **1.6.1 Er det behov for strengere norske spam lover?**

En vil også kunne se på mulighetene og effekten dette lov- og regelverket har på den faktiske reduksjon av spam. Her vil en da måtte analysere data over spam mengde før og etter de forskjellige tiltakene(lover og regler) er satt inn mot spam. En vil undersøke datamateriale fra spørreundersøkelsen for å prøve å trekke en konklusjon.

### **1.6.2 Fungerer dagens spam løsninger tilfredsstillende for de store aktørene på det norske markedet ?**

En vil vurdere dataene som kommer fra spørreundersøkelsen og se på effekten av spamløsningene og hvor tilfredsstillende de er.

### **1.6.3 Tar dagens høgskoler og universiteter det ansvaret som de burde for å stanse spam?**

En vil her bruke data fra spørreundersøkelse for å konkludere med om det blir gjort det som burde gjøres. Dette er instanser som sitter i en viktig posisjon ift. spam spredning og utsendelse.

### **1.6.4 Hvilke tiltak har mest effekt for å redusere spam for de store aktørene på det norske markedet ?**

En vil videre se på hvilke tiltak som kan brukes til å få redusert spam mengden. Da tenker en på holdnings endring, bevisstgjøring av brukere osv. Her vil det være et litteraturstudie blant artikler og publisert materiale på området.

Jeg vil også undersøke hvordan dagens spamfiltre fungerer. For å finne ut av dette vil jeg bruke informasjon som er blitt tilegnet i løpet av høsten 2004.

## **1.7 Oversikt over kapitlene**

Kapittel 2 omhandler en introduksjon til forskjellige måter å løse spam problemet på. Jeg viser metoder innen spamfiltrerings teknikk og muligheter som er tilgjengelige ved kunnskap og holdninger som blant annet spam policy.

I kapittel 3 så er det en gjennomgang av relatert arbeid og noen undersøkelser som er gjort på området.

I kapittel 4 gjør jeg en vurdering av intervju spørsmålene som jeg brukte i telefon intervjuet. Dataene blir så presentert og vurdert i kapittel 5. Diskusjon rundt funnene blir gjort i kapittel 6.

Kapittel 7 summerer konklusjonene av studiet som er gjort, og kommer med forslag til videre arbeid som kan bli gjort.





## 2 Spam Teori

### 2.1 Definisjon av spam

Spam i datasammenheng, betyr noe som ikke er ønsket. Det blir vanligvis brukt til å referere til uønsket e-post eller News-meldinger, og blir nå også brukt ved uønsket Instant Messenger (IM) og mobil Short Message Service (SMS) meldinger. Spam e-post er uønsket, ikke invitert og ofte reklame for å selge noe.

For å referere til e-post spam brukes ofte de engelske uttrykkene:

- Junk E-mail er oversatt til: søppel e-post
- Unsolicited Bulk E-mail (UBE) er oversatt til: uoppfordret masseutsendt e-post
- Unsolicited Commercial E-mail (UCE) er oversatt til: uoppfordret kommersiell e-post
- Opt-Out er oversatt til: trekke seg fra en e-postliste
- Opt-In er oversatt til: registrere seg på en e-postliste.

Personer eller firmaer som sender ut spam blir kalt spammere (eng.: spammers). Bedrifter betaler gjerne profesjonelle spammere for å sende ut reklame-e-post til potensielle kunder.

#### 2.1.1 Nivå av Spam

Den generelle definisjonen av e-post-spam er ikke særlig presis. Jeg vil utvide den generelle oppfatningen av spam til å inkludere følgende, i stigende alvorlighetsgrad:

Nivå 1: E-postspam fra venner, fra en til mange

Nivå 2: E-postspam fra venner, kjede brev, ofte veldedighet eller økonomisk rettet

Nivå 3: E-postspam fra kjente avsendere som sender reklame

Nivå 4: E-postspam fra falske avsendere som sender ut reklame (ulovlig iht norsk lov)

Nivå 5: E-postspam fra falske avsendere som sender ut virus o.l.(ulovlig iht norsk lov)

## **2.2 Hvilke lover omhandler spam?**

Vedkommende som sender spam kan sitte i ett land, og mottakerne i helt andre land. Det er viktig at lovene blir internasjonalisert og samkjørt mellom landene. Lover og regler som alle må forholde seg til vil være de mest effektive. Der er viktig at personvernrettighetene blir ivaretatt ved internasjonal lovgivning.

### **2.2.1 Lovlige e-postlister og ulovlige spamlister**

E-post fra e-postlister er ofte viktig for både mottaker og sender. Viktig for sender for å ha et godt kundeforhold, og for mottakeren som kan få informasjon om produkter og tilbud.

Forskjellen mellom lovlig utsending fra en e-postliste og e-postspam er klar. Den som sender ut lovlig-post, har fått samtykke om at vedkommende ønsker å motta slik informasjon på e-post, mens en spammer ikke har fått slikt samtykke.

### **2.2.2 Registrere seg på en e-postliste (Opt-In)**

Bekreftet registrering skal alltid være til stede ved en registrering. Mottakeren har da bekreftet at han ønsker å stå på den aktuelle listen. Denne bekreftelsen er gjort ved at mottakeren svarer på e-posten om «bekreft registrering» som utseender må få bekreftet før en registrering er fullført.

Detter er standard fremgangsmåte for alle Internett e-postlister, det sikrer at alle er registrerte med en fungerende og gyldig adresse med brukerens samtykke.

Følgende begreper blir også brukt:

- Opt-In: Når en bruker ikke har trekt seg fra en e-postliste, da er vedkommende på listen.
- Dobbelt-Opt-In: Når en bruker har registrert seg to ganger. En første når en e-postadresse ble registrert, og den andre gangen når vedkommende ikke trakk seg fra e-postlisten(opt-out) når vedkommende fikk e-postspam.
- Trippel-Opt-In: Når en person som registrer i tillegg oppgir navn, adresse og interesser.

### **2.2.2 Trekke seg fra en e-postliste (Opt-out)**

Det skal være enkelt å trekke seg fra en e-postliste. Dette skal kunne gjøres ved å henvende seg til den legitime avsenderen av e-posten.

E-postspam kan komme som med «opt-out» uten at en har registrert seg «opt-in» i utgangspunktet. Masseutsendt e-post som er sendt uten at mottaker har eksplisitt registrert seg «opt-in» med sin e-postadressen på den aktuelle listen og som krever at mottakerne må melde seg av listen for å ikke motta flere e-poster, er da e-postspam (UBE Opt-Out) nivå 4 eller 5.

### **2.2.3 USA (United States of America)**

USA fikk CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing)[3] loven som trådte i kraft fra 1. januar 2004. Den forbyr spredning av uønsket masse-reklame, og har gitt flere selskaper mulighet til å saksøke den/de som står bak slike utsendelser. Det siste året er det ført flere rettsaker i USA med bakgrunn i den amerikanske CAN-SPAM[3] loven.

I motsetning til europeisk lovgivning som krever at det innhentes tillatelse fra mottakeren før man sender e-postreklame, krever CAN-SPAM bare at avsenderen ikke skal skjule sin identitet, og at e-posten skal inneholde en ordning som mottakeren kan klikke på dersom man ikke ønsker å motta den typen e-post i framtida (Opt-out). Derfor oppfattes CAN-SPAM mer som en tillatelse til å spamme enn som et helhjertet antispamtiltak. Flere delstater, blant dem California, hadde innført lover med det europeiske prinsippet om forhåndstillatelse, men måtte droppe dem da CAN-SPAM kom.

Det ble understreket da loven ble vedtatt at den måtte håndheves strengt for å være effektiv. Loven gir ikke privatpersoner adgang til å saksøke spammere.

Blant dem som har fulgt virkningen av Can-Spam gjennom hele 2004 er MX Logic som har spesialisert seg på filtreringstjenester for det amerikanske bedriftsmarkedet. Selskapet anslår at 77 prosent av all e-posttrafikk i 2004 er spam, og at 97 prosent av all spam bryter Can-Spam-loven. I november var det visse tegn til bedring, da andelen lovlydig spam nådde 6 prosent.

USAs konkurransemyndighet FTC (Federal Trade Commission) fikk i 2004 medhold i en rett i delstaten Nevada for et krav om øyeblikkelige tiltak mot seks selskaper og fem individer som er anklaget for brudd på spam-loven Can-Spam. Avgjørelsen innebærer

at retten og myndighetene er enighet om at man er juridisk ansvarlig også for den markedsføringen som overlates til tredje part.

Spammen som reklamerte for de anklagedes varer tjenester brøt Can-Spam på flere punkter. Den fulgte blant annet ikke påbudet om å ha ordene «sexually explicit» øverst i meldingene, og den hadde ikke lenker for å la mottakeren stryke seg fra distribusjonslisten.

#### **2.2.4 EU (European Union)**

I EU har de siden 2000 jobbet med en ny lovgivning om personvern som inneholder blant annet sterkere vern mot spam, utgangspunktet var: "E-Privacy Directive Proposal COM(2000) 385" [4]. Denne ble i sin ferdigstilling kalt «DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT» [5] og alle medlemslandene var pliktige til å implementere loven innen 31. Oktober 2003. Vedtak er bare fulgt opp av Danmark, Irland, Italia, Spania, Storbritannia og Østerrike. De resterende medlemslandene Belgia, Finland, Frankrike, Hellas, Luxemburg, Nederland, Portugal, Sverige og Tyskland fikk en advarsel fra EU-kommisjonen - at de må oppgi hvordan de har tenkt å etterkomme vedtaket innen to måneder. Ellers vil de kunne trekkes for en EU-domstol.

I tillegg til å kreve at mottaker av e-post har bedt om å få reklame, setter også EU-direktivet klare begrensinger for bruke av cookies (informasjonskapsler).

Direktivet går mye lenger enn USAs relativt ferske antispam-lov, som tillater uønsket reklamepost så lenge innholdet ikke strider mot lov eller moral og mottakeren enkelt og effektivt kan gi bskjed om at hun eller han ikke ønsker posten for framtida.

#### **2.2.5 Norge**

I Norge fikk vi den 1. mars 2001 implementert et forbud av markedsføring via e-post i markedsføringsloven. Under § 2b. *Begrensninger i bruk av visse kommunikasjonsmetoder*[6], står det: «Det er forbudt i næringsvirksomhet uten mottakerens forutgående samtykke å rette markedsføringshenvendelser til forbrukere ved hjelp av elektroniske kommunikasjonsmetoder som tillater individuell kommunikasjon, som for eksempel elektronisk post, tekstmelding til mobiltelefon, telefaks».

Den norske loven ble skjerpet inn i februar 2005 på bakgrunn av EU-direktivet om personvern og elektronisk kommunikasjon. Det ble innført begrepet fysiske personer, som fører til at heller ikke arbeidstakere og næringsdrivende skal få uanmodet e-

postreklame til individuelle e-postadresser. Dette fører til at det nå blir like strenge regler i hele EØS-området.

Det kommer også en ny regel om unntak fra kravet om forhåndssamtykke når man driver epostmarkedsføring til egne kunder. Kundene skal likevel på en enkel og kostnadsfri måte kunne be seg fritatt for slik reklame.

Hovedforandringen er at det er blitt forbudt å sende uønsket reklame e-post til jobbe-post adresser, før gjaldt bare private e-postadresser.

### 2.2.6 Hvilke land sender ut e-postspam ?

I artikkelen «Sophos reveals latest "Dirty Dozen" spam producing countries» [7] fra IKT-sikkerhetsselskapet Sophos Plc. i USA, offentliggjør de tall som viser hvilke land som sender ut mest spam. Tallmaterialet kommer fra Der ligger USA på førsteplass med 42,53% i august 2004. I deres nye artikkel «Sophos reveals latest "Dirty Dozen" spam producing countries»[8] som kom i april 2005 viser den at USA har nå falt ned til 35,70%.

Land	% spam
1 USA	35.70%
2 Sør Korea	24.98%
3 Kina (inkludert Hong Kong)	9.71%
4 Frankrike	3.19%
5 Spania	2.74%
6 Canada	2.68%
7 Japan	2.10%
8 Brasil	1.95%
9 Storbritannia	1.57%
10 Tyskland	1.23%
11 Australia	1.22%
12 Polen	1.20%
Andre	11.73%

Tabell 2 Land som utsender spam i 2005 Kilde: Sophos Plc.

Prosentvis så kan en se at de store landene i EU som Storbritannia, Spania og Frankrike har økt fra august 2004 til april 2005.

Sør-Korea som ligger på andreplassen over land som sender t spam har økt i tidsintervallet fra 15,42 til 24,98.

Flere amerikansk IKT-sikkerhets selskap hevder at CAN-SPAM loven ikke har vært tilfredsstillende, da spam mengden fortsatt er betydelig.

### **2.3 Hvilke tiltak finnes for å redusere e-postspam?**

Tiltakene kan deles inn i to hovedtyper:

1. Unngå at spam kommer til brukeren
2. Redusere spam mengden som blir sendt

Noen av tiltakene benytter seg av begge hovedtypene for å bekjempe e-postspam

Tiltak:	Tiltaks metode:	
	1	2
«Kjemp på alle områder»	X	X
Best practice	X	X
Nett-ettikette	X	X
Betalingsmetoder	X	X
Real-time Spam Black Lister (RBL)	X	
Known spammers lister	X	
Open relay lister	X	
Svartelisting	X	
Hvitlisting	X	
Grålisting	X	
Regelbasert	X	
Innholdsbaserte	X	
Statistiske filter	X	
Lover og regler		X

Tabell 3 Oversikt over tiltaks metoder delt i 2 hovedgrupper

### 2.3.1 Kjemp på alle områder

B. Leiba og N. Borensteinl[9] hevder at det ikke er *ett* rett svar eller *én* måte som er den mest effektive, men at en må ha tiltak på flere lag for å klare å redusere spam på en effektiv og fremtidsrettet måte. De ser de for seg følgende lag:

- Personlige og organisasjoners preferanser
- Klassifisering og filtrering
- Hvit- og svartlisting, og spamsamlere
- Betaling
- Identitet -autentisering, sertifisering og sporbarhet
- Utfordring/ responssystem, der en krever noe fra brukeren
- Lover og regler

De oppfordrer også til å bruke felles standarder og felles prosedyrer for å bekjempe spam.

### 2.3.2 Best Practice

Best Practice[10] foreslår å følge «best practice» -metoder for å redusere spam best mulig. Best Practice har laget anbefalinger til følgende arbeidsgrupper:

- Stamnett tilbydere & båndbredde selgere (engelsk forkortelse:BPR)
- Internet tilbydere (engelsk forkortelse:ISP)
- Web tjenestertilbyder (engelsk forkortelse:WHS)
- E-postliste tjenestertilbyder (engelsk forkortelse:LHS)
- Søke motorer & Kataloger (engelsk forkortelse: SED)
- Gratis web E-post funksjonalitet (engelsk forkortelse:FWE)
- Gratis webside tilbyder (engelsk forkortelse:FHS)
- Telefon/Fax til e-post tjenester (engelsk forkortelse:P2E)
- Web/E-post til fax tjenester (engelsk forkortelse:W2F)
- Tredjeparts skripting tjenestetilbyder(engelsk forkortelse:3SH)
- Andre gratis web tjenester (engelsk forkortelse:FWS)
- Programtilbehør behandlere (engelsk forkortelse:APM)
- Kolega program for tilsluttet organisjon (engelsk forkortelse:APA)
- E-post liste utgiverer (engelsk forkortelse:MLP)
- Internett utforsker programvare utviklere (engelsk forkortelse:BSD)
- E-post klient software utviklere (engelsk forkortelse:ECS)
- E-post server programvare utviklere (engelsk forkortelse: ESS)
- Media oppkjøpere (engelsk forkortelse:MBY)
- Domene Navne Registratorer (engelsk forkortelse:DNR)
- Webansvarlige / Web designere

Der et av de viktigste budskapene de prøver å formidle er bevisstgjøring av problemet og det ansvaret som ligger på den enkelte for å stanse spam. De tar også frem behovet for overvåking av eget nett for å vite hva som sendes. Kunnskap og veiledning har de gitt ut og har vært tilgjengelig fra år 2000.

### 2.3.3 Nett-ettikette

Ved å følge nett-ettikette som beskrevet i RFC 1855 [11] så kan spam bli unngått i utgangspunktet. Hovedproblemet er at spamerene ikke følger nett-ettikette som beskrevet på denne RFC'en.

Både nett-ettikette og «best practice» er måter en får redusert spam på hvis alle hadde fulgt de. I dag er det filtreringsmetoder og betalingsmetoder utenom lover som blir vurdert som de beste alternativene på kort sikt.



### 2.3.4 Betalingsmetoder

David A. Turner and Daniel M. Havey[12] beskriver en betalingsmetode, en protokoll som er enkel å implementere i dagens system, og som vil kunne kreve betaling av brukerne av e-post i det aktuelle systemet. Alle må da inkludere dette systemet, eller et tilsvarende for å få den tenkte effekten. David A. Turner and Daniel M. Havey mener at dagens filtre bare er et steg mot målet og ikke en løsning av spam på sikt. Filtring av e-post tar først av seg problemet etter at det er oppstått.

Aashin Gautam[13] viser en annen måte å implementere inn en portokoll for å få betalt for e-post. Utgangspunktet er at det koster en «e-krone» for å sende en e-post. Alle brukerne av en e-post server får da x antall e-kroner hver. Disse kan en da bruke til å sende x antall e-post. Hver gang en bruker sender eller mottar en e-post minke eller øker antall e-kroner på kontoen. Ekstra e-kroner kan bli skaffet fra deltakenede e-banker, som muliggjør kjøp og salg av e-kroner. Det er da tre parter i et slikt system; sender, mottaker og e-banken. Dette systemet har følgende egenskaper:

- Null sum: Et hver transaksjon ved dette systemet vil vise at det er balanse mellom e-kroner ut og e-kroner inn.
- Returner bare e-kroner: Når en e-post er mottatt så vil, mottakerens balanse av e-kroner øke og senders balanse minke. Mottakeren har da valget med å returnere e-kroner tilbake ved å sende svar på e-posten som ble mottatt.
- Gjennbruk av e-kroner: E-kronene som er opptjent ved mottaking av e-post kan brukes direkte for å sende ut e-post. Systemet kan også settes opp til å nullstilles hvert døgn med et gitt antall e-kroner til hver bruker.
- Konventerbart til penger: E-kronene som er opptjent ved å motta e-post kan brukes til å veksle dem inn i e-banken til lokal valuta. Som fører til at brukeren blir betalt direkte for tiden de bruker på spam.
- Usynlig for brukeren: Vanlig bruk av e-post vil ikke forandres noe ved å implementer dette systemet. En vil ikke måtte forholde seg til til e-kroner før en begynner å sende ut mye mer e-post en en mottar. En kan ikke smale opp e-kroner over tid.

Betalingsmetoder som krever at brukeren må gjøre et arbeid, eller retttere sagt dens datamaskin, fins det flere av. En av disse er Microsofts Penny Black Project [14]. Her skal CPU'en arbeide i ca 20 sekunder for hver e-post som blir sent. Dette vil da være en liten eller ingen særlig ulempe ved sending av et lite antall e-poster. Det store utslaget blir da for spammere som sender ut veldig store mengder e-post. Ved et eventuelt slikt system så vil det «koste» for mye i form av CPU tid for spammerene til å få sent ut spam i de mengdene som de gjør i dag.

For at det ikke skal være stor forskjell ved bruk av kraftige high end systemer, i forhold til snart utdaterte datamaskiner på tiden det tar å utføre en komplisert regneoperasjon for prosessoren har problemet blitt løst av Martin Abadi, Mike Burrows, Mark Manasse, og Ted Wobber[15] ved bruk av Memory-bound funksjoner.

## 2.4 Hvordan fungerer dagens spamfilter?

Dagens spamfiltre fungerer hovedsaklig etter to prinsipper, statiske og statistiske filter. De tidlige filtrene var statiske og hadde flere ulemper mot de nyere statistiske.

Filterene sjekker om det som kommer i innboksen er gyldig e-post eller spam. Filteret kan ta feil på sin vurdering og en kan da komme opp i følgende situasjoner:

- positive (e-post), e-post som er e-post og blir godkjent som e-post
- falske positive – blir gjenkjent som e-post, men er e-postspam
- negative (e-postspam), e-post som er e-postspam og blir godkjent som e-postspam
- falske negative- blir gjenkjent som e-postspam, men er e-post

### **Konsekvens av feilvurdering av e-post.**

Konsekvensene av feilvurdert e-post kan være store. Ved å få falske positive så vil det ikke ha så stor konsekvens, utenom å være til irritasjon og tidstyveri. Derimot kan konsekvensene ved falske negative være relativt store.

Konsekvens ved:

- Falske positive er irritasjon, spam i innboksen.
- Falske negative er tapte e-poster, som kan ha høy konsekvens. Tap av e-post betyr at informasjonen kan være borte for alltid eller for en gitt tid. Noe som anses som en mye mer katastrofal konsekvens enn irritasjonen ved å få litt spam i innboksen.

## 2.5 Plassering av spamfilter

En kan redusere spam problemet ved bruk av spamfilter som har følgende plassering:

- På server siden
- På klient siden
- Kombinert på server og klient

### 2.5.1 Spam filtrering på klient

Ved spamfiltrering på klientsiden når all spam helt frem til mottakeren før den blir vurdert, noe som belaster nettverket. Da kjøres enten et eget spamfilter, slik som spampal[16]. En slik løsning sitter mellom e-post programmet og innboksen og

sjekker e-posten. Så tar programmet og merker all e-post som den tror er spam i emnefeltet. En setter så opp e-postklienten til å flytte alle e-poster med dette merket over i en egen katalog. En kan bruke spampal hvis en har en standard POP3 eller IMAP4 e-postadresse sammen med en e-postklient som Outlook, Outlook Express eller Eudora.

På nyere e-postklienter er det innebygt et spamfilter, dette gjelder blant annet Mozilla Thunderbird, Opera™ og MS Outlook 2003. Spamfiltrering som filtrerer på e-postklienten er lettere å tilpasse individuelle forskjeller, enn hvis det er på serveren. Både Opera og Mozillz Thunderbird har muligheter for at spam filteret lærer av brukerens merking av e-postspam.

### **2.5.2 Spam filtrering på server**

Ved å ha filtrering og fjerning av spam på server så slipper en å belaste internettet med e-postspam mer enn nødvendig. En slik løsning vil i de fleste tilfeller også være lettere å drifte og holde oppdatert.

De fleste anti-spam løsningene som er beregnet for flere brukere (SMB-bedrifter) vil oppnå fordeler med sentralisert filtrering på server.

De fleste open-source og kommersielle løsningene, vil være tilgjengelig i både server og klient utgave.

Typisk så kjører f.eks.open-source anti-spamfilteret SpamAssassin på serveren og vurderer alle e-post som kommer inn til postkontoret, SMTP-serveren. All e-post blir klassifisert etter hvor stor sannsynlighet for at det er gyldig e-post. Det blir f.eks. brukt en gradering fra 1-15, der 0 er e-post og over 8 blir betegnet som spam, SpamAssassin kan da bli satt opp til å slette alle e-post med klassifisering over 12. E-post med klassifisering fra 8-12 blir merket som spam, og sendt til mottaker.

### **2.6 Real-time Spam Black Lister (RBL)**

Et alternativ eller supplement til egne svartelister, er real-time spam svarte lister. En kan abonnere på slike lister. De fleste listene er gratis og enkelte må en betale for. Hver e-post som kommer blir sjekket opp mot RBL'en, noe som tar båndbredde fra nettverket.

## 2.7 Known spammers lister

Slike lister kan blokkere hele domener eller spesifikke ip-adresser, og er oftest statiske og må lastes ned med jevne mellomrom.

## 2.8 Open relay lister

Dette er lister som inkluderer domener som spammerene bruker for å sende/videresende spam fra. Disse listene kan inkludere uskyldige brukere som ikke er klar over at deres e-post server blir brukt til å sende ut spam med.

## 2.9 Svartelisting

Svartelisting fungerer ved at en oppretter en liste over e-post adresser eller SMTP-servere som ikke er godkjente. Alternativt kan en lagre de hashede verdiene av meldingene i et register og sjekke opp mot dette. Det er også mulig å laste ned milliover av spam signaturer hver natt. En hver forandring av meldingen vil føre til en forandring av hashen og føre til at filtrerings metoden feiler, så nesten alle spamere legger ved en random tekst streng for å tvinge frem en forskjelling digital signatur på hver spam e-post som sendes.

Tidligere ble svartelisting brukt som en spamfiltrering teknikk på egenhånd. Nå brukes ofte hvitlisting og svartlisting sammen med andre teknikker for å øke nøyaktigheten til spamfilteret.

## 2.10 Hvitlisting

Hvitlisting er filtrering som fungerer på motsatt måte av svartlistingen, slik som TMEDA[17]. I disse systemene blir all e-post anntatt å være spam hvis ikke meldingen kommer fra en kjent og godkjent sender, eller inneholder en kjent og godkjent passerings frase. Avanserte hvitlisting system vil sende en utfordring til sender når senderen ikke er kjent og godkjent. Hvis senderen svarer passende vil da filterert legge senderen til godkjent listen.

Det er også mulig å bruke bekreftede avsender system (smarte hvitelister) som automatisk legger inn e-postadresser i hvitelisten hvis det blir sendt ut en e-post til vedkommende.

## 2.11 Grålisting

Grålisting av Evan Harris[18] fungerer slik at bare den tålmodige kommer igjennom. En innbiller seg at spamerene er for late til å fortsette å prøve.

Før en aksepterer innkommende e-post så vil e-post serveren se på:

- IP adressen fra hosten som prøver å sende
- Hvem e-posten er fra
- Hvem som skal motta e-posten

Hvis denne kombinasjonen er ny, sender e-postserveren tilbake en foreløpig leveringsfeil(temporary delivery failure).

Lovlige e-postsendere vil prøve igjen. Etter en viss forsinkelse vil e-posten bli akseptert og hvem, hvor, hva -kombinasjonene blir lagt til en hvitliste for en gitt tid.

Spammere vil vanligvis ikke ha programvare konfigurert til å prøve igjen etter å ha mottatt en slik feilmelding fra e-postserveren, siden dette fortsatt er relativt ny teknologi. Dette fører til at spammen aldri kommer frem til mottakeren.

Alle sendere blir første gang informert om den midlertidige feilen.

Hovedfordelene ved grålisting er :

- at en legger en del av ulempen over på spammeren, spesielt på åpne relay pga. at de kontinuerlig må prøve å levere spam. Dette medfører en god grunn for å få de åpne relayene stanset.
- at systemet er relativt transparent for sender og mottaker.

En del av problemene ved grålisting er at den uskyldige part får en del ulemper. Det å ha mange e-poster liggende i kø krever diskplass. All e-post som ikke er hvitlistet enda og går igjennom et gråfilter vil bli bli forsinket.

Hvis forsinkelsen er 1 time, og e-post serveren ikke prosesserer køen kontinuerlig, vil det føre til at en rask e-post utveksling ved f.eks. helpdesk, som uten grålisting ville tatt 15 min kan nå ta 3 timer, på grunn av en « foreløpig leveringsfeil» på begge sider.

Evan Harris[18] forklarer at grålisting baserer seg på den antagelsen at spammeren er lat og at deres e-post servere ikke oppfører seg riktig. Begge antagelsene er sannsynligvis riktige til dags dato. Siden spammerene er avhengig av at deres e-postspam skal bli levert vil de nok i fremtiden løse dette problemet.

Evan Harris sier også at hvis grålisting ble brukt i utstrakt målestokk, vil spamere helt klart følge etter, noe som bare vil føre til at en del e-post, inkludert spam er unødvendig forsinket.

## 2.12 Innholdsbaserte filtrering

Innholdsbaserte filter eller nøkkelord søk er en annen form for filtrering, hvor et sett av ord er definert som "spam merke" og søkt etter i hver innkommende e-post. Hver melding som inneholder nøkkelordet vil da bli slettet uavhengig om det er ekte spam eller ikke. Det er innholdet i både emnefeltet og i selve hoveddelen som blir sjekket. Dette er den vanligste formen for spamfiltre, disse er ofte teknisk enkle for spammerene å unngå ved blant annet følgende teknikker:

- Spammer, kan sende bilder, som ikke vil bli lest av det innholdsbaserte filteret.
- Spammer, kan skrive «feil» og ha en random fremstilling av noe av teksten.

### 2.12.1 Regelbasert filtrering

Heuristisk tilpasset filter bruker en menneskelig ekspert til å komme frem til et sett av trekk som f.eks en string, eller tilstedeværelse i en database. Hver av trekkene har forskjellig vektning, enten menneskelig gitt, eller generert av en algoritme som f.eks. et navralt nett. Nevrale nett er sterkt forenklete modeller av levende organismers hjerne. Hvis en innkommende melding overgår en terskel, det blir frastøtt som spam, hvis ikke så går systemet ut fra at det er OK. Basisen for denne fremgangsmåten er at eksperten sjekker spam og ikke spam meldinger for interessante karakteristiske egenskaper. Derfor blir bare et relativt lite antall trekk (noen få hundre) undersøkt.

### 2.12.2 Statistiske filtrering

Statistiske spamfilter baserer seg på e-postene og metadata om e-postene. De analyserer e-postene ut fra hva de er lært opp til for å prøve å vurdere om en e-post er e-postspam eller ikke. De er veldig effektive etter en innlæringsperiode.

### 2.12.3 Bayesian

Bayesian er dagens "state of the art"-filter, dette er statistiske innholdsbaserte filter . Disse er basert på hyppigheten av enkelte ord som har trekk av interesse. CRM114, Sparse Binary Polynomial Hashing [19] er et slikt filter. En av styrkene til disse filterne er at de gir få falske positive e-poster. En annen styrke er egenskapen til å lære, når brukeren markerer en e-post som gyldig og ikke spam, så lærer filteret det, og husker det til neste gang det kommer en e-post av den typen. Noe som på sikt fører til at nøyaktigheten til filteret vil øke over tid.

#### **2.12.4 Markovian**

Markovian filter[20] baserer seg på en utvidelse og vidererutvikling av grunnegenskapene til Bayesian filteret. Det er ikke bare enkle ord som teller, flere ord samlet blir vektet mer en enkle. Dette fører til en enda høyere treffsikkerhet av rette, samt et lavt antall falske positive og falske negative. CAMRAM[21] er et spamfilter som baserer seg på Markovian teknologien. Eric Johansson [22] ga sine erfaringer om CAMRAM på Spam Conferance 2004. Han vurderte her effekten av filteret opp mot andre filter. Han beskriver de egenskapene som gode, med et veldig lavt antall falske positive og falske negative med dette filteret.

#### **2.13 Hvilke metoder bruker spammeren for å finne din e-postadresse ?**

Matt Bishop [23] beskriver flere teknikker som spammerne bruker for å få tak i e-post adresser. Noen av måtene er:

- Scanning av hjemmesider (www sider)
- Scanning av nyhetsgrupper (news group)
- Oppkjøp av e-post lister /databaser
- Random sending til alle mulige e-post adresser på et domene.
- Tilfeldig kjente navn og kjente etternavn

#### **2.14 Hvilket merarbeid påfører spam brukeren ?**

I mai 2003 ble spam mengden for første gang i historien større enn den legitime e-postmengden. S.J. Vaughan-Nichols[24] forklarte da at mer en 50% av overførte e-poster som var e-postspam, som bruker båndbredde og nettverksressurser som i utgangspunktet skulle vært tilgjengelig for brukeren.

Det blir rapportert fra en engelske spørreundersøkelsen[25] som ble gjort i forkant av konferansen «Infosecurity Europe 2005» at 42 prosent av britiske arbeidstakere sier de har overskredet en tidsfrist fordi en e-postmelding ble stoppet i spamfilteret. To tredeler av respondentene sa de hadde opplevd å få blokkert legitime meldinger som de skulle ha mottatt, og to tredjedeler av disse igjen sa at problemet oppsto minst en gang i måneden, mens en firedel mente det skjedde hver uke.

Brukeren får merarbeid i form av sletting av e-postspam og sortering av falske positive. Selv med spamfilter er dette et daglig problem for de fleste.

Brukerne kan også få et stort merarbeid ved falske negative. Dette problemet er da mye større og tar lenger tid å oppdage. Ofte blir det ikke oppdaget før det allerede er oppstått et problem.

## 2.15 Spam filterenes logiske oppbygning

Filterene bruker vanligvis en algoritme som kan beskrives logisk som dette:

```
if sender {  
  is white listed}  
then email = email
```

```
If sender{  
  is black listed}  
then email = spam
```

```
if content {  
  look like spam}  
then email = spam
```

En kan også bruke flere filter i seriell for å få luket ut mest mulig spam. Dette er en teknikk som flere benytter seg av blant annet open-source spamfilteret SpamAssassin.



## 3 Relatert arbeid

### 3.1 Undersøkelser

I artikkelen «Fed-up users, experts offer spam-fighting tricks»[26] skriver John Hogan om undersøkelsen der 1303 ikt-arbeidere jobber med e-postdrifting. Følgende data ble presentert etter at respondentene ble spurt om: hvor stort er e-postspam problem ditt?

Prosentandel	Beskrivelse av tilstand
48%	Problemet er stort men vi har kontroll på det.
20%	Uholdbart, vi gjør nå drastiske tiltak.
18%	Vi har store problemer og klarer ikke å få «hode over vannet».
12%	Det er ikke så stort problem for oss.

Tabell 4 Undersøkelse av IKT arbeidere i forhold til spam

Dette viser situasjonen i år 2003, 38% svarer at de har problemer som de på det stadiet ikke har en god løsning for. En vil anta at situasjonen er bedre i dag, da de fleste e-postserverene har installert anti-spamfilter de siste årene.

Jerry Berkman gjennomførte en spam-undersøkelse[27] i 2002, hvor han publiserte noen spørsmål på SANS University Security e-postliste, og andre universitets tilsvarende lister. Spørsmålene gikk på hvilke anti-spam systemer de brukte og hadde brukt. Han fikk respons fra personer som var ansvarlige for e-postdriftingen på andre universiteter i USA.

Han oppsummerer med at de fleste ønsker å benytte en spamfilterløsning som den Open Source baserte SpamAssassin eller et kommersielt produkt som PureMessage (tidligere PerlMX) for å merke e-post som e-postspam. Begge produktene lager en poengsum basert på over 150 vanlige uttrykk, i tillegg til at det er mulighet for å legge til black hole lister og spamdatabaser.

Mange av universitets it-avdelinger bruker en black hole liste for å blokkerer e-post fra visse hoster eller i poengsum baserte systemer som SpamAssassin. Respondentene gav uttrykk for at black hole listene ikke alltid var til å stole på.

Generell blokkering og merking av e-post er gjort hos de aller fleste uten at brukeren har noe valg.

IT-sikkerhetsselskapet Trend Micro, Inc. Utførte i 2003 undersøkelsen «*Security and productivity concerns make spam a top IT priority*»[28], blant it-arbeidere og it-beslutningstakerer om deres oppfatning av spamproblemet. Hovedfunnene var :

- Mer en 70 prosent av respondentene mente at en spam epidemi var på gang.
- Mer en halvparten hadde i sin organisasjon opplevd en spam økning på 25-100 prosent de siste 3 månedene.
- Ca. 2/3 er bekymret av nedsatt arbeids effektivitet som følge av at spam tar med seg usikker/ondsinnset kode og virus.
- 1 av 3 respondenter mente at virusproblemer starter fra spam som kommer.
- Spam er blant topp 3 prioriteringer for ca 50 prosent av respondentenes organisasjoner

Forslag til forbedringer ble :

- Å ha et spamfilter ved gateway eller server for hele organisasjonen.
- Velge en spamfilterløsning som har: et bra omdømme, lavt antall falske-positive og lavt antall falske-negative.
- Bruke spamfiltermetoder som: real-time spam black list(RBL) og regelbaserte spamfilterløsninger.

Det var over 200 respondenter der alle representerte nettverkt med flere enn 100 brukere i. Alle respondentene identifiserte seg selv som anti-spam innkjøpsinnflytelsesrike eller -ansvarlige.

The Transatlantic Consumer Dialogue (TACD) publiserte i februar 2004 en rapport [29] om forbrukers holding til e-postspam. TACD er et forum med 65 forbrukerorganisasjoner som utvikler og blir enige om felles anbefalte handels policyer for EU og USA. TACD utførte en online spørreundersøkelse. Over 21 000 respondenter svarte. Holdningene som ble rapportert var:

- 96% sa at de hatet eller ble forstyrret av e-postspam.
- 84% sa at all uoppfordret kommersiell e-post burde vært forbudt.
- 83% sa at de trodde at det meste av all e-postspam er svindel eller bedrag.
- 82% sa at myndighetene ikke burde tillate kommersielle e-poster som ikke er godkjent av mottakeren på forhånd. (Opt-in)

- 80% sa at det ville hjelpe hvis uoppfordret kommersiell e-post var merket som reklame.
- 65% sa at e-postspam kostet dem eller deres arbeidere tid eller penger.
- 52% sa at de handlet mindre eller ikke i det hele tatt på grunn av faren for e-postspam.
- 62% sa at de bruker et anti-spamfilter, men bare 17% sa at filteret fungerte tilfredsstillende.

### 3.2 Artikler

Dennis W. K. Khong gjør en økonomisk undersøkelse av virkningene fra spam lovene med arbeidet sitt i artikkelen «an economic analysis of spam law»[30]. I den første delen av artikkelen utvikler han et økonomisk argument for regulering og utsending av e-postspam. Han undersøker effektiviteten av forskjellige måter å regulere e-postspam på. Videre utvikler han en modell for å vise at ved å ikke ha lover og regler vil e-postspam være ineffektiv. I artikkelen foretar han en analyse av de tre mest vanlige måtene å forholde seg til spam på i USA.

1. Filtrere ut «Melde seg av e-post listen (opt-out)» e-postspam.
2. Blokkering
3. Filtrere ut «Melde seg på e-post listen (opt-in)» e-postspam

Studiet viser at spam i forhold til modellen hans både kan være positivt og negativt, sannsynligvis i større grad negativt. Han konkluderer at å filtrere valgt-inn(opt-in) er den beste løsningen tilgjengelig, så utarbeider han en policy:

1. Bare valgt-inn reklame e-post er lovlig. Annen e-postspam er forbudt.
2. Valgt-inn e-postlister er det mulig å trekke seg fra, en klar og enkel metode for å melde seg av er tilgjengelig.
3. Emnet-feltet må ikke være missledende og skikkelig identifisert. Standardisert filtrering-vennlig identifisering trenger ikke være brukt hvis det er uoppfordret e-post er lovlig.
4. Relay filtrering er lovlig hvor det er klart at den spesielle senderen eller kilden sender uoppfordret e-mail. SMTP identifikasjon er ikke nødvendig, siden standard regel er at uoppfordret e-postspam ikke er lov.
5. Stater bør gi sivile botemiddler i formen av hvor stor skade som kan sannsynliggjøres. I tillegg tillate tiltak mot uoppfordret e-post spam.

Han konkluderer med at ved filtrering av e-post som krever avregistrering (opt-out) ikke er den beste måten å håndtere e-postspam på. Ved å bruke den alternativ nr 2,

blokkering og filtrere så øker en de totale kostnadene rundt spam, mens den beste løsningen er alternativ nr 3, som tar å filtrer på «opt-in» e-postspam.

## 4 Vurdering av intervju

Jeg valgte å intervju høyskoler og universitet i Norge for å vurdere i hvilken grad de klarer å håndtere spamproblematikken. For på den måten vurdere om de vil være i stand til å stå imot spamproblematikken på en god måte i årene som kommer.

Jeg ønsket å intervju alle de 42 utdannings institusjonene for høyere utdanning. Det lyktes å få intervjuet 37 av disse med den tiden jeg hadde til rådighet.

### 4.1 Overføring av kunnskap

Det vil være mulig å overføre denne kunnskapen til andre institusjoner / organisasjoner og SMB'er med disse måtene å løse problemet på. En vil kunne vurdere egne tiltak opp mot det som er vanlig for norske utdanningsinstitusjoner. En vil også kunne vurdere effekten på egne tiltak opp mot det som en kan forvente seg av gitte metoder.

### 4.2 Gjennomføring av intervjuene

Det ble tatt utgangspunkt i samordna opptaks liste over læresteder i Norge. Enten ble leder på IT-avdelingen eller e-post/spam-ansvarlig intervjuet. Jeg ønsket i utgangspunktet å intervju den personen med mest fagkompetanse på området for å få et mest mulig riktig bilde av situasjonen. Intervjuet ble gjort per telefon, der jeg tok utgangspunkt i 31 spørsmål. De 6 første spørsmålene brukte jeg som faste variabler. Det henvises da til statistiske faste variabler, variabler som i denne sammenhengen ikke skal være varierende.

Intervjuskjemaet ligger som appendiks nr 1

### 4.3 Formålet/vurdering av spørsmålene:

De forskjellige spørsmålene ble laget for å få kunnskap om noen spesifikke forhånds bestemte emner. En vurdering eller beskrivelse av formålet med det aktuelle spørsmålet er vist.

#### 4.3.1 Generelle spørsmål

##### *Spørsmål nr 1*

*Arbeider/jobber ved :*

*Navn:*

*Tlf:*

Vurdering av nr 1: Ble mest brukt for å registrere data/kontakt informasjon om vedkommende som ble intervjuet for å kunne ta kontakt igjen, eller ringe tilbake når det passet.

***Spørsmål nr 2***

*Hvor mange brukere har dere ?*

Vurdering av nr 2: Ble brukt for å finne ut om det var noen sammenheng mellom antall brukere og spam problemene. Sammenheng mellom antall brukere og spamløsning ble også vurdert.

***Spørsmål nr 3***

*Type utdannings institusjon med fokus på : teknisk eller annet?*

Vurdering av nr 3: Ble brukt for å se på om det er en sammenheng mellom utdanning innen tekniske fag, og en høy teknisk kompetanse på IT-avdelingen.

***Spørsmål nr 4***

*Er det utdanning på doktor grads nivå ?*

Vurdering av nr 4: Ble brukt for å se om det er en sammenheng mellom et høyt utdannings nivå og en høy teknisk kompetanse på IT-avdelingen.

***Spørsmål nr 5***

*Hvilken landsdel?*

Vurdering av nr 5: Ble brukt for å se om det er en sammenheng mellom landsdelene når det gjelder valg av løsning og problemer med spam.

**4.3.2 Spørsmål om kompetanse**

***Spørsmål nr 6***

*Hvilken utdanning har de ansatte som drifter e-post /spam ?*

***Spørsmål nr 7***

*Hvor lang arbeidserfaring ved e-post /spam drifting har ansatt som drifter e-post / spam ?*

Vurdering av nr 6 og nr 7: Disse to spørsmålene ble brukt for å kunne gjøre en samlet vurdering av hvor stor kompetansen til de som har ansvaret eller drifter e-post/spam løsningen har.

#### **4.3.3 Spørsmål om risiko**

##### **Spørsmål nr 8**

*Har dere student boliger på nettet ?*

Vurdering av nr 8: Ble brukt for å kunne gjøre en vurdering av hvor stor risikoen er for å få spam. Den blir ansett som større hvis en har student boliger på nettet , som en følge av økt eksponeringstid. Risiko = tid \* konsekvens.

##### **Spørsmål nr 9**

*Har dere trådløst nett tilgjengelig for brukerne ?*

Vurdering av nr 9: Ble brukt for å kunne gjøre en vurdering av hvor stor risikoen er for å få spam. Den blir ansett som større hvis en har trådløst nett tilgjengelig på skolen. En kan da bruke private bærbare pc'er som ikke er tilstrekkelig sikret og som da kan utgjøre en risiko.

#### **4.3.4 Spørsmål om spamfilter**

##### **Spørsmål nr 10**

*Hvilket spamfilter bruker dere?*

Vurdering av nr 10: Ble brukt for å finne ut om det er en sammenheng mellom nøyaktigheten, effektivitet og driftstid opp mot hvilket spam filter som brukes.

##### **Spørsmål nr 11:**

*Hvilken type spamfilter bruker dere?*

<i>Kommersielt</i>	<i>Open-source</i>	<i>Egenutviklet</i>	<i>Out-sourcet</i>	<i>Annet :</i>	<i>ukjent</i>
--------------------	--------------------	---------------------	--------------------	----------------	---------------

Vurdering av nr 11: For å vurdere og få oversikt av hvilke løsninger som velges, og om det er en sammenheng mellom type spamfilter som benyttes og effektiviteten, driftstid og nøyaktigheten.

##### **Spørsmål nr 12**

*Hvilket spamfilter teknologi(er) bruker dere ?*

<i>Hvit-listing</i>	<i>Svart-listing</i>	<i>Grå-listing</i>	<i>Innhold-basert</i>	<i>Statistisk</i>	<i>Protokoll-sjekk</i>	<i>ukjent</i>
---------------------	----------------------	--------------------	-----------------------	-------------------	------------------------	---------------

Vurdering av nr 12: For å vurdere og få oversikt over typer spamfilter teknologi som blir valgt, om en type teknologi har høyere effektivitet, nøyaktighet og krever mindre driftstid enn andre typer spamfilter teknologi.

### **Spørsmål nr 13**

*Hvor står spamfilteret(ene) ?*

<i>Front side</i>	<i>Server side</i>	<i>Kombinert</i>	<i>ukjent</i>
-------------------	--------------------	------------------	---------------

Vurdering av nr 13: For å få vurdert om det har en effekt å ha spamfilter på klient siden også, om det er verdt bryet med ekstra arbeidet. Hvis man oppnår tilfredsstillende resultater med å kjøre spamfilter på server vil det være mest gunstig for driften og for nettverksbelastningen.

### **Spørsmål nr 14**

*Hvem har dere out-sourcet e-post driften til?*

<i>Ikke out-sourcet</i>	<i>UNINETT</i>	<i>Annen ISP</i>	<i>ukjent</i>
-------------------------	----------------	------------------	---------------

Vurdering av nr 14: For få en oversikt over hvem som har egen kompetanse på området og hvem som har out-sourcet. For å se på sammenheng med effektiviteten på de som driver in-house og de som har out-sourcet.

### **Spørsmål nr 15**

*Hvor stor prosent andel av e-post er spam ?*

Vurdering av nr 15: For få en oversikt over hvor stort spam problemet er, samt for å få en oversikt over om det kan være sammenheng mellom preventive tiltak som blant annet, offisiell spam-/viruspolicy. En vil også kunne oppnå lavere prosentandel av spam ved bruk av forskjellige spam/virus teknikker, som grålisting. Men eksponering og økt risiko vil øke muligheten for økt prosentandel.

### **Spørsmål nr 16**

*Har dere en offisiell spam-/viruspolicy kundene/brukerene blir informert om ?*

<i>Ja, ved e-post</i>	<i>Ja, ved brev/papir</i>	<i>Ja, ved web sider</i>	<i>ukjent</i>
-----------------------	---------------------------	--------------------------	---------------



Vurdering av nr 16 : For å få en oversikt over om det er satt i gang preventive tiltak for å reduserer spam mengden, for å se om det er en helhet i spambekjempelsen.

**Spørsmål nr 17**

*På hvilken måte er kunde/bruker forpliktet til å følge policyen som det henvises til i spørsmål 16 ?*

<i>Avtaleforpliktet</i>	<i>Oppfordret</i>	<i>Ikke forpliktet</i>	<i>ukjent</i>
-------------------------	-------------------	------------------------	---------------

Vurdering av nr 17 : For å se på hvilke forpliktelser det er gjort, og om avtalen er formalisert eller ikke. Ved å formalisere det vil det heve bevisstheten. For å få en oversikt over om det er satt i gang preventive tiltak for å reduserer spam mengden, for å se om det er en helhet i spambekjempelsen.

**Spørsmål nr 18**

*Hva blir prioritert mest av spam og virus ved IT-driften ?*

<i>Spam</i>	<i>Like mye</i>	<i>Virus</i>
-------------	-----------------	--------------

Vurdering av nr 18: For å finne ut av prioritering mellom spam og virus, for å få en indikasjon på hvor stort problemet er.

**Spørsmål nr 19**

*Hvor mange falske positive (spam som blir gjenkjent som e-post) får dere ?*

Vurdering av nr 19: For å få en indikasjon på nøyaktigheten og effekten av spam filteret.

**Spørsmål nr 20**

*Hvor mange falske negative (e-post som blir gjenkjent som spam) får dere ?*

Vurdering av nr 20: For å få en indikasjon på nøyaktigheten og effekten av spam filteret. Ideelt sett så vil falske negative være tilnærmet lik eller lik 0, på bekostning av flere falske positive som har en mye mindre konsekvens.

**4.3.5 Spørsmål om prioritering**

**Spørsmål nr 21**

*Hvor mange arbeidstimer brukes på spamdrifting per måned?*

Vurdering av nr 21: For å vurdere tid på drifting, etter hvilket spamfilter som benyttes, og mot oppnådde resultater.

**Spørsmål nr 22**

*Hvor mange arbeidestimer er satt av til å holde seg oppdatert på spam-problematikken pr. måned ?*

<i>0 timer</i>	<i>0-1 timer</i>	<i>1-2 timer</i>	<i>2-4 timer</i>	<i>1 dag eller mer</i>
----------------	------------------	------------------	------------------	------------------------

Vurdering av nr 22: Måler her prioriteringen som ledelse/ansatte har på kompetanseheving. En vil med en høy grad av fokus på å holde seg oppdatert, kunne ligge i forkant når det gjelder spamproblematikken. Jeg vil her få inn data om hvor mye spamproblematikken blir prioritert

**Spørsmål nr 23**

*Hvor mye tid er satt av til kompetanseøkning vedrørende spam-problematikken i mnd. for ansatte ved e-post/spam drift?*

<i>0 timer</i>	<i>0-1 timer</i>	<i>1-2 timer</i>	<i>2-4 timer</i>	<i>1 dag eller mer</i>
----------------	------------------	------------------	------------------	------------------------

Vurdering av nr 23: Måler her prioriteringen som ledelse har på kompetanseheving av de ansatte. En vil med en høy grad av fokus på kompetanseheving, kunne ligge i forkant når det gjelder spamproblematikken. Jeg vil her få inn data om hvor mye spamproblematikken blir prioritert

**4.3.6 Spørsmål om lover og regler**

**Spørsmål nr 24**

*Vil internasjonale lover være et effektivt virkemiddel for å redusere spam ?*

<i>Veldig mye</i>	<i>Mye</i>	<i>Vet ikke</i>	<i>Lite</i>	<i>Veldig lite</i>
-------------------	------------	-----------------	-------------	--------------------

Vurdering av nr 24 : Vil vurdere om de mener internasjonale/globale lover vil være effektive for å redusere spam, vil også vurdere dette opp mot norske lover.

**Spørsmål nr 25**

*Vil norske lover være et effektivt virkemiddel for å redusere spam ?*

<i>Veldig mye</i>	<i>Mye</i>	<i>Vet ikke</i>	<i>Lite</i>	<i>Veldig lite</i>
-------------------	------------	-----------------	-------------	--------------------

Vurdering av nr 25 : Vil vurdere om de mener norske lover vil være effektive for å redusere spam, vil også vurdere dette opp mot internasjonale/globale lover. Det ble registrert at det hadde vært nyttig å hatt et eget valg om norske lover ville hjelpe for norsk spam.

**Spørsmål nr 26**

*Har dere et eget system for å oppdage utsendelse av spam fra deres nettverk? Ja/nei*

Vurdering av nr 26: Viser om nettverket har systemer for å hindre utsendelse av spam. Et automatisk system som stenger utsendelse vil klart være det mest effektive for å redusere muligheten for dette.

**Spørsmål nr 27**

*Har dere oppdaget brukere/kunder som bevisst sender ut spam fra deres nett? Ja / nei*

**Spørsmål nr 28**

*Har dere oppdaget brukere/kunder som ubevisst sender ut spam fra deres nett? Ja / nei*

Vurdering av nr 27 og nr 28: For å kartlegge spamkildene internt i forhold til om en har et system for å automatisk oppdage utsendelse av spam. Vil også vurdere om dette problemet kan løses med bruk av policy eller automatiske system, eller en kombinasjon av disse. En vil også se på om det er forskjeller i måten å løse problemet på avhengig om det er bevisst eller ubevisst sendt ut e-postspam.

**4.3.7 Spørsmål om tiden fremover**

**Spørsmål nr 29**

*Hvordan fungerer deres nåværende spamfilterløsning ?*

<i>Veldig tilfredsstillende</i>	<i>Tilfredsstillende</i>	<i>Lite tilfredsstillende</i>	<i>ukjent</i>
---------------------------------	--------------------------	-------------------------------	---------------

Vurdering av nr 29: For å finne ut av hvor stort problemet er, og hvordan en oppfatter sitt eget system som er valgt. En kan da sammenligne type system som brukes, for å se om tilfredsstillelsesgraden avhenger av type.

**Spørsmål nr 30**

*Hvilke egenskaper ved dagens spamfilter fungerer ikke tilfredsstillende ?*

Vurdering av nr 30: For å få en vurdering av hva som kan gjøres bedre med dagens system, ut fra førstehånds opplysninger og erfaring. Vil kunne gi en pekepinne på hvor forbedringspotensialet er.

**Spørsmål nr 31**

*Hvor mange år tror du det vil det ta før spam vil være et mindre problem enn i dag pga. bedre håndtering av spammengden grunnet lover og regler og filtreringsmetoder?*

<i>1-2 år</i>	<i>3-4 år</i>	<i>5-6 år</i>	<i>Aldri</i>
---------------	---------------	---------------	--------------

Vurdering av nr 31: For å få en pekepinne på om de føler at det er et stort problem, som en aldri blir kvitt, da det kan ha en del å si på innfallsvinkelen som blir valgt for å løse problemet.

## **5 Presentasjon og Vurdering av data fra Intervju.**

### **5.1 Datagrunnlaget**

Datagrunnlaget består av muntlig intervju med 37 utdanningsinstitusjoner for høyere utdanning i Norge. Disse har i gjennomsnitt 3801 brukere av e-postsystemet sitt. De er fordelt geografisk med 29,73 % fra vestlandet, 40,54% fra østlandet, 10,81% fra midtnorge og 18,92% fra nordnorge. Det er 49% som kommer fra institusjoner som har teknisk utdanning, og 30% har utdanning på doktorgradsnivå. 65 % har student boliger som er knyttet opp til Internett. Det er 84% som har trådløst nettverk tilgjengelig for brukerne.

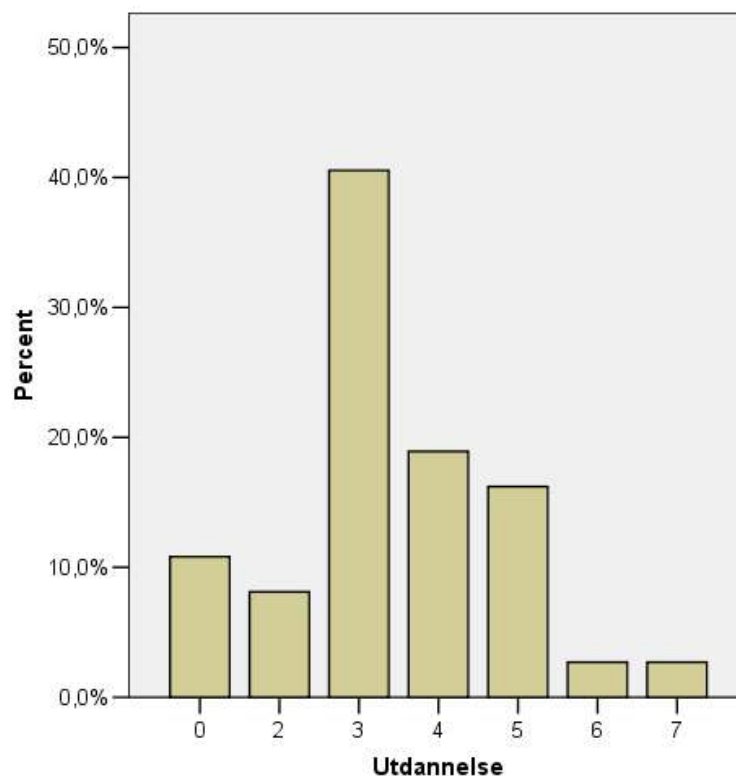
De som er intervjuet har i gjennomsnitt en 3,3 årig utdanning fra høyskole/universitet, og 11,86år med erfaring fra e-postdrift eller it-ledelse.

### **5.2 Presentasjon av data**

De dataene som er mest interessante blir her presentert De resterende dataene fra undersøkelse, vises i Appendiks nr 3.

### 5.2.1 Spørsmål nr 6:

Vurdering av data fra spørsmål om ansattes utdanning

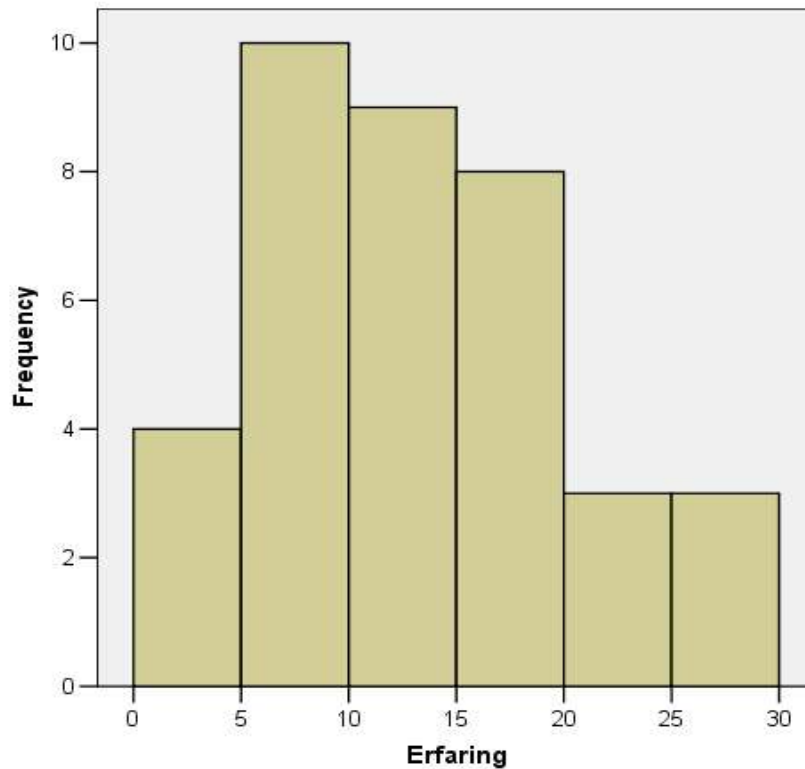


*Illustrasjon 1 Oversikt over utdannelsen til de ansatte*

En ser fra figur 1 at det er en 3årig høyskole/universitetsutdanning som har høyest forekomst med 15 stk(40%) Det er fordelt som vist i histogrammet., med et gjennomsnitt på 3,3år. Det viste seg at de fleste med en 3 årig utdanning hadde en ingeniør utdanning, ofte innen data eller tele. Det var også en stor forekomst av ansatte som hadde en can.mag utdanning bestående av IKT fag og administrative fag.

### 5.2.2 Spørsmål nr 7:

Vurdering av data fra spørsmål om ansattes erfaring

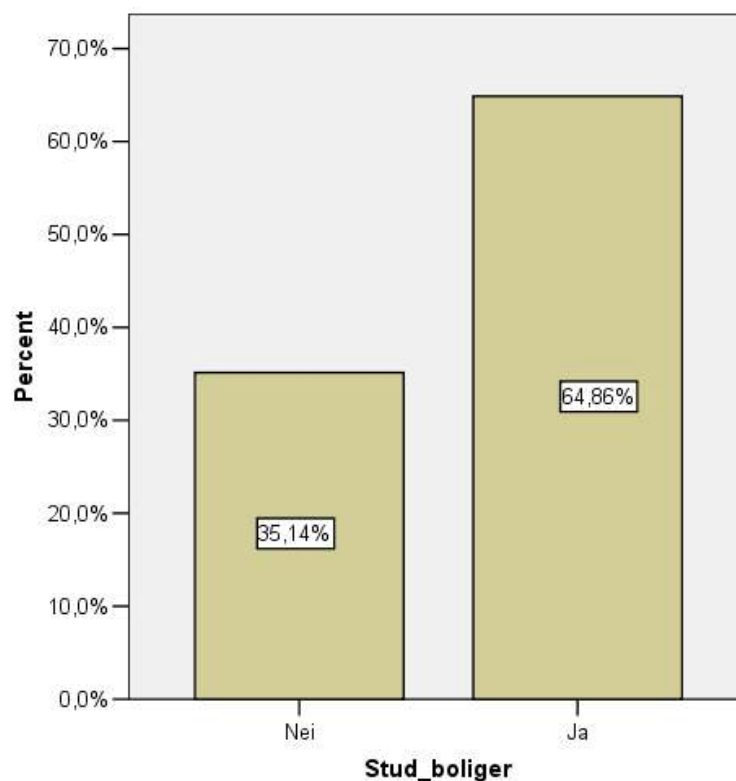


Illustrasjon 2 Oversikt over erfaringen til de ansatte

En ser fra oversikten at det er de med erfaring fra 5-10 år som er oftest representerte, med 10 tilfeller. Gjennomsnitts erfaringen er på 11,86 år. De med lav formell utdannelse var de som ble representert med lang erfaring. De ble utført statistiske beregninger for å finne ut om det var sammenheng med kompetansenivået: utdanning og erfaring, i forhold til hvor mange falske positive og falske negative. En slik sammenheng ble ikke funnet.

### 5.2.3 Spørsmål nr 8:

Vurdering av data fra spørsmål om tilknyttede studentboliger.



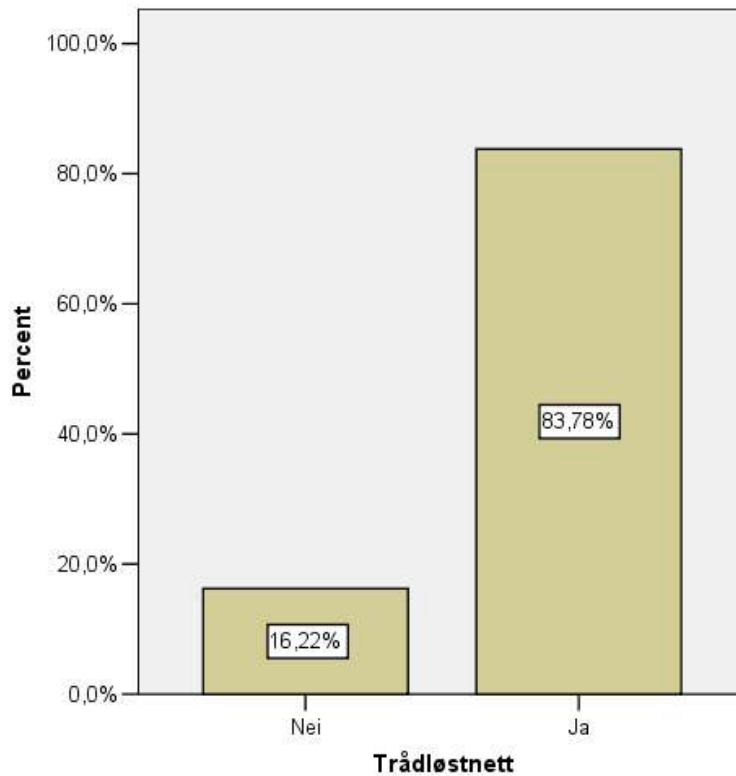
*Illustrasjon 3 Oversikt over student boliger som er tilknyttet nettverket*

Det ble undersøkt om det var koblet til studentboliger på nettverket til institusjonen. Ved en slik kobling så vi risikoen for spam øke. Det var 65% som svarte at de hadde koblet på studentboliger på nettet. En har erfaring med sikkerhetsnivået på studentboligene, er lavere en på utdanningsinstitusjonenes datamaskiner da ikke er vanlig med systematisk oppdatering og vedlikehold av brukerens private datamaskiner.



### 5.2.4 Spørsmål nr 9

Vurdering av data fra spørsmål om de har trådløst nett tilgjengelig for brukerne.

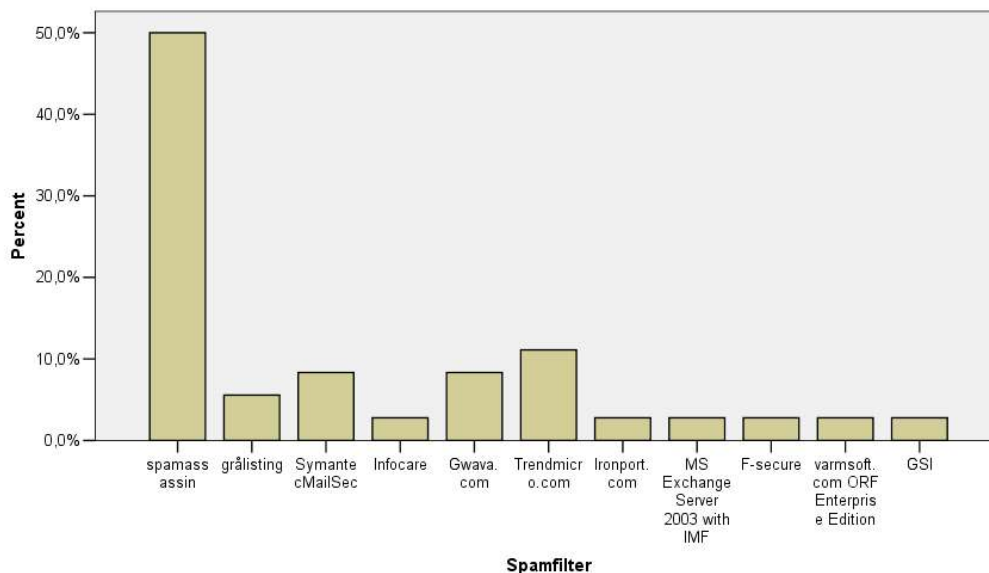


Illustrasjon 4 Oversikt over trådløste nettverk som er tilknyttet nettverket

Det ble undersøkt om det var tilgang på trådløst nett på de forskjellige plassene, noe som er en risikofaktor. 84% svarte positivt til det. En så stor utbredelse av trådløsenett på utdanningsinstitusjonene er relativt mye med hensyn på at det er relativ ny teknologi, som gir en sikkerhetsrisiko selv ved bruk av kryptering. Ved bruk av tilgjengelig programvare på Internett så er det mulig å utnytte svakheter ved dagens trådløse krypterings algoritmer, som beskrevet av Scott Fluhrer, Itsik Mantin og Adi Shamir i artikkelen «Weaknesses in the Key Scheduling Algorithm of RC4[31]». Ved å ikke ha oversikt over hvem som er logget-på nettverket så har en potensiell sikkerhets svakhet.

### 5.2.5 Spørsmål nr 10

Vurdering av data fra spørsmål om hvilket spamfilter som benyttes.

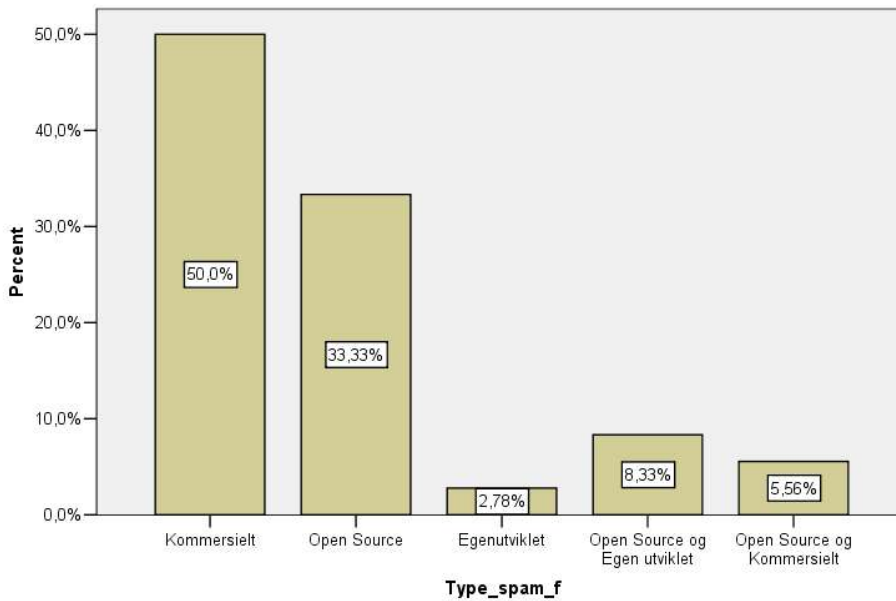


Illustrasjon 5 Oversikt over hvilke spamfilter som ble brukt

Det ble undersøkt hvilke spamfilter som ble brukt, og SpamAssassin ble den desidert mest brukte med 50%. De andre fikk fra 11% til 3%. Det ble fordelt mellom 11 forskjellige typer spamfilter. Dette stemmer bra med internasjonale trender[27] de siste årene, der SpamAssassin ofte blir anbefalt. SpamAssassin ble hos flere brukt sammen med grålisting og e-post-klienter som Mozilla Firefox og MS Outlook 2003. Det var ikke registret noen som brukte flere spamfilter på server i seriell.

### 5.2.6 Spørsmål nr 11

Vurdering av data fra spørsmål om hvilken type spamfilterteknologi som benyttes.

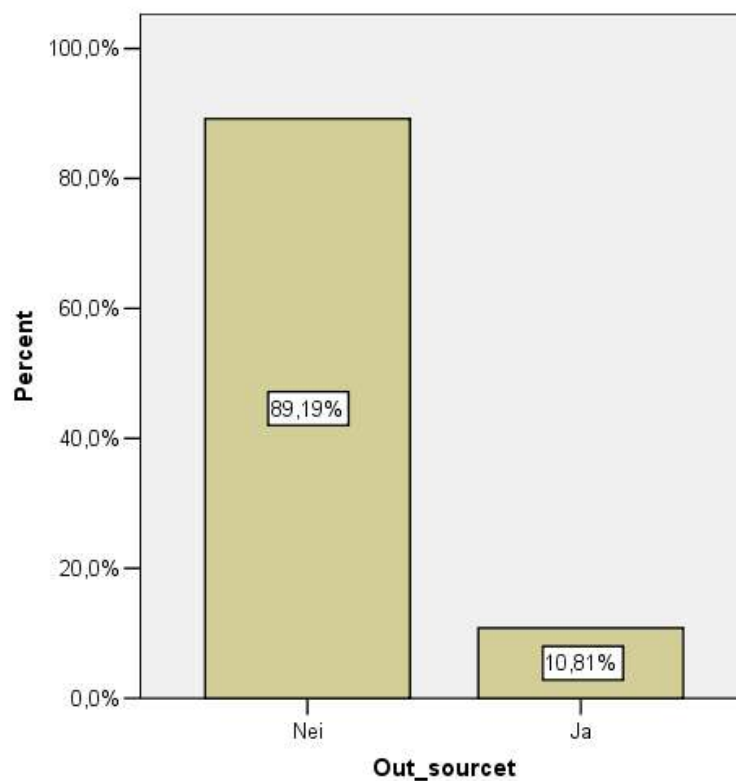


Illustrasjon 6 Oversikt over hvilken type spamfilter som ble brukt

Det ble undersøkt hvilke spamfilter type(r) som ble brukt. Det ble registrert at det var 50% som brukte kommersielle produkter. 47% bruker open-source produkter alene eller sammen med enten egenutviklede eller kommersielle produkter. Det kan tyde på høy egenkompetanse hos driftspersonalet når de utvikler egne spamfilterløsninger. I kategorien «open-source og egenutviklet» var det kombinasjonsløsninger med SpamAssassin som filtergrunnlag sammen med egneproduserte regler.

### 5.2.7 spørsmål nr 14

Vurdering av data fra spørsmål om de benyttet seg av out-sourcing av e-post driften.

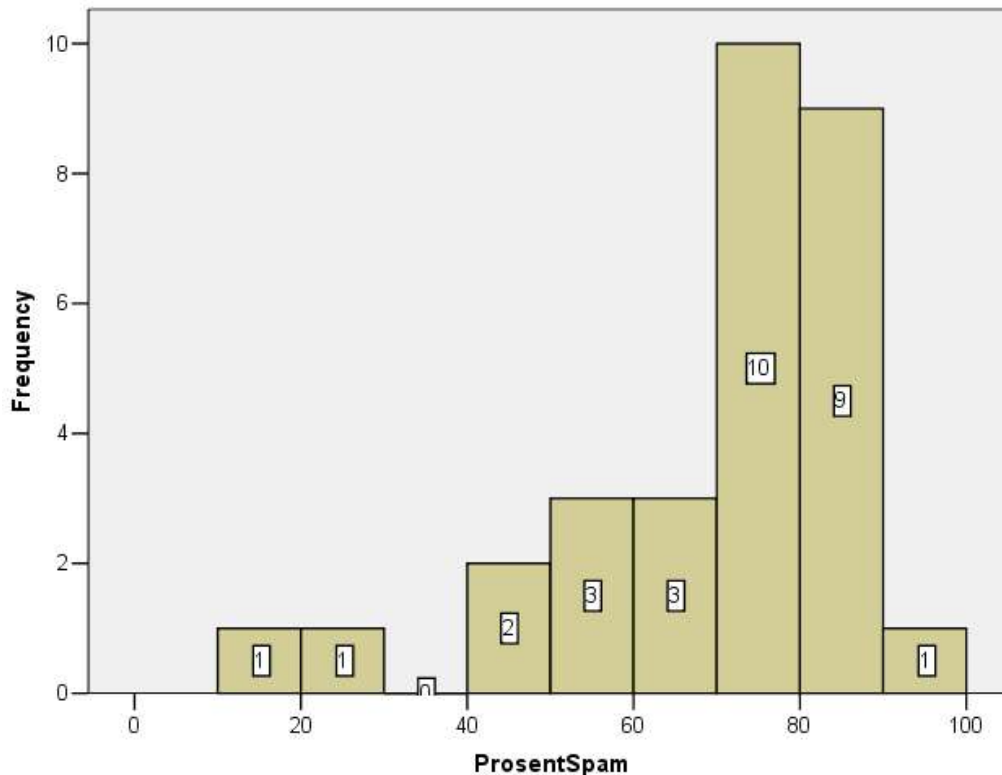


Illustrasjon 7 Oversikt over hvor mange som out-sourcet e-post driften sin

Det er kun 11% av de spurte som hadde out-sourcet e-post driften. Når 89% av høyskolene og universitetene drifter nettet og datatjenestene in-house så tyder det på at de sitter med en betydelig erfaring og kompetanse. Noen av de som out-sourcet e-post driften gjorde det av arbeidskraft hensyn og andre pga. avtaler de hadde som gjaldt e-postdrift.

### 5.2.8 Spørsmål nr 15

Vurdering av data fra spørsmål om hvor stor prosentandel som er spam av all e-post som kommer inn.



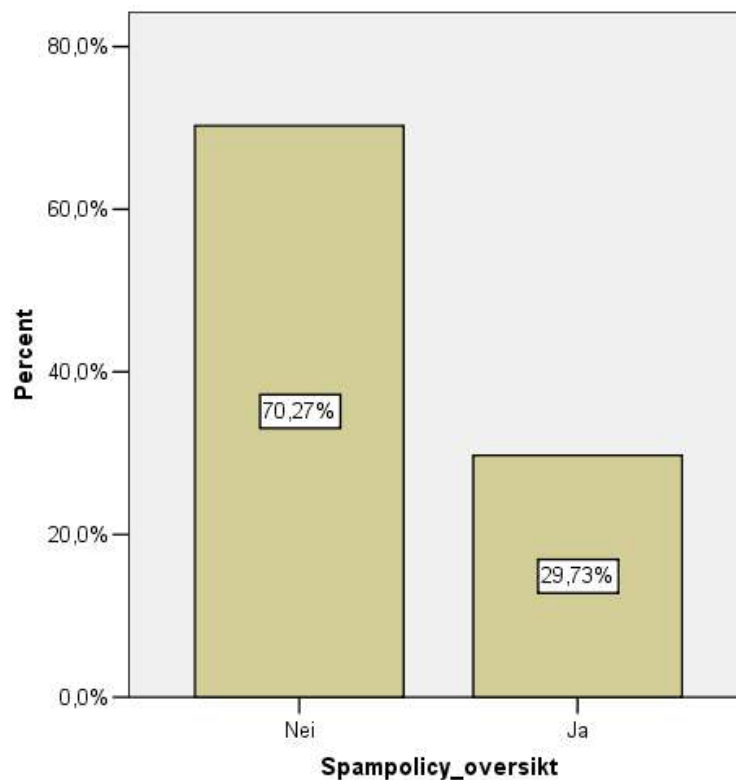
Illustrasjon 8 Oversikt over hvor stor prosent spam av e-post

Som histogrammet viser så er det et gjennomsnitt på 67% spam. Det er en fordel å få stanset så mye av spam mengden som mulig før den når spam filteret. Metoder for å få dette til vil være preventive tiltak som beskrevet i kapittel 4, grålisting, challenge/respons system og virus filtrering i forkant av spamfilter.

Noe av grunnen til at datagrunnlaget varierer er blant annet at noen har viruskanning før spamfiltreringen, da blir alle e-post med virus fjernet, så registrerte e-postspam blir laverer en det reelt er. Andre hadde ikke helt oppdaterte data, så da ble det registret det det som var mest oppdatert, noen ganger opp til 6 måneder siden.

### 5.2.9 Spørsmål nr 16

Vurdering av data fra spørsmål om hvor mange som har spampolicy.



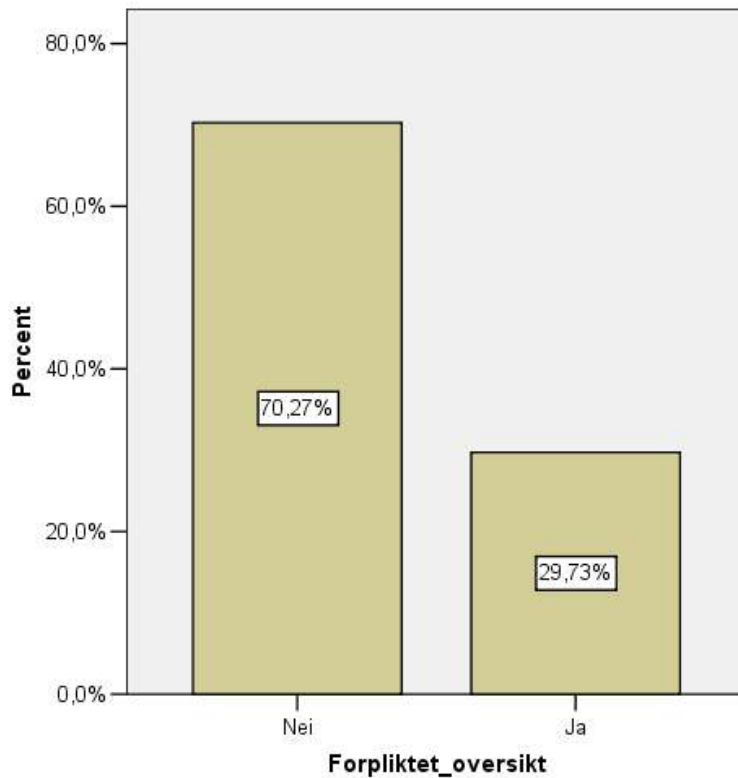
Illustrasjon 9 Oversikt over hvor stor andel som har en spampolicy

En spampolicy er en policy som går ut over det en vanlig sikkerhets-policy gjør, den har fokusering på spam og mail. Det ble registrert at kun 30% som hadde en spampolicy. 5% hadde en spampolicy som ble sendt skriftlig ut til brukerne, 5% hadde en spampolicy som ble sent ut på e-post til brukerne og 19% hadde bare spampolicyen sin på sine hjemmesider.

En ser at det er få som benytter seg av denne metoden for å få ned spam mengden, noe som burde tilsi at det er et stort potensiale her. En spampolicy omhandler blant annet hvordan en kan unngå å eksponere e-postadressen mer en nødvendig. Det skal også komme frem en fremgangsmåte på hvordan en håndterer e-postspam. Automatisk svar fra e-posten når en er borte fra jobb, er også noe som en kan med fordel regulerer med en spampolicy.

### 5.2.10 Spørsmål nr 17

Vurdering av data fra spørsmål om hvor mange som er forpliktet til å følge spampolicyen



Illustrasjon 10 Oversikt over hvem som er forpliktet til å følge spampolicyen

En ser fra undersøkelsen at det er kun 10% som har gjort brukerne forpliktet til å følge spampolicyen med en skriftlig avtale av de som har en spam policy. Det vil si at av totalen blir det kun 3% som har en forpliktende avtale.

Det var 90% som var oppfordret via informasjon om å følge spampolicyen, av totalen blir det 27.% som ble oppfordret.

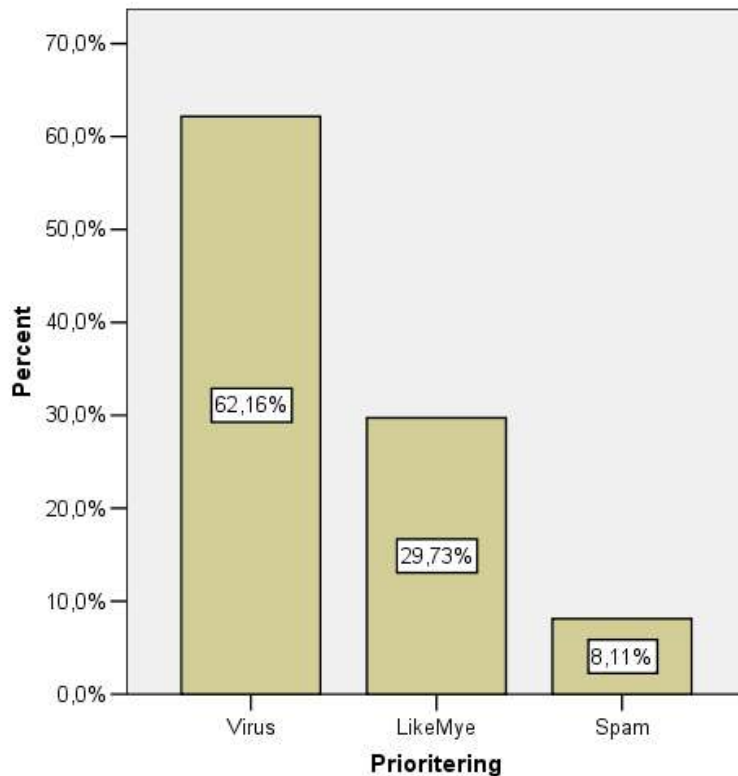
En ser fra figuren at det er kun 30% som har gjort brukerne forpliktet eller oppfordret til å følge spampolicyen, de resterende 70% er kun oppfordret til å følge policyen, noe som lett fører til lite oppfølging fra brukerne.

Ved at brukerne forplikter seg til spampolicyen ved en skriftlig avtale kan brukerne være rettslig ansvarlige hvis spampolicyen brytes.



### 5.2.11 Spørsmål nr 18

Vurdering av data fra spørsmål om prioritering av virus- eller spamproblematikk.



Illustrasjon 11 Oversikt over hvordan prioriteringen er hos it-avdelingen

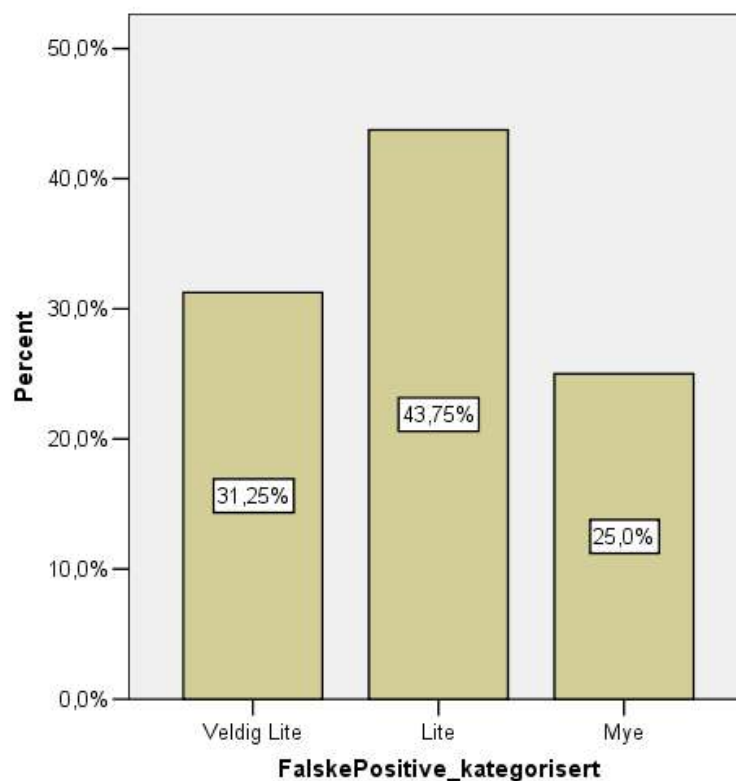
En ser her at prioriteringen helt klart ligger på virus, noe som er naturlig da et virus angrep når det først inntreffer kan ha en større skade for bedriften. Det er viktig i den daglige driften å ikke skille disse to som helt separate problem, da spam kan ha med seg virus. En kan forebygge og drive preventive virus tiltak, med og ha en effektiv spamfiltrering.

E-postspam som inneholder virus kan muligens her være registrert som virus. På den måten har ikke spam fått en høyere prioritering hos respondentene. En mulig årsak til

den lave prioriteringen av e-postspam kan være at spamproblematikken er relativt ny sammenlignet med faren for virus.

### 5.2.12 Spørsmål nr 19

Vurdering av data fra spørsmål om falske positive e-post



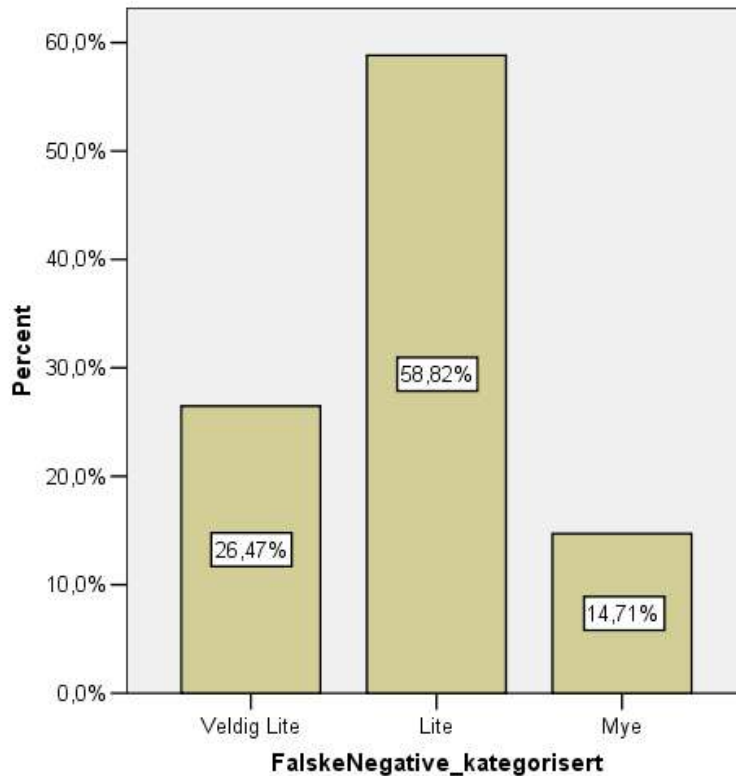
Illustrasjon 12 Oversikt over falske positive

Her har de falske positiv e-post blitt katalogisert inn i tre grupper, for lettere å kunne vurdere dem. Veldig lite er definert som 0-1%, lite fra >1 -5% lite, og >5% mye. På grunn av at noe av datagrunnlaget var usikkert så ble dataene kategorisert for å kunne gjøre en fornuftig vurdering.

«Veldig lite» blir klart å foretrekke og bør være målet til et effektivt filter. Kommer en opp i kategorien «mye», så har en absolutt et problem med filteret sitt. De 25% som har kommet opp i denne kategorien vil ha mye å hente på å forbedre løsningen sin.

### 5.2.13 Spørsmål nr 20

Vurdering av data fra spørsmål om falske negative e-post,



Illustrasjon 13 Oversikt over falske negative

Her har de falske negative e-post blitt katalogisert inn i tre grupper, for lettere å kunne vurdere dem. Veldig lite er definert som 0-0,01%, lite fra 0,1-0,25%, og >0,25% som mye.

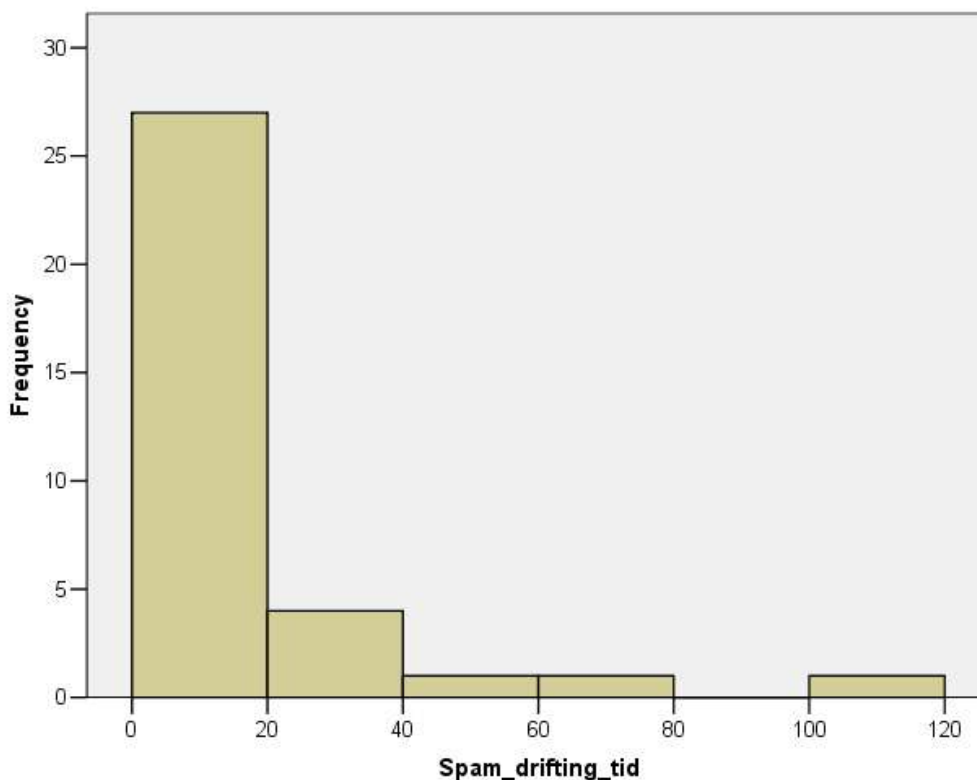
Falske negative, e-post som blir vurdert som spam, av spamfilter og eventuelt slettet er en alvorlig feil vurdering som spamfilteret gjør.

Veldig lite blir klart å foretrekke og bør være målet til et effektivt filter. Kommer en opp i kategorien mye, så har en absolutt et problem med filteret sitt. De 15% som har kommet opp i denne kategorien vil ha mye å hente på å forbedre spamløsningen sin. Falske negative kan være et mye mer alvorlig og tidkrevende problem en falske positive.

Falske negative blir registrert av it-avdelingene når de får en henvendelse fra brukerne om at de ikke har mottatt forventet e-post. Falske negative blir ikke alltid oppdaget da det er kun manuell registrering av disse.

### 5.2.14 Spørsmål nr 21

Vurdering av data fra spørsmål om hvor mange arbeidstimer som blir brukt på spamdrifting,

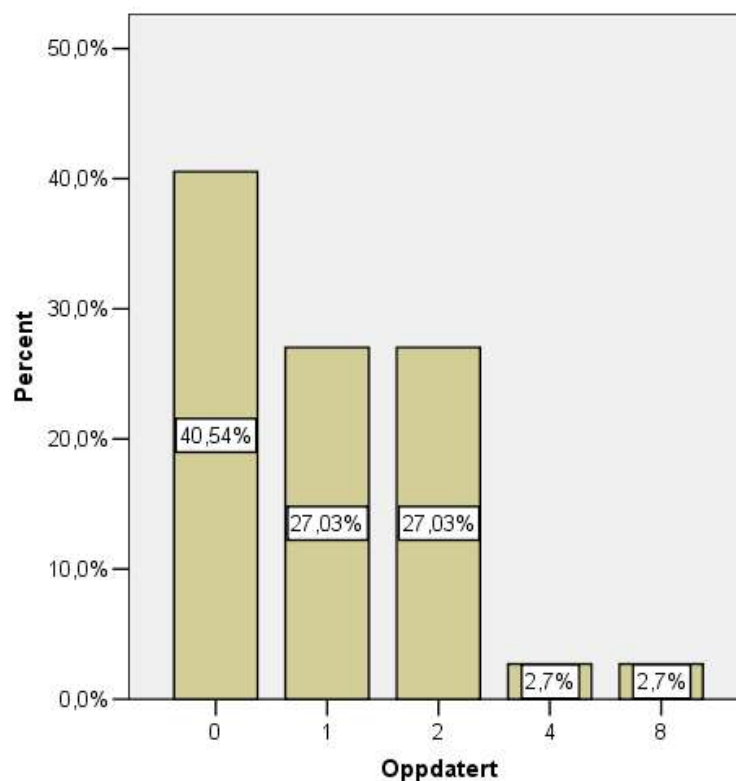


Illustrasjon 14 Oversikt over arbeidstimer som brukes til spam drifting

Som en ser fra oversikten så ligger gjennomsnittstiden det brukes på spamdrifting på 13,79 timer per måned, noe som tilsvarer ca. 10% av en full stilling. Når en tenker på at dette innbefatter daglig drift og oppdateringer så er det ikke mye. I et ideelt system, ville det ikke kreve noe daglig/ukentlig vedlikehold, og oppdateringene ville gå automatisk, noe de færreste gjør i dag. Mye av tiden som brukes går til å lese ren-tekst logg filer, noe som flere ga tilbakemelding på som lite tilfredsstillende. Ellers gikk tid med til oppdatering av programvare på server, spamfilter. Noe tid gikk også med til å finne e-post fra brukere som de mener ikke har kommet frem til dem, pga. spamfilteret.

### 5.2.15 Spørsmål nr 22

Vurdering av data fra spørsmål om hvor mye tid som blir satt av til å holde seg oppdatert.



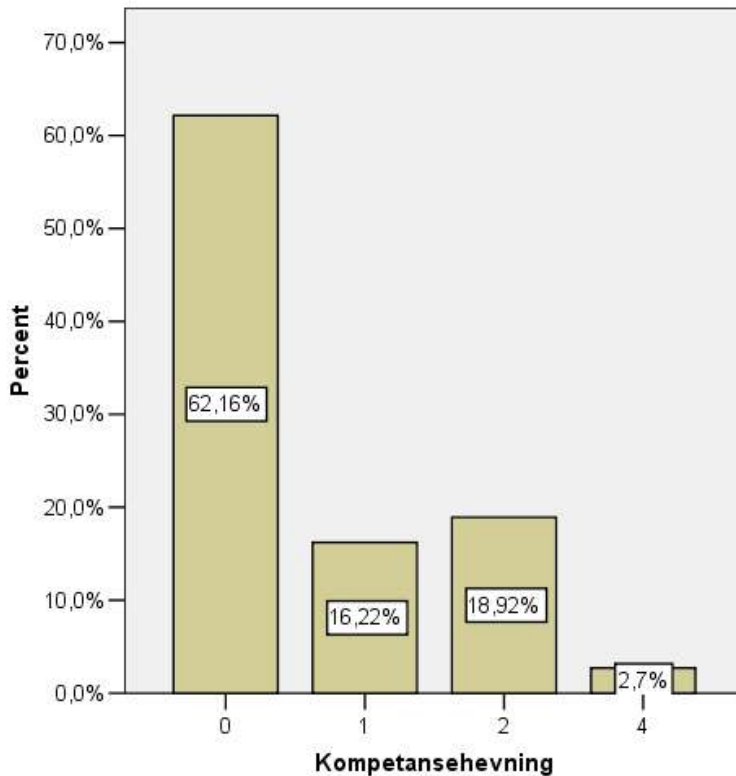
Illustrasjon 15 Oversikt over arbeidstimer som brukes til å holde seg oppdatert

Det er relativt få timer i måneden som blir satt av til å holde seg oppdatert. Gjennomsnittet er på 1,14 timer pr. mnd. Ca. 40% bruker ikke noe tid i det hele tatt på å holde seg oppdatert og de er alle blant de som heller ikke bruker tid på kompetanseøkning, slik som beskrevet i spørsmål nr 23.

Ved at ikke it-avdelingen kontinuerlig holder jeg oppdatert på spamproblematikken vil en bli satt betydelig mer tilbake de gangene spammeren bruker en ny teknikk.

### 5.2.16 Spørsmål nr 23

Vurdering av data fra spørsmål om hvor mye tid som blir satt av til kompetanseheving.



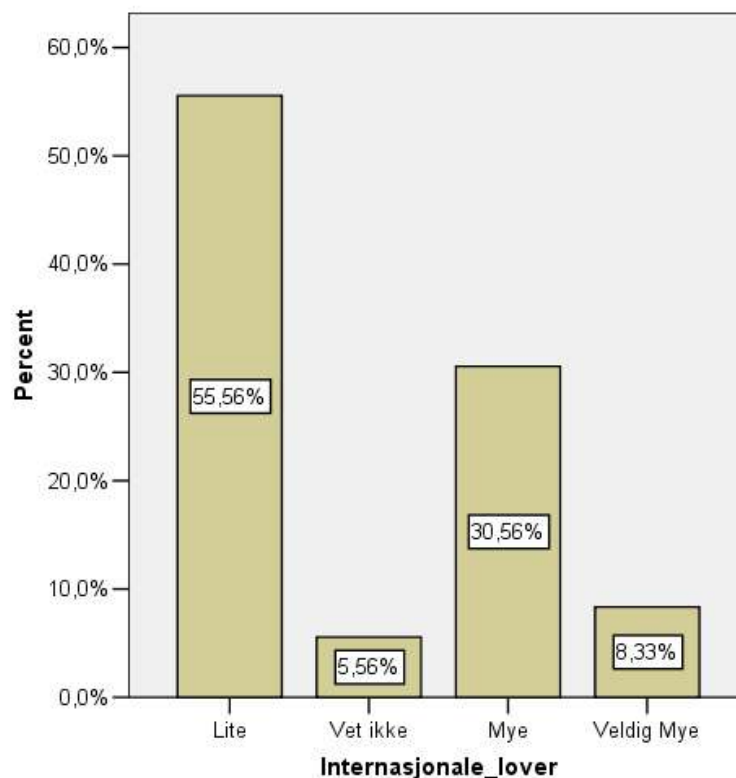
*Illustrasjon 16 Oversikt over arbeidstimer som brukes til kompetanseheving*

Undersøkelsen viser at det er relativt få timer i måneden som blir satt av til kompetanseheving og ca 60% bruker ikke noe tid i det hele tatt.

Ved å ikke sette av noe tid i det hele tatt vil en ikke forbedre situasjonen, men en vil kanskje klare å holde kompetansen på nåværende nivå. Det kan tenkes at i fremtiden vil spammerene være enda mer avanserte enn de er i dag og da blir det enda viktigere å ligge i forkant av spamutviklingen. En vil også kunne bidra til at andre får økt kunnskap ved å være en aktiv deltaker i et relevant fagmiljø.

### 5.2.17 Spørsmål nr 24

Vurdering av data fra spørsmål om en tror at det vil virke reduserende på spam mengden med internasjonale lover.



Illustrasjon 17 Oversikt over hvor stor effekt en tror internasjonale lover har

Kun 39 tror at det kan være virkningsfullt med internasjonale lover. Flere av de intervjuede kommenterte at hvis internasjonale lover skal kunne ha en effekt så må de gjelde over alt. På den måten får en ikke smutthull, der en kan sette opp server som sender ut spam, fra lovløse friområder. Å få internasjonale lover til å gjelde i alle land og stater kan naturlig nok bli problematisk å gjennomføre.

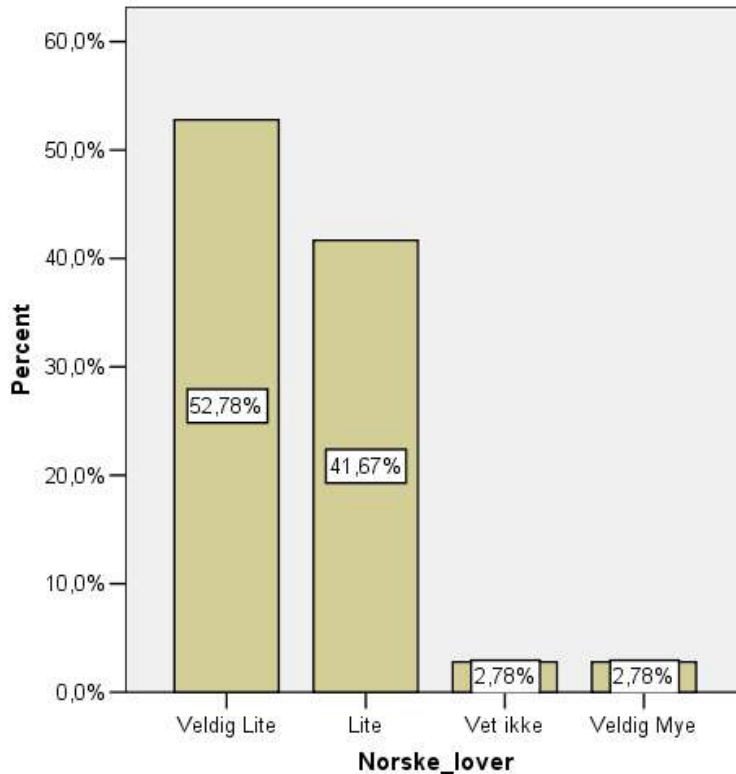
For at det skal blir et effektivt tiltak, må det implementeres i alle lands lovgivning, det må bli fulgt opp av landets myndigheter, og sanksjoner må gis når loven brytes. Det må etterfølge av normal rettspraksis som på andre tilsvarende lover. For å få til dette kreves det et godt samarbeid mellom landene. En årsak til at dette ikke vil la seg



gjennomføre enkelt er at lovene medfører større ugunst en gunst for en del av utviklingslandene.

### 5.2.18 Spørsmål nr 25

Vurdering av data fra spørsmål om en tror at det vil virke reduserende på spam mengden med norske lover.



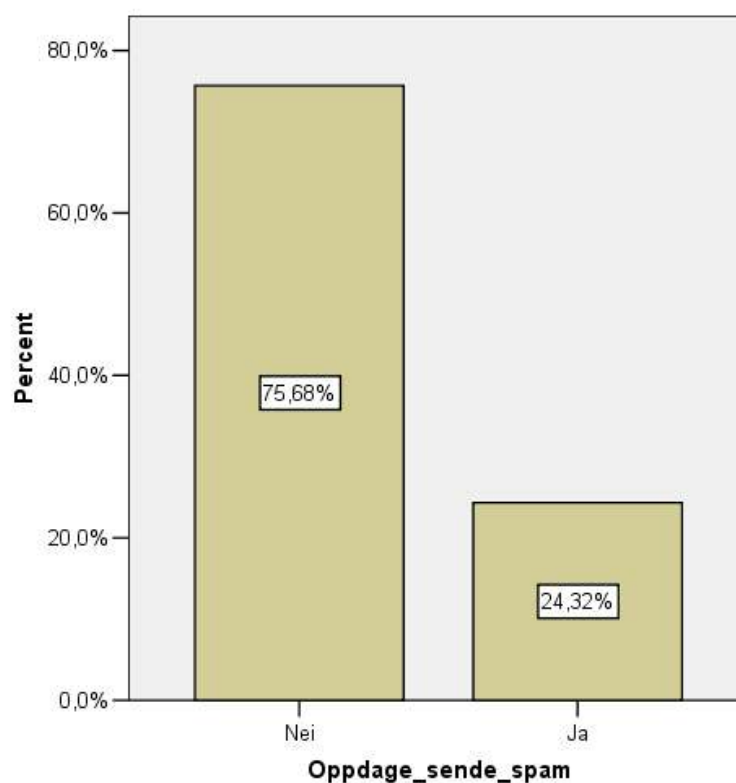
Illustrasjon 18 Oversikt over hvor stor effekt en tror norske lover har mot spam

31% tror at det kan være virkningsfullt med norske lover, for å hindre spam som kommer fra Norge. En har enda ikke opplevde spam på nivå 4 med utsendelse fra Norge. Den delen av spamen som kommer fra Norge opplevde de fleste som liten og er som oftest på nivå 1-3 og nivå 5 ved kompromitterte maskiner.

28 prosent av de spurte mente i tillegg at norske lover kunne ha en stor effekt på «norsk-postspam».

### 5.2.19 Spørsmål nr 26

Vurdering av data fra spørsmål om en har et system for å oppdage utsendelse av spam fra eget nettverk



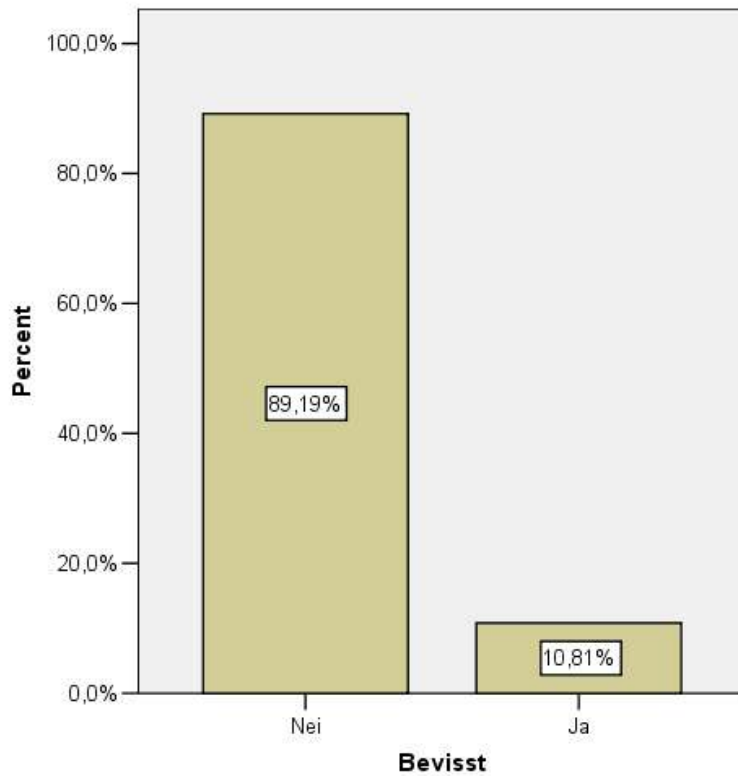
*Illustrasjon 19 Oversikt over om en har et system for å oppdage sending av spam*

Som en ser fra oversikten så er det kun 24% som har et system for å hindre at spam blir sendt ut fra nettverket. For å hindre at en blir medansvarlig i utsendelse av spam bør en ha et slikt system. Når nettverk har flere tusen brukere er det enda viktigere å ha et slikt system, for å begrense mulighetene for at det blir sendt ut spam (ubevisst eller bevisst).

En vil enda ikke ha noe rettslig ansvar ved å ikke ha et system som oppdager utsending av e-postspam men dette er «bestpractice» og vurderes som et krav til norske ISP'er fra myndighetene i Norge.

### 5.2.20 Spørsmål nr 27

Vurdering av data fra spørsmål om en har oppdaget noen som bevisst har sendt ut spam fra eget nettverk,



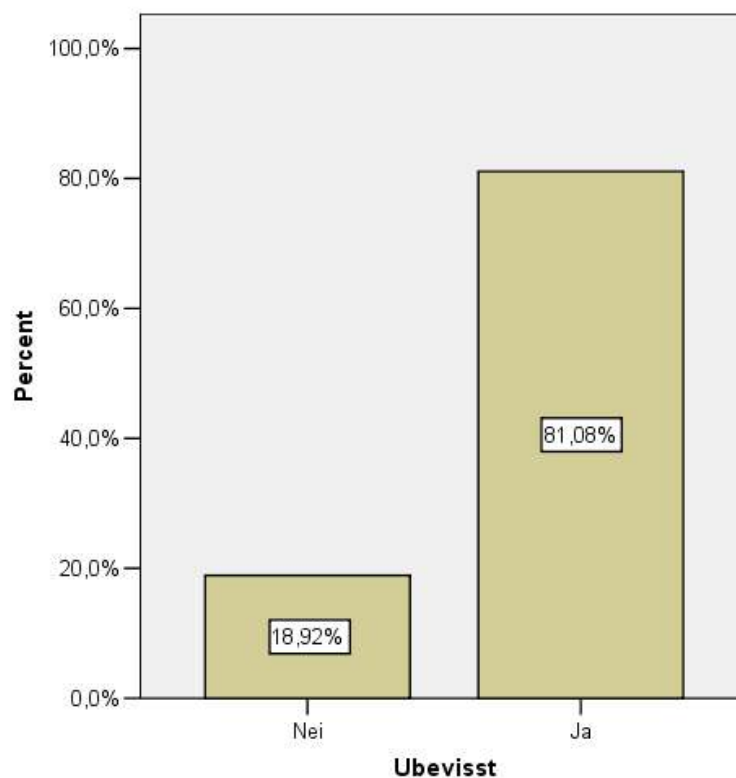
*Illustrasjon 20 Oversikt over bevisst utsending av spam*

Det er kun 11% som har registrert at noen har sendt ut spam bevisst. Selv om dette er lave tall så viser dette at det viktig å ha et system som stanser e-post spam. En kan regne med at personer som ikke var sikre vil på dette spørsmålet svare «nei» for å være på den sikre siden, så en kan ikke se bort fra at det er under-rapportert.

De som ble registrert som «bevisst» var av spam på nivå 1-4.

### 5.2.21 Spørsmål nr 28

Vurdering av data fra spørsmål om en har oppdaget noen som ubevisst har sendt ut spam fra eget nettverk,



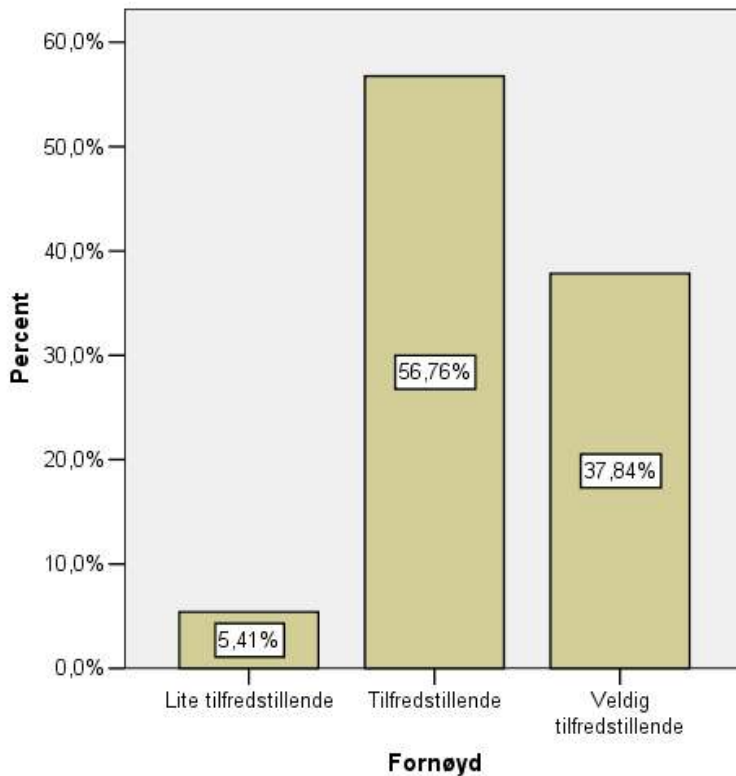
*Illustrasjon 21 Oversikt over ubevisst utsending av spam*

Det er hele 81% som har registrert at det er blitt sendt ut spam ubevisst fra deres eget nettverk. Årsaken til dette var i de aller fleste tilfellene at et virus eller en trojansk hest hadde kompromittert maskinen til en bruker. Slike maskiner var ofte ikke under administrasjon av it-avdelingen, men under brukeren selv. Brukeren hadde da som oftest ikke oppdatert programvare som operativsystem og anti-virus

De som ble registrert som «ubevisst» var av spam på nivå 5.

### 5.2.22 Spørsmål nr 29

Vurdering av data fra spørsmål om hvor fornøyd en er med spamfilterløsningen som en bruker i dag (april 2005),



Illustrasjon 22 Oversikt over tilfredshetsgraden av spamfilter løsningen

Det er et stort flertall på hele 95% som er fornøyd med spamfilter løsningen som de har i dag. 57% synes løsningen er tilfredsstillende og 38% synes løsningen er veldig tilfredsstillende. Det er kun 5% som ikke er fornøyd.

En vil allikevel se en stor forskjell hvis en sammenligner det ideelle systemet mot det systemet som de intervjuede var veldig tilfredsstilte med.

### 5.2.23 Spørsmål nr 30

Vurdering av data fra spørsmål om hvilke egenskaper ved dagens spamfilter som ikke fungerer tilfredsstillende

**Effektiviteten:**

Det som flest ikke er fornøyd med er effektiviteten til spamfilterløsningen. Hele 37% er ikke tilfreds med effektiviteten. Det er hovedsaklig for mye falske positive og falske negative e-poster som er årsaken til at de ikke er fornøyd med effektiviteten.

**SMTP:**

Det var 10% som mente at dagens SMTP-protokoll hadde for mange svakheter. Det ble nevnt egenskaper som autentisering og signering av e-post.

**Oppdateringer:**

Det var flere som savnet automatiske oppdateringer av spamfilteret. Det var noe som flere utsatte å gjøre, selv om det var nye oppdateringer tilgjengelige. Mange synes det er en omfattende og tidkrevende prosess. Manuell oppdatering ble utsatt for å forhindre problemer og konflikter som eventuelt ville kunne oppstå ved en oppdatering.

**Pris:**

Det ble nevnt at prisen var for høy på dagens kommersielle produkter. Dette ble hevdet fra noen som har valgt en av de store og kjente kommersielle løsningene.

**Feil oppsatte epost servere:**

Det ble fra mange registrert at det var flere epost-servere som ikke var satt opp riktig. Dette hindrer protokollsjekk rutiner for å luke ut eventuelle spammere.

**Automatisk hvitlisting:**

Det kunne vært ønskelig og nyttig med automatisk hvitlisting av alle e-post adresser som det blir sendt til. Det er en stor fordel ved automatisk hvitlisting for brukerne som er sikre på å unngå falske negative e-poster.

**Bedre logger:**

De fleste spam-systemene genererer mange viktige logger, men det som flere savner er et verktøy som gir den hele oversikten når det brukes forskjellige systemer. Et felles grensesnitt fra de forskjellige loggene, gjerne med en grafisk fremstilling av de viktigste tallene for å synliggjøre tvilstilfeller var savnet.

**Automatiske RBL-lister:**

Det ble savnet hel-automatisk oppdatering av RBL-listene, for å få ned driftstid på spamløsningen.

**Diffrensing på brukere:**

En ønsker å differensiere på brukerne da spamfilterbehovet til tider er veldig individuelt. Med dagens løsninger så er det ikke mulig å få en sentralt styrt løsning til å differensiere på forskjellige brukere.

Sentral styring av spam-klienter:

Når en bruker desentraliserte spamfilter i e-postklienten, som feks Mozilla Thunderbird, Opera eller MS Outlook 2003, så ønsker en sentral styring av dette for å få oversikt over driften.

Spam IDS:

Et system for å oppdage om det blir sendt spam i/fra nettverket. Dette finnes det flere løsninger for, men det er fortsatt lite kjent i markedet, noe som kommer frem av undersøkelsen. Det viste seg at kun et fåtall bruker et slikt verktøy i kampen mot spam.

Høy last:

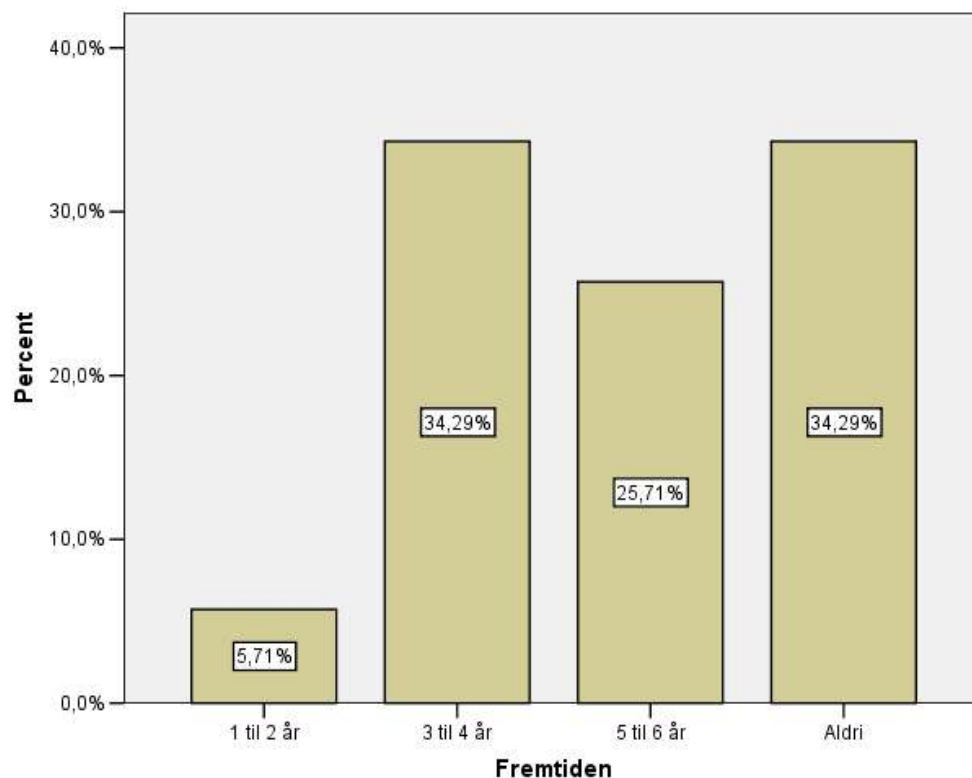
Problemer med høy last, fører til at noen av dagens spamfilter slipper igjennom mer spam for å «spare» CPU-en. Noe som ikke er en bra løsning sett fra et anti-spamståsted. En løsning på dette problemet kan da være å kjøpe mer regnekraft (CPU-kraft), men andre oppfatter det som et problem at de må kjøpe kraftigerer maskiner. Teknisk så er det ikke noe problem å løse dette med parallellprosessering av e-postspamen.

Bruker må forholde seg til spam:

Det blir nevnt at det er et problem at brukerne må forholde seg til spammen som kommer. Dette skyldes som oftest at spamfilteret ikke er effektivt nok.

### 5.2.24 Spørsmål nr 31

Vurdering av data fra spørsmål om hvor lang tid det vil gå før en får et mindre spam-problem som en følge av bedre spamfiltreringsmetoder og regler og lovverk.



Illustrasjon 23 Oversikt over hvor lang tid det tar før spamsituasjonen blir bedre

Oversikten viser at det er 6% som tror på en snarlig forbedring, mens et flertall på 60% tror på en forbedring innen 6 år. 34% tror ikke at det vil bli noen forbedring i det hele tatt. Det som var grunnlaget da var blant annet det faktum at internasjonale lover og regler ikke vil være gode nok. Samt at så lenge det er penger å tjene på spam, så vil spammerene bruke mye ressurser på å finne nye teknikker for å komme forbi morgendagens spamfiltre.



## 6 Diskusjon

### 6.1 Risiko faktorer som fører til økt spam mengde

På bakgrunn av litteraturstudiet og intervjuene så har jeg kommet frem til en del faktorer som kan føre til økt spammengde. Det er en klar sammenheng mellom lav sikkerhet og høy grad av sannsynlighet for å sende og motta spam ufrivillig. En kan først se på de åpenbare risikofaktorene:

1. Ikke patchet/oppdatert server/programvare:

Hvis en er sårbar for kjente svakheter, som en følge av ikke å ha oppdatert software vil en ha en lavere sikkerhet. Flere av de kjente sårbarhetene som blir utnyttet er virus eller trojanere som sprer seg som spam.

2. Ikke sikkert trådløst nettverk:

Selv dagens WPA og WEP teknikker vil ikke sikre et nettverk tilfredsstillende. Ved å ha et slikt trådløst nettverk er det en risikofaktor, som igjen øker muligheten for spam.

3. Ikke sikre bruker pcer:

Ved å ikke ha krav til sikkerhetsnivået på brukernes pcer, vil disse erfaringsmessig være en risikofaktor for økt spam. Som Intervju spørsmål nr 16 og nr 17 tar opp. Dette kom frem under intervjuene at flere av de som hadde sendt spam fra nettverk sitt.

4. Nettetikette:

Ved en oppførsel/holdning som er lite sikkerhetsbevisst, vil en lett legge fra seg e-post adressen sin på nyhetsgrupper, forum og internettbutikker. Dette øker spam mengden.

De mindre opplagte risikofaktorene vil være blant annet følgende:

1. Bruken av lynmeldinger:

Sårbarheter i chatte program som MSN Messenger, ICQ, IRC og tilsvarende vil øke sjansen for spam, da trojanere, ormer og virus spres via brukerens adresse liste.

2. E-post til venner:

Ved e-post til mange venner samtidig uten bruk av BBC (blind kopi) vil en spre e-postadresser veldig fort, da til venner og til venners venner. Dette fører til stor og ikke heldig eksponering av e-postadressen.

3. Automatisk svar:

Ved å ha automatisk svar på e-postadressen sin når en f.eks. er borte så vil spammere registrerer aktivitet fra e-postadressen og eksponeringen av den gitte e-postadressen øker, med mer spam som sannsynlig utfall.

## 6.2 Vurdering av forskningsspørsmål

Vurderer her forskningsspørsmålene opp mot datagrunnlaget fra litteraturstudiet og intervjuet.

### 6.2.1 Er det behov for strenge norske spam lover?

Slik som det er i Norge i dag vil det ikke medføre store forskjeller med strengere lover. Dagens lov som regulerer spam er: Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven), som ble sist justert januar 2005.

Etter den siste justeringen ble det ulovlig å sende reklame til fysiske personer med mindre de har gitt sitt samtykke på forhånd.

Bedrifter som bryter forbudet vil kunne få bøter og etterhvert bli politianmeldt av Forbrukerombudet.

Juridisk sett befinner markedsføring på nettet og i andre digitale medier seg i en gråsoner. Tradisjonelt sett er det markedsføringsloven, kringkastingsloven og dels personopplysningsloven som sier hva som er lov og ikke i reklame. Dette gjelder ikke alltid for Internett. Norsk lov gjelder ikke når nettsidene (eller TV-stasjonen) ligger på utenlandske servere. Mange overser lovene - fordi det ikke er noen som har kapasitet til å kontrollere alle nettsider som finnes.

Loven i dagens formulering ser ut som den virker etter hensikten. Den krever at aktører på det norske markedet må hente samtykke for å få sendt ut spam e-post (spam nivå 3 og 4).

Bedrifter som bryter forbudet, får med forbrukerombudet å gjøre. Strafferammene i den nye markedsføringsloven er også betydelig skjerpet. Man risikerer nå større forelegg, fengsel i inntil seks måneder, eller begge deler.

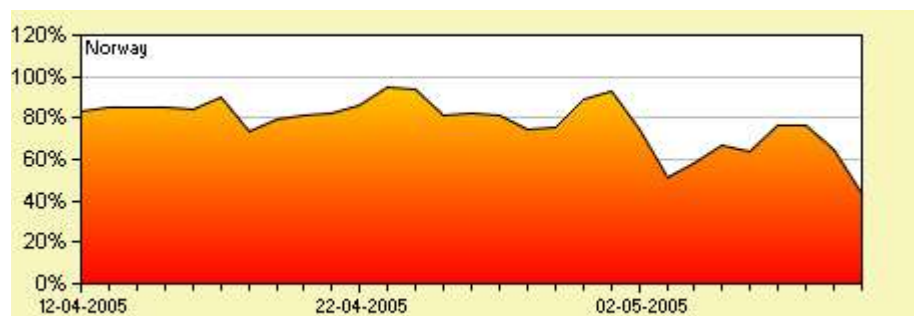
Det er flere aktører som har kommentert hull også i den nye loven. KK88-sjef Harald Marthinussen [32] har blant annet kommentert at det vil fortsatt være mulighet for å:

- sende ut uønsket e-post til jobb og privat som ikke inneholder reklame, men undersøkelser, konkurranser og annet som fører personer til en gitt hjemmeside.
- sende reklame til alle typer felles-adresser som [alle@bedrift.no](mailto:alle@bedrift.no). Mottakeren er da vanligvis bare en e-postliste-tjeneste som videresender e-post direkte til alle i bedriften.

Lovverket som hittil har stoppet uønsket reklame i både analoge og digitale postkasser har bare omfattet privatpersoner. Dette smutthullet oppdaget enkelte norske bedrifter i 2002 og begynte å sende ut reklame via e-post til norske arbeidstakere. Ut fra erfaringen fra tidligere så vil en anta at det er flere norske aktører som vil bruke de hullene som er i den nye markedsføringsloven fra 2005.

Ut fra intervjuene jeg har gjennomført så virker det som om it-avdelingene på utdanningsinstitusjonene har liten tro på at norske lover skal kunne reduserer spammengden. En del nevner at norske lover vil være effektive mot spam som kommer fra norske spammere. Jeg fikk også tilbakemelding om at de fleste norske aktører som sender spam på nivå 3 stoppet med utsending av slik spam etter en henvendelse. En vil også kunne dra den konklusjonen at det er bra med et lovverk i Norge som er effektivt og tydelig for de store massene.

Når en ser på oversikten over hvor mye spam vi har i Norge i april- mai 2005<sup>[33]</sup> fra sikkerhetsselskapet camendo så ser en at det er et stort behov for effektive anti-spam løsninger.



Illustrasjon 24 Oversikt over spam mengden for Norge 1 mnd i 2005.

En ser på illustrasjon nr 24 at det kan se t som en nedgang i spammengen. Men dette er ikke tilfelle hverken i Norge eller internasjonalt.

For å kunne løse spamproblemet med lover, så må det være internasjonale lover som alle land forplikter seg til å håndheve i hver sine land.

Det har flere åpenbare utfordringer, som kompetanse i det enkelte land(u-land), «fri-stater» og samarbeid over landene med lovverket. Internasjonale lover vil helt klart ha større effekt enn lover i Norge, ut fra det fakta<sup>[7]</sup> at e-postspam veldig sjeldent kommer fra Norge, sammenlignet med f.eks. USA og Sør-Korea. For at internasjonale lover skal kunne reduserer spammen må et stortstilt samarbeid til.

Men forbudet vil neppe gjøre den store forskjellen for IT-sjefer og enkeltbrukere - i prosent utgjør ikke europeisk spam mye i forhold til alt som kommer fra USA.

Et problem for lovens voktere er at spammerne i stadig større grad bruker zombienett – PC-er som er kapret gjennom ormer, trojanere og virus – til å sende e-postreklame. Etter en undersøkelse gjennomført i april 2004 anslo MX Logic<sup>[34]</sup> (Amerikansk antispam selskap) at 30 til 50 prosent av all spam stammer fra kaprede PC-er. En tilsvarende undersøkelse fra november-desember 2004 tyder på at andelen nå er økt til 69 prosent. Dette viser noe av utfordringen som lovene stilles over.

Det vil ikke være mulig å stanse spam med strengere norske lover, men det er mulig å regulere de få prosentene av spamen som kommer fra Norge.

### **6.2.2 Fungerer dagens spam løsninger tilfredsstillende for de store aktørene på det norske markedet ?**

Utdannings institusjonenes egen oppfatning av spamfilter løsningene viser at 94,6 % har en tilfredsstillende eller veldig tilfredsstillende spamfilter løsning. De nevner allikevel flere punkter som de ikke er fornøyd med blant annet effektiviteten, lite egnet SMTP-protokoll, bedre grensesnitt mot loggene og automatisk oppdatering av spamfilter programvare.

Det som ikke er tilfredsstillende er at dagens spamfilterløsninger i liten grad eller aldri er satt opp for å fange opp spam som sendes fra eget nettverk og ut på nettet. Undersøkelsen viser at kun 24% har et slikt system. Dette fører til en økt belastning for alle parter, og gjør at spam er et større problem enn strengt tatt nødvendig. Ifølge sikkerhetselskapet Sophus[7] så stammer ca 40% av all spam fra komprimerte pcer.

Av det som finnes tilgjengelig i dag så er det løsninger som fungerer tilfredsstillende for de store aktørene på det norske markedet. Hovedoppgaven etter min mening er å få tak i det rette systemet. Det finnes kommersielle appliances som er effektive og brukervennlige men som koster mye. Eller en kan legge seg på den andre siden med Open-Source produktet SpamAssassin som også er veldig effektiv kombinert sammen med f.eks. grålisting.

Etter å ha undersøkt hva som brukes og hva som finnes av produkter tilgjengelig så er ikke hovedproblemet at en ikke har et godt nok produkt, men at det produktet man har ikke er satt riktig opp eller oppdatert regelmessig nok.

Etter at en har funnet den løsningen som fungerer tilfredsstillende må denne implementeres og vedlikeholdes. Gjøres dette på en grundig måte vil anti-spam løsningen fungerer best.

### **6.2.3 Tar dagens høyskoler og universiteter det ansvaret som de burde for å stanse spam?**

Dagens utdanningsinstitusjoner tar hensyn til sine egne brukere på en tilfredsstillende måte ved at alle har et anti-spamsystem. Tar de det ansvaret de har ved at de er et knutepunkt(hub) for mange brukere?

Nettverk med mange brukere har et større moralsk ansvar enn en privat bruker f.eks. for å hindre spredning av spam. Det er først i år 2005 at samferdsels-departementet ser på saken og henvender seg til de norske ISP'ene gjennom en henstilling[35] spesielt rundt spam zombier. Det er en oppfordring til å iverksette konkrete tiltak for å prøve å identifisere komprimerte pc'er og luke ut disse. Samferdsels-departementet har nå inngått et internasjonalt samarbeid mot spam, gjennom «operation spam zombies»[36]. Der de plikter på å håndheve lovverket, forske på spam-teknikker, gi informasjon til forbrukere og næringsdrivende, ta politiske initiativ og samarbeid mellom offentlig og privat sektor.

#### **6.2.4 Hvilke tiltak for å redusere spam har mest effekt for de store aktørene på det norske markedet ?**

De tiltakene som hadde størst effekt for utdanningsinstitusjonene var å gå over til nyere spamfilterteknologi. Det ble også rapportert inn gode erfaringer og resultater ved oppgradering av eksisterende teknologi. Det gjelder å ligge et hakk foran spammerene i den teknologiske utviklingen hele tiden.

Ved å ha en spampolicy som er avtalefestet med alle brukerne oppnår man både økt bevissthet og reduserer spam mengden. Her er det et stort forbedrings potensiale for utdanningsinstitusjonene.

Det er blitt gjennomført statistiske undersøkelser for å se om det er en statistisk sannsynlighet for at geografisk tilhørighet eller erfaring og utdanning har noe å si på spamhåndteringen, uten at dette har vist noen sammenheng.

Det som ble registrert som det mest effekt tiltaket mot spam var å oppgradere spamfiltert, eller bytte over til en nyere type spamfilterteknologi. Det ble også vist under spamfilter-skiftet[37] som Universitetet i Tromsø hadde i 2004.

For å få den store effekten så er det flere tiltak som må til for å bekjempe e-postspam på en mest gunstig måte. Som undersøkelsen bekrefter kan en benytte seg av følgende:

1. Oppdatert spamfilter
2. Spam-policy
3. System for å hindre utsending av e-postspam.

Lover og regler vil også hjelpe, men det er ikke noe som vil på noen som helst måte erstatte spamfilter.



### **6.3 Oppsett på ideelt system.**

En vil i et ideelt system ikke måtte ta hensyn til eksponering som e-post adresser blir utsatt for på Internett, forum osv. Spamfilteret vil kunne skille e-post fra spam med 100% sikkerhet under alle omstendigheter.

I den virkelige verden vil et ideelt spamfiltersystem ha følgende egenskaper:

- høy grad av effektivitet uten å bli påvirket av høy belastning
- 0% falske positiv
- $0.1\% <$  falske negative

En vil i tillegg bruke andre alternative virkemidler:

- Opplæring av brukerne.
- En har tiltak for å sikre lav eksponering av e-post adresser på nettet
- En spampolicy som blir fulgt opp av de ansatte.

## 6.4 Etiske og lovlige betraktninger

En vil ikke måtte utføre noe som kommer andre mennesker på noen som helst måte til ugunst. Datagrunnlaget som ble dannet på grunnlag av intervjuet er anonymisert for å hindre sporbarhet.

Det ble ikke registrert noen personopplysninger eller andre person-sensitive data som reguleres av personopplysnings loven[38]

Det ble lagret informasjon som i noen tilfeller kan være skadelig gjørende hvis den kommer på avveie. Det er da skade på renommé og omdømme som kan bli utfallet. For å redusere denne muligheten til et minimum er det satt inn tiltak for å redusere sporbarheten til informasjonen. Det er også lagt vekt på at bedrift ikke skal føle seg lurt, ved å bidra med informasjon som kan fremstå som negativt.

Kopi av datagrunnlaget kan utgis ved henvendelse til meg, Erling Olai Hauge, Lunaveien 2B, 1160 OSLO eller på e-post via hjemmesiden <http://www.erlinghaug.com>. Det datagrunnlaget som da vil bli gitt ut vil være anonymisert.

## 7 Konklusjon og videre arbeid

### 7.1 Konklusjon

For å besvare problemstillingen om hvilke hovedutfordringer universitet og høyskoler står overfor i forhold til spamproblemet så må en se på følgende punkter:

- Utdanningsinstitusjonenes løsning av spam problematikken er på mange områder tilfredsstillende.
- Undersøkelsen viser at det er store svakheter i systemene når det gjelder utsending av spam fra eget nettverk. Undersøkelsen viste at kun 24% av respondentene hadde et slikt system.
- Dessuten hadde kun 3% en spampolicy som er avtalefestet, noe som viser seg å ikke være gunstig i forhold til spammengden. Spesielt vil dette bidra til å øke brukerens bevisstgjøring. Her har utdanningsinstitusjonene et forbedringspotensiale.

Norges lover som omhandler spam, markedsføringsloven, begynner å bli tilfredsstillende. Utfordringen ligger i å få flest mulig land til å implementere like lover.

Hypotesen; hverken ISP'er eller høyskolene og universitetene gjør en god nok jobb i forhold til spam i dag, blir oppfylt. Det er to hovedgrunner til dette:

- De fleste har ikke et system for å hindere utsending av spam.
- De fleste har ikke en avtalefestet spampolicy.

### 7.2 Videre arbeid

Ved å utføre en sammenligning mellom et ideelt antispam-system og dagens systemer på utdanningsinstitusjonene vil en da finne ut hvor stort gevinstpotensialet er. En vil da kunne gjøre en kost/nytte vurdering av en slik implementasjon.

Det vil være nyttig å måle effekten av å innføre et system som stanser utsending av e-postspam fra utdanningsinstitusjonene.



## REFERANSER

- 1: Postel, J., On the junk e-mail problem, 1975Internet Engineering Task Force., <http://www.rfc-archive.org/getrfc.php?rfc=706> (Besøkt Juni 2005)
- 2: Gauthronet, S. Drouard, E., "Junk" e-mail costs internet users euro 10 billion a year worldwide, 2001Unsolicited Commercial Communications and Data Protection, [http://europa.eu.int/comm/justice\\_home/fsj/privacy/studies/spam\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/studies/spam_en.htm)
- 3: The CAN-SPAM Act of 2003, 2003, <http://www.spamlaws.com/pdf/pl108-187.pdf> (Besøkt Juni 2005)
- 4: , E-privacy Directive Proposal COM(2000) 385, 2000EU, [http://europa.eu.int/comm/information\\_society/policy/framework/pdf/com2000385\\_en.pdf](http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf) (Visited Juni 2005)
- 5: , DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2002., [http://europa.eu.int/lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu.int/lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf) (Besøkt juni 2005)
- 6: , Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven), 2005,,Kapittel 1: Kontroll med markedsføring <http://www.lovdatab.no> (Besøkt mai 2005)
- 7: , Sophos reveals latest "Dirty Dozen" spam producing countries, 2004., <http://www.sophos.com/spaminfo/articles/dirtydozenaug04.html> (Besøkt juni 2005)
- 8: Graham Cluley, Sophos reveals latest "Dirty Dozen" spam producing countries, 2005., <http://www.sophos.com/> (Besøkt juni 2005)
- 9: B. Leiba and N. Borenstein, A Multifaceted Approach to SpamReduction, 2004,,In Proceedings of the First Conference on E-mail and Anti-Spam <http://www.research.ibm.com/spam/papers/multifacetedapproach.pdf> (Besøkt april 2005)
- 10: Best Practice Org, Best Practice in Email Spam Prevention and Eradication., 2004., <http://www.bestprac.org> (Besøkt juni 2005)
- 11: S. Hambridge, RFC 1855 - Netiquette Guidelines, 1995,,Network Working Group <http://www.faqs.org/rfcs/rfc1855.html> (Besøkt mai 2005)
- 12: David A. Turner and Daniel M. Havey, Controlling Spam through Lightweight Currency, 2003,,Department of Computer ScienceCalifornia

- State University San Bernadino  
[http://www.csci.csusb.edu/turner/papers/turner\\_spam.pdf](http://www.csci.csusb.edu/turner/papers/turner_spam.pdf) (Besøkt mai 2005)
- 13: Gautam, A., Stamping Out Spam, 2004,  
<http://www.cs.utexas.edu/ftp/pub/techreports/tr04-19.pdf> (Besøkt juni 2005)
- 14: Birrell, A., Dwork, C., Microsofts Penny Black Project, 2004,  
<http://research.microsoft.com/research/sv/PennyBlack/> (Besøkt juni 2005)
- 15: Abadi, M., Burrows, M., Manasse, M., Wobber, T., Moderately Hard, Memory-bound Functions, 2003,  
<http://research.microsoft.com/research/sv/pennyblack/demo/memory-final-ndss.pdf> (Besøkt juni 2005)
- 16: Open Source, SpamPal, 2005., <http://www.spampal.org> (Besøkt juni 2005)
- 17: Mustaler, J., Tagged Message Delivery Agent (TMDA), 2001,  
<http://www.tmda.net/> (Besøkt mai 2005)
- 18: Harris, E., The Next Step in the Spam Control War: Greylisting, 2003,  
<http://projects.puremagic.com/greylisting/whitepaper.html> (Besøkt mai 2005)
- 19: S. Yerazunis, W., Sparse Binary Polynomial Hashing and the CRM114 Discriminator, 2003,,Mitsubishi Electric Research Laboratories  
[http://crm114.sourceforge.net/CRM114\\_paper.html](http://crm114.sourceforge.net/CRM114_paper.html) (Besøkt mai 2005)
- 20: S. Yerazunis, W., The Spam Filtering Plateau at 99.9% Accuracy and How to Get Past It., 2004,,Mitsubishi Electric Research Laboratories, ( MERL ), MIT Spam Conference 2004  
<http://www.merl.com/reports/docs/TR2004-091.pdf> (Besøkt juni 2005)
- 21: S. Johansson, E., CAMRAM, 2002., <http://www.camram.org/> (Besøkt juni 2005)
- 22: Johansson, E., Best Practices for Sender-Pays Antispam Systems, 2004,,Spam Conferance 2004 <http://www.spamconference.org/> (Besøkt jan 2005)
- 23: Bishop, M., Computer Security Art and Science, 2003,ISBN 0-201-44099-7
- 24: S.J. Vaughan-Nichols, Saving Private E-mail, 2003,,IEEE Spectrum, vol. 40, no. 8, pp. 40-44

<http://www.spectrum.ieee.org/WEBONLY/publicfeature/aug03/spam.html>  
(Besøkt jan 2005)

25: Mirapoint, Spam Filtering Makes Workers Miss Deadlines, 2005,,  
<http://www.techweb.com/wire/161601072> (Besøkt mai 2005)

26: Hogan, J., Fed-up users, experts offer spam-fighting tricks, 2003,,  
<http://searchwin2000.techtarget.com> (Besøkt Juni 2005)

27: Jerry Berkman, Spam Survey Results, 2002,, [http://ist-socrates.berkeley.edu:7309/public/spam\\_survey.html](http://ist-socrates.berkeley.edu:7309/public/spam_survey.html) (Besøkt juni 2005)

28: Trend Micro Inc., Security and productivity concerns make spam a top IT priority, 2003,,  
<http://www.trendmicro.com/en/about/news/pr/archive/2003/pr101303.htm>  
(Besøkt Juni 2005)

29: The Transatlantic Consumer Dialogue (TACD), Report of TACD's online survey on spam, Oct - Dec 2003 , 2004,, <http://www.tacd.org> (Besøkt juni 2005)

30: Dennis W. K. Khong, AN ECONOMIC ANALYSIS OF SPAM LAW, 2004,, <http://www.eler.org/archive/2004/eler-2004-1-23-khong.pdf>  
(Besøkt Juni 2005)

31: Fluhner, S., Mantin, I. og Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, 2001,, [http://www.drizzle.com/%7Eaboba/IEEE/rc4\\_ksaproc.pdf](http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf) (Besøkt Juni 2005)

32: Einar Ryvarden, Ny lov stopper ikke all spam, 2005,,  
<http://www.digi.no/php/art.php?id=116126> (Besøkt Juni 2005)

33: Comendo, Cversikt over spamprosent av e-post i Norge 1 mnd i 2005, 2005,, Spam og antivirus selskap <http://www.comendo.dk> (Besøkt Mai 2005)

34: mxlogic inc., , 2004,, <http://www.mxlogic.com> (Besøkt juni 2005)

35: Samferdsels departementet, "Operasjon spam-zombier": Nettleverandørene må ta ansvar, 2005,, Pressemelding Nr.: 66/05  
<http://odin.dep.no/sd/> (Besøkt June 2005)

36: USA Federal Trade Comission, 2005 Operation spam zombies, 2005,  
<http://www.ftc.gov> (Besøkt June 2005)

37: Ingeborg Hellemo, grålisting - sølvkule eller skudd i foten, 2004,  
<http://www.uninett.no/uninytt/2004-1/kms.html> (Besøkt April 2005)

38: Justis- og politidepartementet, Lov om behandling av personopplysninger, 2000,, <http://www.lovdatab.no> (Besøkt Februar 2005)

39: Richard V. Dragan, 10 Tips for Fighting Corporate Spam, 2003, <http://www.pcmag.com/article2/0,1759,849550,00.asp> (Besøkt mai 2005)

40: B. Postel, J., RFC 821 - Simple Mail Transfer Protocol, 1982, <http://www.rfc-archive.org/getrfc.php?rfc=821> (Besøkt Juni 2005)



## Appendiks I Spam-Spørreskjema for utdanningsinstitusjonene

*Fremgangsmåte: Sett kryss/ring rundt rett alternativ. Prøv å gi et mest mulig riktig bilde av tilstanden. Spørreundersøkelsen er anonym.*

Fylles ut av meg :

1 Arbeider/jobber ved  
Ønsker til sendt rapport?

Navn:

Tlf:

2 Hvor mange brukere har dere ?

3 Type utdannings institusjon med fokus på : teknisk eller annet?

4 Er det utdanning på doktor grads nivå ?

5 Hvilken landsdel ?

Spørsmål :

*Kompetanse*

6 Hvilken utdanning har de ansatte som drifter e-post /spam ?

7 Hvor lang arbeidserfaring ved e-post /spam drifting har ansatt som drifter e-post /spam ?

*Risiko*

8 Har dere student boliger på nettet ?

9 Har dere trådløst nett tilgjengelig for brukerne ?

*Spamfilter*

10 Hvilket spamfilter bruker dere?

11 Hvilken type spam filter bruker dere?

Kommersielt	Open-source	Egenutviklet	Out-sourcet	Annet :	ukjent
-------------	-------------	--------------	-------------	---------	--------

12 Hvilket spamfilter teknologi(er) bruker dere ?

Hvitlistin g	Svartlistin g	Grålistin g	Innholdba sert	Statisti sk	Protokolls j ekk	ukjent
-----------------	------------------	----------------	-------------------	----------------	------------------------	--------

13 Hvor står spamfilteret(ene) ?

Front side	Server side	Kombinert	ukjent
------------	-------------	-----------	--------

14 Hvem har dere out-sourcet e-post driften til?

Ikke out-sourcet	UNINETT	Annen ISP	ukjent
------------------	---------	-----------	--------

15 Hvor stor prosent andel av e-post er spam ?

16 Har dere en offisiell spam-/viruspolicy kundene/brukerne blir informert om ?

Ja, ved e-post	Ja, ved brev/papir	Ja, ved web sider	ukjent
----------------	--------------------	-------------------	--------

17 På hvilken måte er kunde/bruker forpliktet til å følge policyen som det henvises til i spørsmål 16 ?

Avtaleforpliktet	Oppfordret	Ikke forpliktet	ukjent
------------------	------------	-----------------	--------

18 Hva blir prioritert mest av spam og virus ved IT-driften ?

Spam	Like mye	Virus
------	----------	-------

19 Hvor mange falske positive (spam som blir gjenkjent som e-post) får dere ?

20 Hvor mange falske negative (e-post som blir gjenkjent som spam) får dere ?

*Prioritering*

21 Hvor mange arbeidstimer brukes på spamdrifting per måned?

22 Hvor mange arbeidstimer er satt av til å holde seg oppdatert på spam-problematikken pr. måned ?

0 timer	0-1 timer	1-2 timer	2-4 timer	1 dag eller mer
---------	-----------	-----------	-----------	-----------------

23 Hvor mye tid er satt av til kompetanse økning vedrørende spam-problematikken i mnd. for ansatte ved e-post/spam drift?

0 timer	0-1 timer	1-2 timer	2-4 timer	1 dag eller mer
---------	-----------	-----------	-----------	-----------------

*Lover og regler*

24 Vil internasjonale/globale lover være et effektivt virkemiddel for å redusere spam ?

Veldig mye	Mye	Vet ikke	Lite	Veldig lite
------------	-----	----------	------	-------------

25 Vil norske lover være et effektivt virkemiddel for å redusere spam ?

Veldig mye	Mye	Vet ikke	Lite	Veldig lite
------------	-----	----------	------	-------------

26 Har dere et eget system for å oppdage utsendeelse av spam fra deres nettverk? Ja/nei

27 Har dere oppdaget brukere/kunder som *bevisst* sender ut spam fra deres nett? Ja /nei

28 Har dere oppdaget brukere/kunder som *ubevisst* sender ut spam fra deres nett? Ja /nei

*Fremover*

29 Hvordan fungerer deres nåværende spamfilterløsning ?

Antispam-drifting i stor skala

---

Veldig tilfredsstillende	Tilfredsstillende	Lite tilfredsstillende	ukjent
--------------------------	-------------------	------------------------	--------

30 Hvilke egenskaper ved dagens spamfilter fungerer ikke tilfredsstillende ?

31 Hvor mange år tror du det vil ta før spam vil være et mindre problem enn i dag pga. bedre håndtering av spammengden grunnet lover å regler og filtreringsmetoder ?

1-2 år	3-4 år	5-6 år	Aldri
--------	--------	--------	-------

## Appendiks II Tips for å redusere spam

Med utgangspunkt i Richard V. Dragans[39] tips får å få redusert spam så har jeg kommet frem til følgende 10 punkt.

Implementer et spamfilter på server siden. Utenom dette kan it-avdelingen gjøre følgende for å få redusere antall spam som kommer til spamfilteret.

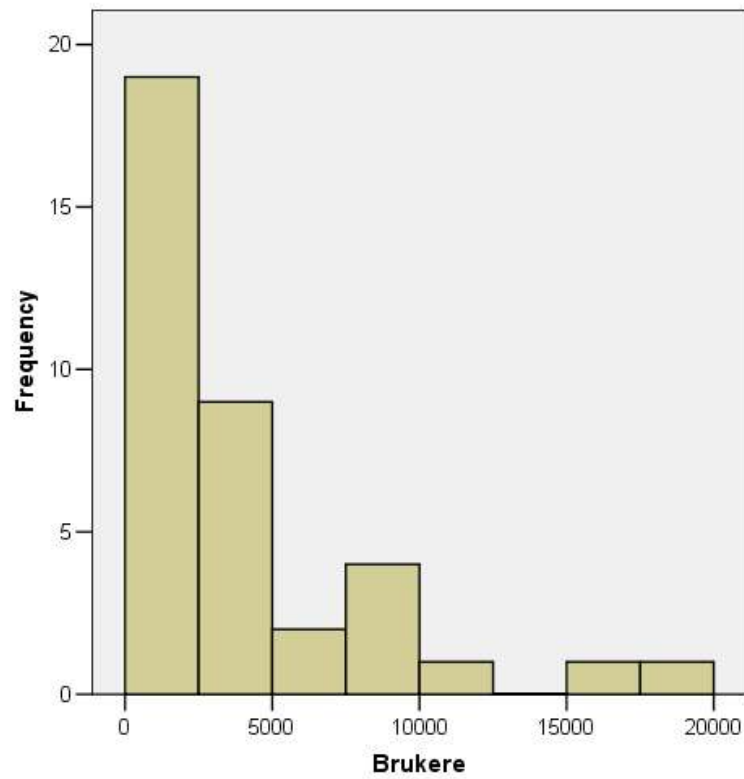
1. Lag en spampolicy send den ut til alle ansatte og publiser den på intranett/web sidene. Lag detaljstyrt instruksjon for hvordan behandle uønsket e-post. En god policy skal også spesifisere om det er lov å melde seg på nyhetsbrev, og registrere seg på nettet med e-post adresse. Alle ansatte/brukerene skal undertegne policyen.
2. Informer om at en ikke skal svare på spam, heller ikke for å bli tatt av e-post lister, da dette ofte bare gir spammeren en bekreftelse på at e-postadressen er i bruk.
3. Publiser ikke rene e-post-adresser på nettet. Bruk forkledning som: Ola\_Norman@hig[TA BORT DETTE].no, eller kodede e-post adresser. En må da alltid publisere en forklaring til hvordan en benytter seg av e-post adressene som blir lagt ut.
4. Begrens eller forby all personlig e-post aktivitet (på jobben), spesielt bursdags kort. En kan også vurdere om en skal forby banning i e-postene , hvis ikke det er et spesielt behov for å ha muligheten til det. Det fører til at det er lettere å sette opp spamfilteret.
5. Krev at brukerne skjuler sin e-postadresse, eller bruker alternative e-postadresser i nyhetsgrupper (newsgroup), forum eller online-chatting.
6. Sett brukernes web leser til det anbefalte sikkerhets nivået. Hvis ikke sikkerhetsnivået er satt høyt nok kan bots(små program koder/script) ta brukers e-postadresse når brukerne besøker hjemmesider.
7. Vær sikker på at brannmuren er satt opp til å stanse all trafikk som ikke er godkjent.
8. Installer antivirus på gateway, server og på klientene. Bruk gjerne antivirus produkt fra ulike antivirus selskap på hvert nivå. Hvis en løsning ikke fanger inntrengeren, så vil kanskje neste gjøre det.
9. Vær sikker på at din e-postserver ikke oppfører seg som et open-relay.
10. Påse at en følger RFC 821[40] SMTP standarden for e-postutveksling.



## Appendiks III Data fra intervju

Her blir mindre viktige data fra intervjuet representert, som blant annet de statistisk faste variablene.

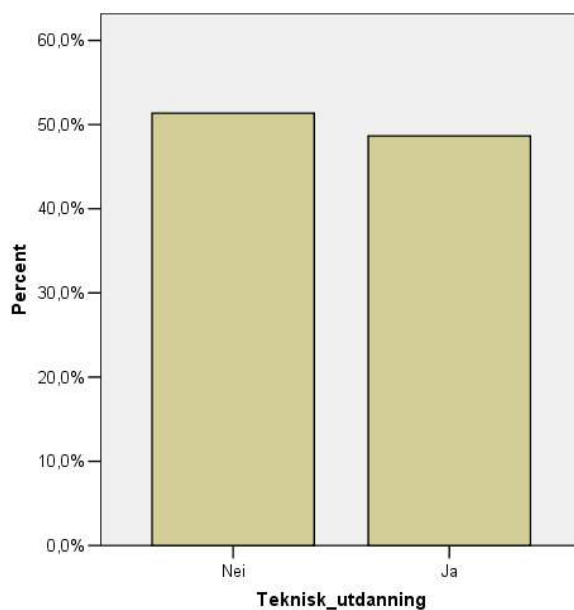
### Kommentar av om antall brukere, spørsmål nr 2:



Som en ser fra datagrunnlaget så kan man se at de fleste respondenter som kommer fra utdanningsinstitusjoner har mellom 1000-5000 brukere.

**Kommentar av data om institusjonen tilbyr tekniskutdannelse, spørsmål nr 3:**

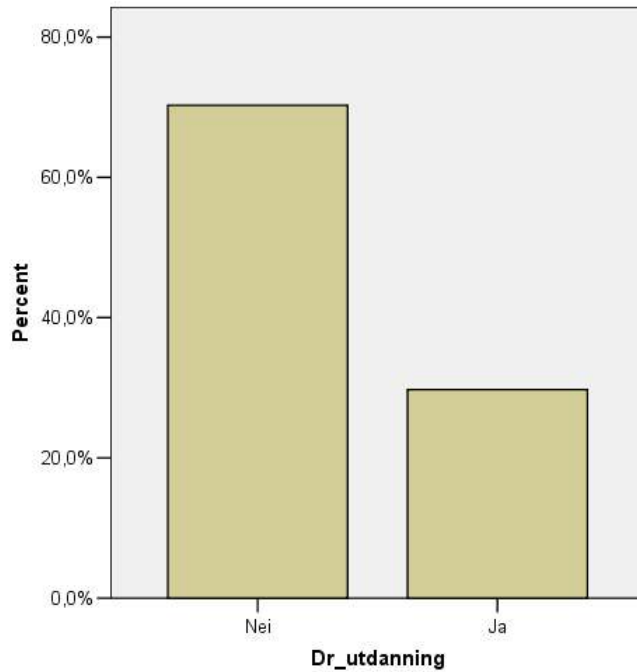
En ser her at det er en fordeling på ca 50%. Det er 49% som har undervisning av tekniske fag. Det er 51% som ikke har undervisning av tekniske fag. Ved å ha brukere



av tekniske fag vil det kunne være en faktor for mer spam, som følge av mer bruka av Internett. Det vil også kunne være en faktor for å kunne få mindre spam som følge av mer kunnskap om IKT generelt. Det ble utført en statistisk analyse for å se om det var en sammenheng mellom de som tilbyr tekniskutdannelse opp mot spammengden. Det ble ikke funnet en slik sammenheng

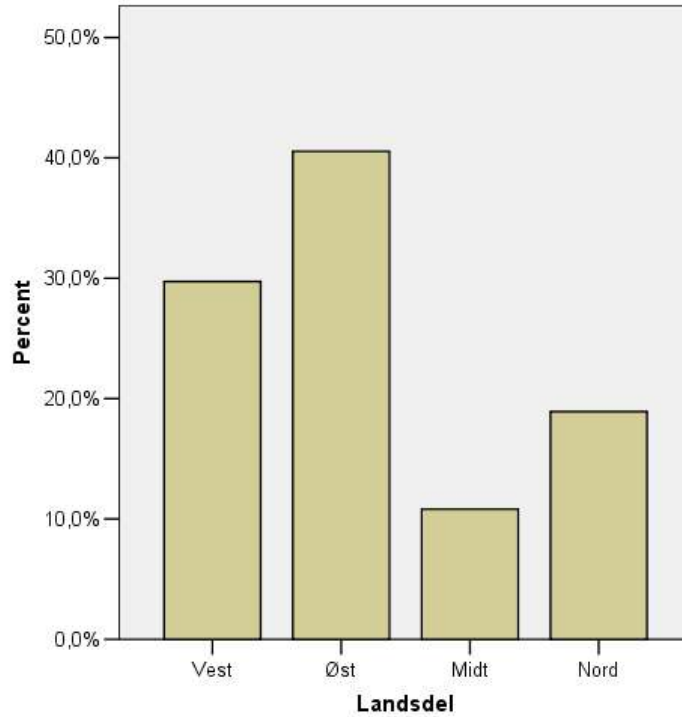


**Kommentar av data fra spørsmål om utdanning på doktorgradsnivå, spørsmål nr 4:**

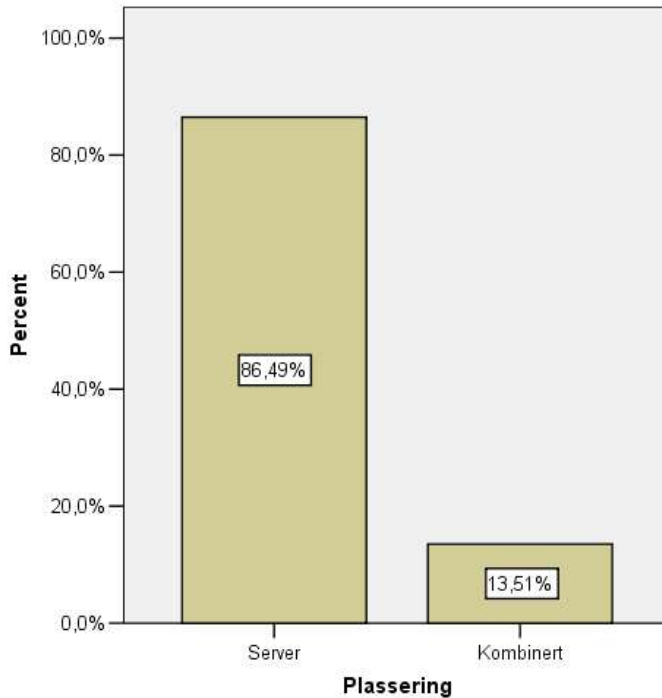


En ser at det er flertall for institusjoner som ikke tilbyr doktorgradsutdanning med 70%, og kun 30% tilbyr doktorgradsutdanning. Det ble utført en statistisk analyse for å se om det var en sammenheng mellom de som tilbyr doktorgrads utdanning opp mot spammengden. Det ble ikke funnet en slik sammenheng

**Vurdering av data fra spørsmål om geografisk plassering, spørsmål nr 5:**



Det er 30% som ligger på vestlandet, 40% på østlandet, 11% i midtnorge og 19% i nordnorge.

**Kommentar fra spørsmål om plassering av spam filteret, spørsmål nr 13**

Det ble registrert at det var 86% av de spurte som hadde plassert spamfilteret på serveren og bare der. De resterende 14% hadde plassert spamfilter både på serversiden og på klientsiden. En slik kombinert løsning vil i de fleste sammenhenger kreve mer vedlikehold og men vil kunne gi brukerne noe mer personlig konfigurering av filteret, som er en fordel ved. Brukervennligheten ved bruk av spamfilter som er plasserte på serveren vil i de fleste tilfeller være økt. Plassering på server anbefales ofte som det beste på grunn av at da tar en og får fjernet uønsket trafikk før det kommer inn i nettverket. Samtidig som det til være gunstig med hensyn til it-driftavdeling.