Att lära säkert

IT-säkerhet i Nätuniversitetets distansutbildningar

Päivi Jokela & Peter Karlsudd

Umeå Centre for Evaluation Research
November 2005

Förord

I denna rapport belyser och granskar fil dr Päivi Jokela och fil dr Peter Karlsudd, Kalmar Högskola, IT-säkerheten inom Nätuniversitetet. Studien har gjorts på uppdrag av UCER och utgör en delstudie inom ramen för ett större utvärderingsprojekt (se www.ucer.umu.se). Rapporten kan med fördel läsas som en fristående rapport. Den kommer också att användas som underlag i en slutrapport som presenteras nästa år.

Studien baseras på tre enkäter som distribuerats via e-post. Enkäterna har skickats ut till drygt 700 studenter och drygt 100 kursansvariga, samt cirka 50 IT-pedagoger. På grund av låg svarsfrekvens (39-65%) finns det skäl att vara försiktig med att dra några långtgående slutsatser om IT-säkerheten inom Nätuniversitetet utifrån denna studie, vilket forskarna också betonar. Den skevhet som kan finnas i enkätsvaren är att de studenter och lärare som besvarat enkäterna kan antas ha en positivare inställning till IT än studenter och lärare i allmänhet. Sammantaget kan den bild som framkommer i materialet vara något positivare än den generella bilden.

Detta är den första studie som undersöker IT-säkerhetsfrågor inom Nätuniversitetet ur studenters, lärares och IT-pedagogers perspektiv. Den utgör därmed ett viktigt bidrag till att ringa in och beskriva IT-säkerhetsproblematiken. Framförallt uppmärksammas kännedomen om regler och riktlinjer för IT-säkerhet, hur reglerna uppfattas och tillämpas, samt mer allmänt hur studenter och lärare tänker och agerar på IT-säkerhetsområdet. Författarna lämnar också förslag på vad som kan göras för att öka IT-säkerheten.

Rapporten aktualiserar en rad viktiga frågor. Bland annat uppmärksammas en del brister i IT-säkerheten, t.ex. att möjligheten till fusk är större jämfört med campusstudier, likaså framkommer brister i såväl kunskap om, som hantering av, personuppgifter och publicering på nätet. Samtidigt tycker studenter och lärare att IT-säkerheten i allmänhet är god. Studien tyder på att IT-säkerheten på flera sätt kan vara otillräcklig, därför kan säkerhetsfrågorna behöva granskas på fler sätt, t.ex. genom att IT-säkerhetsexperter granskar säkerheten. Mot bakgrund av denna studie finns det skäl att se över säkerhetsrutiner och noga följa utvecklingen kring IT-säkerheten inom Nätuniversitetet.

Umeå november 2005

Anders Hanberger
Projektledare för utvärderingen

ABSTRACT

The current higher education, both distance education and traditional campus courses, relies more and more on modern information and communication technologies (ICT). The use of computer systems and networks results in a wide range of security issues that must be dealt with in order to create a safe learning environment. In this work, we study the security status within the Swedish Net University, where several universities collaborate in order to offer ICT supported higher education distance courses. The total ICT-security is defined as a combination of computer security and information security, and the focus in this work is on the information security. The four main components of the information security that are used in the study are: confidentiality, integrity, availability and accountability.

The data gathering was made in two steps: first preliminary interviews then the main questionnaire. The interview respondents were a small number of students, teachers and ICT-experts at various universities, and the results of this preliminary study were then used to complete the questionnaire. The main questionnaire was sent to approximately 700 students, 100 lectures and 50 ICT-pedagogues. The answers were analysed both quantitatively and qualitatively. However, due to a relatively low answering rate, we must point out that the conclusions made are based on these limited results, and are therefore not necessarily generally applicable within the distance education.

The results show that both teachers and students involved in distance education consider that they have relatively good basic competence regarding the use of various ICT-resources. In addition, they consider that the computers and network connections they are using have adequate technical standard. However, the respondents also express a need for more information and training in various areas that are directly connected to information security issues. What is more, both students and teachers require that adequate computer support is constantly available. Several respondents have not developed procedures for backing up files in a regular basis. There seems also be some uncertainty concerning which measures should be taken in order to protect computer system from viruses and also what should be done if the computer is infected. Many teachers consider that the risk for cheating, especially for plagiarism, is greater in the distance education than in campus courses. These teachers also spend more time to prevent this problem in distance courses, and may have special procedures in order to detect plagiarism.

Even if several security issues are indicated, most of the respondents consider that the general ICT-security in distance education has a relatively high standard. This may be a sign of some discrepancy between the users' knowledge and their actual behavior when they use the computer systems.

INNEHÅLL

SAMMANFATTNING

Denna rapport undersöker IT-säkerheten inom Nätuniversitetet och bygger på tre enkäter som skickats ut till över 700 studenter och drygt 100 lärare samt ett 50-tal IT-pedagoger. På grund av låg svarsfrekvens, särskilt bland studenter, bör man dock vara försiktig med att dra några långtgående slutsatser.

Studien visar att distanslärare och studenter anser sig ha en relativt bra grundkompetens när det gäller datoranvändning. Lärarna har en något större datorkunskap och datavana än studenterna, studenter inom ämnesområdet Medicin/Vård bedömer sina kunskaper som lägst. Studenter och lärare anser sig ha god teknisk prestanda på de datorer som de använder vid distansstudier och distansundervisning.

Även om grundkunskaperna är tillfredsställande finns det hos både lärare och studenter ett uttalat behov av information och kunskap om regler och policy kring datoranvändning och man efterfrågar även utbildning i de regler som gäller för publicering på nätet.

Studenter och lärare är i regel nöjda med de distansverktyg som används, endast ett fåtal har problem att hantera verktygen. Många studenter och lärare efterlyser dock mer information och undervisning kring användandet av distansverktygen. Samma behov finns kring support och stöd. Studenterna litar på att lärarna handskas med personuppgifter på ett korrekt sätt och lärarna menar att de följer de regler som gäller. Det finns ett antal studenter och lärare som känt sig hotade eller personligt attackerade i distanskurser. Många studenter känner oro för att material som skickas kan komma fel, försvinna, eller läsas av obehöriga.

Det är många studenter och lärare som menar att de inte har några problem med versionshantering men det är trots allt ett flertal som anger att de har problem att hålla ordning på de olika dokumentversionerna. När det gäller säkerhetskopiering är det förhållandevis många, både lärare och studenter, som anger att de sällan gör någon säkerhetskopiering. Många studenter använder diskett som lagringsmedia vilket ur säkerhetssynpunkt inte är det mest lämpliga. Huvuddelen av studenterna och lärarna uppger att de konstruerar lösenord enligt de rekommendationer som ges.

Bland såväl studenter som lärare saknas det betryggande kunskaper om och hur man ska agera när datorn blivit smittat av datorvirus. Det finns relativt många studenter som inte uppdaterar sitt virusskydd och många av studenterna önskar ett ökat stöd inom detta område. Att program och dokument från osäkra miljöer hämtas hem och öppnas förekommer både i kretsen studenter och lärare. Ett flertal studenter rapporterar inte tekniska fel till kursansvarig eller IT-ansvarig/pedagog. Åtgärder som tydliggör hur man ska agera och vem man ska kontakta när tekniska problem inträffar efterfrågas från båda grupperna.

Det är en mindre andel studenter som anser att det är större risk för fusk vid distansstudier i jämförelse med traditionell campusutbildning. Här är det däremot nästan var fjärde lärare som indikerar att risken för fusk är större vid distansstudier. Många lärare vidtar speciella åtgärder för att beivra fusk men om dessa skiljer sig från den traditionella utbildningen framgår inte i resultatet. Det är dock många lärare som ägnar mer tid åt att förebygga fusk i distansutbildning i jämförelse med campusutbildning.

Trots uppenbara säkerhetsbrister anser studenter och lärare att IT-säkerheten är god. Det verkar följaktligen finnas en diskrepans mellan respondenternas kunskaper/attityder och deras agerande i verkliga situationer.

1 INTRODUKTION

Nätbaserad högre utbildning kännetecknas av att studierna är flexibla och i hög grad oberoende av tid och rum, men starkt beroende av välfungerande och pålitlig IT-infrastruktur. Studenterna arbetar ofta självständigt och förväntas att ta stort ansvar för sitt eget lärande. Likaså måste de kunna utnyttja IT- resurserna på ett effektivt sätt för att hantera stora mängder information och för att kommunicera med kursledare och övriga kursdeltagare.

Man kan lätt få uppfattningen att nätbaserad utbildning använder metoder som inte är tillgängliga för konventionell utbildning, ofta benämnd campusutbildning, traditionell utbildning eller närutbildning. Detta är inte med sanningen överensstämmande, då samma tekniska möjligheter många gånger erbjuds lärare som undervisar i campusutbildningen. Likväl är det fortfarande många lärare som inte utnyttjar de resurser som står tillförfogande (Karlsudd, 2002). Att utnyttja IKT (information- och kommunikationsteknologi) i undervisningen handlar många gånger mer om ett paradigmskifte och förändringar i undervisningskulturen inom den högre utbildningen, än om rent tekniska lösningar (Jandér, 2005).

Skillnaden mellan distansutbildning och den mer konventionella utbildningen är på väg att försvagas. De senaste årens snabba utveckling av datorer och nät har gett nya förutsättningar för att planera och genomföra utbildning (Dahlin, 2000).

> ”Skillnaden mellan dessa två utbildningsformer håller på att upplösas allteftersom datormedierad kommunikation blir mer vanlig även i den campusbaserade undervisningen.” (a.a., s 1)

Konsekvensen av denna utveckling är att kommunikationen i både campus- och distansutbildningarna i allt högre grad sker i form av skriftliga meddelanden och i viss mån även via audio- eller videoförbindelser. I distansutbildningen är fysiska möten mellan kursledare och kursdeltagare relativt få, likaså fysiska möten mellan kursdeltagare. Det som fortfarande skiljer campusutbildningarna från distansstudier är att det på campus finns större möjlighet för lärare och studenter att träffas öga-mot-öga och kommunicera muntligt, i viss mån även mera informellt. Likaledes finns det större möjligheter för studenterna att befinna sig på samma plats vid föreläsningar, gruppövningar och laborationer vilket kan gynna den muntliga, mer informella kommunikationen (Light & Cox, 2001).

Att kurserna blir alltmer beroende av IT-resurser ställer stora krav på utbildningens informationssäkerhet. För att skapa förtroende mellan kursdeltagare och kursledare är det ytterst väsentligt att den presenterade informationen är korrekt och lättillgänglig, och att kommunikationskanalerna är pålitliga. Likaså är det nödvändigt att kunna spåra originalkällan till informationen, inte minst när studenternas individuella kunskaper och färdigheter ska bedömas vid examination (Gunnarsson m.fl., 2002). Mot bakgrund av detta är det angeläget att uppmärksamma och undersöka de områden och faktorer som berör IT-säkerheten. Denna undersökning har för avsikt att granska och diskutera dessa frågor.

1.1 Rapportens disposition

I nästa kapitel ges en detaljerad bakgrund och definitioner till det aktuella området. IT-säkerheten definieras som en kombination av datorsäkerhet och informationssäkerhet. Undersökningens tyngdpunkt ligger i informationssäkerheten. Informationssäkerheten och dess fyra delområden samt deras koppling till distansutbildningen behandlas liksom hot och risker i distansutbildningen. Säkerhet ur ett juridiskt perspektiv diskuteras och därefter behandlas fusk och dess betydelse för informationssäkerhet i distans-utbildningen. Kapitlets avslutande del behandlar etik och moral samt användaransvaret.

Kapitel tre fastställer undersökningens syfte.

I kapitel fyra beskrivs metod och praktiskt genomförande av den empiriska undersökningen. I samma kapitel redogörs för de inledande intervjuerna med IT-pedagoger, kursansvariga lärare och en säkerhetsansvarig. Kapitlet avslutas med en detaljerad beskrivning av enkätundersökningar utförd bland studenter, kursledare och IT-ansvariga/IT-pedagoger.

I det näst sista kapitlet redovisas resultatet från enkätundersökningen. Detta femte kapitel kompletteras med Bilaga 1, där enkätsvaren finns presenterade i tabellform. I kapitlet ges även en deskriptiv sammanfattning av bakgrundsvariablerna. De övriga avsnitten i resultatkapitlet är kategoriserade enligt följande: Kunskap och attityder, agerande, teknik samt kontroll och uppföljning.

Rapporten avslutas med en diskussion där resultatet belyses utifrån informations-säkerhetens fyra delområden. Därefter presenteras de pedagogiska konsekvenser som kan bli aktuella. Diskussionskapitlet avslutas med förslag till fortsatt forskning.

2 BAKGRUND

Kombinationen av billiga datorer, snabb multimediateknik och Internet har enligt många bedömare skapat de förutsättningar som behövs för att förnya lärandet och att öppna nya möjligheter för det livslånga lärandet (Edenholm, 2000). Distansutbildning kan vara idealisk för att skapa en situation där utbildningen är lärarstödd i stället för lärarledd (Hjelm & Sandred, 1997). Men i takt med att utbudet av distansutbildningar ökar blir även kraven på IT-säkerheten större. Ett större antal studenter ska hanteras i de system som erbjuder avancerad kommunikation och lärsystem.

När man studerar säkerhetsfrågor, är det viktigt att göra skillnad mellan datorsäkerhet och informationssäkerhet. Datorsäkerheten avser de tekniska aspekterna i samband med obehörig åtkomst och förändring eller olika slags störningar i ett datorsystem, medan informationssäkerhet inkluderar säkerhetsproblem som är kopplade till hantering av information i olika verksamheter. I detta arbete definieras IT-säkerhet som en kombination av datorsäkerhet och informationssäkerhet. Information är för många verksamheter den viktigaste resursen. Det är därför utomordentligt viktigt att den behandlas på ett korrekt sätt. En ovarsam hantering kan äventyra verksamhetens mål på såväl kort som lång sikt. Det är inte bara sekretessbelagd information som behöver skyddas. Om den publika informationen manipuleras eller förstörs kan det få förödande konsekvenser för verksamheten. För att nå upp till en önskad skyddsnivå kan det krävas en serie insatser (Brandt & Wennberg, 2004; Statskontoret, 1997:29). Inom Nätuniversitetets utbildningar handlar det många gånger om att göra korrekt och riktig information lättillgänglig, snarare än att skydda information från insyn. I detta arbete är det huvudsakligen informationssäkerheten som står i centrum för undersökningen.

Ett modernt datorbaserat utbildningssystem grundas på en stark interaktivitet mellan mänskliga användare och datorer och många forskare betraktar den mänskliga, ”mjuka” delen av systemet som avgörande för systemets totala säkerhetsnivå (Mikkonen, 2000; Gali, 1992). En fullgod informationssäkerhet kräver en välstrukturerad organisation med tydliga riktlinjer och strategier och tillförlitliga tekniska lösningar. Samtidigt är det inte tillräckligt att den organisatoriska och tekniska grunden till säkerheten finns ifall systemets användare tillämpar regler på ett slarvigt sätt eller helt struntar i att följa dessa. Det är av ytterst vikt att samtliga användare är medvetna om potentiella säkerhetsrisker vid användandet av datoriserade system och känner ansvar för den totala säkerheten. Användare måste ha accepterat säkerhetssystemet och ha hög motivation att använda dess funktioner. En viktig förutsättning för detta är att användaren har tillräcklig förståelse och de färdigheter som behövs för att kunna dra nytta av systemet, vilket vanligtvis kräver utbildning. Man kan också konstatera att det inte alltid är enkelt att förena användbarhet med informationssäkerhet. (Mikkonen, 2000; Brandt & Wennberg, 2004; Allwood, 1998) Inom universitet och högskolor är det särskilt viktigt att säkerhetsåtgärderna inte bygger hinder för den enkelhet och tillgänglighet som är nödvändig för verksamheten.

2.1 Informationssäkerhet

Informationssäkerhet kan delas upp i fyra delområden: riktighet, tillgänglighet, sekretess och spårbarhet (Statskontoret, 1997:29).

2.1.1 Riktighet

Begreppet riktighet innefattar personintegritet, systemintegritet och informationskvalitet. Med integritet menas att de objekt som är föremål för skyddet ska fredas mot obehörig förändring. Förlust av riktighet kan vara förlust av användardata eller andra IT-resurser som tillhandahåller servrar, program och nät. Förlusten kan förorsakas avsiktligt eller oavsiktligt genom obehörig förändring av data, tillägg eller radering av meddelande, filer osv. Med informationskvalitet menas att de tjänster och de data som tillhandahålls är felfria och har rätt detaljeringsgrad. Information som produceras ska vara korrekt, aktuell och begriplig (Statskontoret, 1997:29).

När studenterna planerar sin nätutbildning söker de information om t.ex. kursernas/programmens innehåll, tidsplan och examinationsformer. Om dessa uppgifter är felaktiga och/eller inaktuella eller om de presenteras på ett obegripligt sätt kommer informationskvaliteten att försämras. Eftersom kursinformation ofta spelar en avgörande roll för studentens val av kurs, kan sämre informationskvalitet påverka utbildningens ansökningssiffror i negativ riktning.

Ett annat allvarligt problem är att inkorrekta eller otydliga beskrivningar av kursens innehåll och examinationskrav kan resultera i att studenter riskerar att bli underkända. I vissa fall kan otydliga examinationskrav leda till att kursdeltagare blir anklagade för fusk, t.ex. om flera studenter samarbetar vid individuell hemtentamen (se även avsnitt 2.5. för mera detaljerad beskrivning av fusk).

Om kursen använder automatiserade test som en del av examinationen är det speciellt viktigt att kursledaren kontrollerar testresultatets riktighet innan det registreras. Dels är examinatorn ansvarig för att testet fungerar på ett korrekt sätt dels omfattas datorbaserade test där enskilda studenters personuppgifter hanteras av personuppgiftslagen, (Legala handboken, Nätuniversitet).

2.1.2 Tillgänglighet

Tillgänglighet innebär möjligheten att för behöriga användare utnyttja resurser efter behov och inom önskad tid. Om användare genom t.ex. driftsavbrott och störningar hindras från att utföra funktioner i IT-systemet är det att betrakta som exempel på tillgänglighetsförlust. För en organisation som kräver hög grad av tillgänglighet kan kravet vara att nå systemet 24 timmar per dygn och att antalet korta avbrott (mindre än 10 minuter) i genomsnitt inte får överstiga två per vecka (Statskontoret, 1997:29).

Under kursperioden måste studenterna ha kontinuerlig tillgång till kursmaterial, program och system. För den asynkrona delen av nätutbildningen kan man sätta tillgänglighetskrav på 24 timmar per dygn, sju dagar i veckan och samma nivå bör rimligtvis gälla även för tillgången till biblioteksresurser. Om tekniska problem uppstår är det också viktigt att studenterna har tillgång till IT-support - både i asynkron och i

synkron form, såsom e-post resp. telefon. Att kunna kommunicera med kursledaren är likaledes en väsentlig förutsättning för lyckat studieresultat. Tidigare undersökningar har visat att studenterna ställer höga krav på lärarnas tillgänglighet (Westerberg & Mårald, 2004) och det är därför viktigt att kunna etablera en rimlig miniminivå för tillgängligheten när det gäller bl.a. lärarresurser och IT-support.

Speciella tillgänglighetsproblem och förlust av värdefull information kan uppstå vid hantering av längre dokument, t.ex. hemuppgifter, rapporter och uppsatser, om studenten inte tillämpar korrekta rutiner för versionshantering och säkerhetskopiering. Dessa problem kan accentueras när flera personer arbetar med samma dokument.

E-postbilagor och nedladdade program och filer kan vara smittade av skadlig kod (virus, mask, trojan) som sedan sprids vidare via nätverket. Likaså finns det risk för obehöriga intrång då ”hackers” får åtkomst till IT-resurser och utnyttjar dem på ett skadligt sätt. Dessa säkerhetsproblem kan i värsta fall leda till förlust av information och skador i datasystem och nätverk. Lärosäten har i regel rutiner för hantering av skräppost, skadlig kod och intrång för den IT-utrustning som finns på campus, men om studenter mestadels arbetar hemifrån måste de själva ansvara för skydd av sin datorutrustning och den information som finns lagrad i datorn. Goda rutiner skulle bl.a. innebära att skydda sin hemdator med antivirusprogram och brandvägg samt att lagra dokument på lärosätets server eller på ett annat sätt försäkra sig om regelbunden säkerhetskopiering av den viktigaste informationen.

2.1.3 Sekretess

Sekretess innebär att känslig information inte får avslöjas för obehöriga. All information ska vara underordnade regler för åtkomst och behörighet. Förlorande av sekretess uppstår när en behörig eller obehörig användare försöker få access till information som användare inte har rättighet till. Förlust av sekretess omfattar också oavsiktlig tillgång till känslig information. Detta kan uppstå när en utskrift blir synlig eller tillgänglig för någon annan eller när en skärmbild blir synlig för obehöriga. Ett annat exempel är när elektronisk post går till fel person på grund av fel i systemet. Med konfidentialitet menas ofta i IT-sammanhang ett slags insynsskydd som syftar till att skydda hemlig eller känslig information från obehörig insyn. Obehörig åtkomst gäller inte bara informationen utan även andra IT-resurser som t.ex. avsiktlig eller oavsiktlig körning av program som man inte är behörig att exekvera (Statskontoret, 1997:29).

Kursmaterial i form av text och bilder innehåller sällan speciellt känsliga uppgifter och sådant material kan ibland finnas tillgängligt på nätet i helt oskyddad form. Det kan dock vara viktigt att påpeka att kursmaterial inklusive de studentarbeten som publiceras på nätet omfattas av upphovsrättslagen (SFS 1960:729; SFS 2005:359; SFS 2005:360). En vanlig situation är att studenterna måste vara registrerade för att bli behöriga och få access till lärosätets lärplattform och även för enskilda kurser.

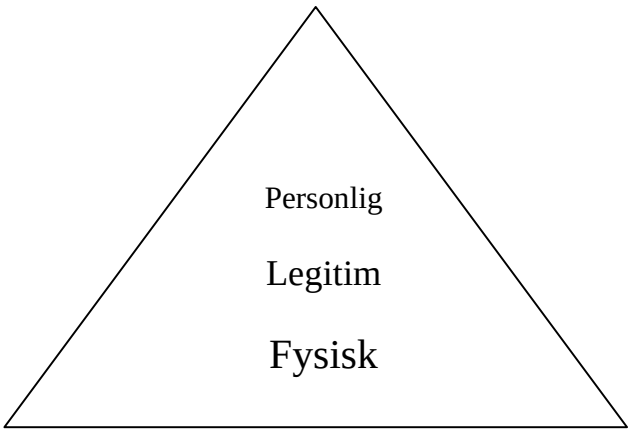
Om än kursmaterialet som sådant har låg säkerhetsklassning, är sekretess viktig när studenter vill ha konfidentiell kommunikation med kursledaren. Eftersom studenter och lärare har få tillfällen att träffas öga mot öga, måste det ömsesidiga förtroendet byggas upp genom virtuella möten i en trygg miljö. Likaså måste studenternas personuppgifter i samband med kursregister hanteras enligt personuppgiftslagens (SFS 1998:204) bestämmelser så att den personliga integriteten skyddas.

2.1.4 Spårbarhet

Spårbarhet och oavvislighet ger skydd från förluster och brott mot säkerheten. Saknas denna spårbarhet innebär det att användaren inte kan hållas ansvarig för sin IT-verksamhet och att systemadministratörer och systemoperatörer inte kan knytas till sina administrativa aktiviteter, användarna inte kan göras ansvariga för användning av tjänster eller utförande av transaktioner.

Oavvislighet är en typ av spårbarhet. Det innebär att användaren inte i efterhand kan förneka att han/hon har skickat eller mottagit ett meddelande. Användaren kan heller inte förneka att han/hon deltagit i eller orsakat en handling. Autentiseringen av användare möjliggör spårbarhet. Finns det möjligheter att logga in under falsk identitet uppstår brist på korrekt spårbarhet. Falsk inloggning innebär obehörig åtkomst med alla de risker och hot som kan följa (Statskontoret, 1997:29).

Autentisering inom distansutbildningen kan beskrivas i tre nivåer. Den första, den **fysiska**, är att genom IP-adressen identifiera den dator som använts. Den andra nivån, den **legitima,** är att identifiera vem som är personligt ansvarig för det användarnamn och lösen som använts vid inloggning. Den legitima nivån är även giltig för digitala signaturer. Den tredje nivån, den **personliga**, innebär att försäkra sig om att det som skrivs och skickas verkligen producerats/författats av den som står bakom användarnamnet, vilket många gånger är den svåraste nivån att kontrollera (figur 2.1).



Figur 2.1. De tre nivåerna för autentisering

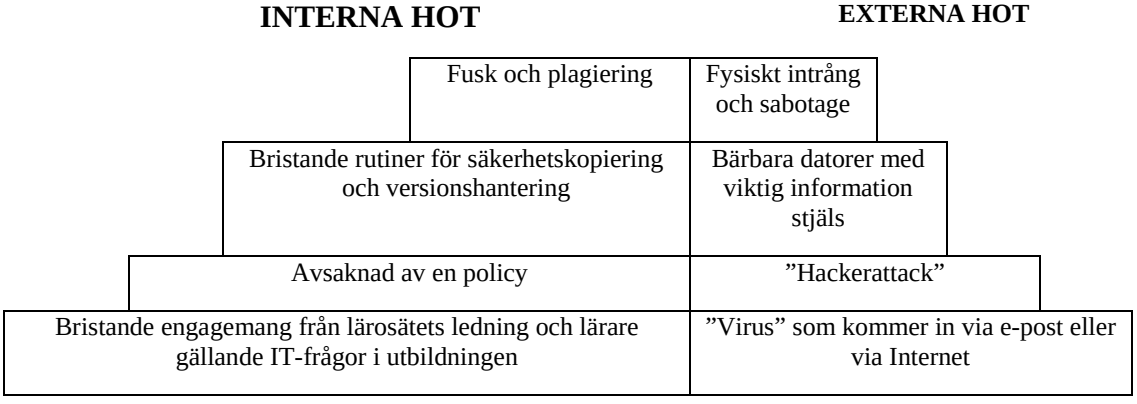
En fördel med att access till kursens information och kommunikation kräver inloggning med lösenord är att kursdeltagarnas verksamhet blir spårbar, varje användare blir explicit ansvarig för sina handlingar. Eftersom kursdeltagare inte kan förbli helt anonyma bör risken för olämpligt uppförande minska vid kommunikation med lärare och övriga deltagare. Kursledare kan följa upp deltagarnas aktivitetsnivå, ifall detta är önskvärt för t.ex. examination och betygssättning. För kursdeltagare innebär spårbarhet bl.a. en bekräftelse på att inlämningsuppgifter och rapporter har skickats och mottagits av lärare i rätt tid.

Det traditionella fallet av bristande spårbarhet inträffar när någon loggar in under falsk identitet så att en obehörig användare kan få access till skyddad information eller andra IT-resurser. Vid nätutbildningar finns också risk för att en behörig användare lämnar in en studieprestation under sitt eget namn även om arbetet är gjort av någon annan, med andra ord är det fråga om fusk (se avsnitt 2.5). Kritik mot IT-säkerheten vid examination har framförts i en nyligen genomförd undersökning vilket kan indikera behov av särskilda krav på säkerheten vid examinationstillfällena (Westerberg & Mårald, 2004).

2.2 Hot och risker

Ett hot kan definieras som ”en möjlig, oönskad händelse som, om den inträffade, skulle få negativa följder”. (Statskontoret, 1997:29, s 15) Risk kan definieras som sannolikheten för att hotet ska realiseras. Det är viktigt att organisationer har klart för sig vilka hot som kan finnas mot den egna verksamheten då hotbilden ändras över tid och riktar sig mot olika delar i organisationen. De vanligaste hoten mot IT-verksamheten är vardagliga händelser, som förorsakas av b1.a. brister i administrativa rutiner och i själva IT-verksamheten. Hot av denna kategori brukar kallas oavsiktliga hot. Alla organisationer som använder informationsteknik kommer någon gång att drabbas av negativa händelser som t.ex. kraschade skivminnen och överföringsfel som uppkommer helt oavsiktligt. Utöver dessa ouppsåtliga hot finns även de interna avsiktliga hoten (a.a.). Interna hot kan vara svåra att skydda sig mot, då det ofta utförs av personer med tillgång till datorsystemet (Borg m.fl., 1997).

Ett stort antal organisationer är dessutom utsatta för externa hot, som ofta kan benämnas avsiktliga hot, dvs. att någon enskild eller en organisation försöker komma över viss information eller sabotera hela IT-verksamheten. Det är viktigt att bedöma hotbilden mot IT-verksamheten och att bedöma sannolikheten för att hotet ska realiseras. Exempel på hot som måste observeras i distansutbildningen presenteras i figur 2.2.



Figur 2.2 Risktrappan, exempel på interna och externa hot

Enligt Gali (1992) är de helt avgörande riskerna med datasäkerhet grundade i den mänskliga faktorn. Ofta är det den egna personalen som oavsiktligt skapar situationer

som hotar säkerheten. Anledningen är i de allra flesta fall bristande utbildning för en viss arbetsuppgift och/eller stress. Oavsiktliga handlingar från den egna personalen står för ca 65 procent av hotbilden och avsiktliga handlingar från den egna personalen för ca 32 procent. Angrepp från individer utanför organisationen svarar endast för tre procent av de hot som riktas mot organisationen (a.a.).

2.3 Säkerhet ur ett juridiskt perspektiv

Som ansvarig för säkerheten inom en organisation måste man hela tiden göra avvägningar mellan säkerhetsåtgärdernas nytta, ställd mot de resurser som måste avsättas och den möjliga integritetskränkning som åtgärderna kan medföra. Hur mycket kontroll som är nödvändig, vilka lagar som styr insatserna som planeras och vilka reaktioner som är att förvänta av personalen är frågor som måste diskuteras. Inom högskolans och universitetets verksamhet kan administrationsrättigheter över personalens arbetsdatorer vara en fråga som väcker diskussionen om integritet.

Den lagtext som reglerar företags och organisationers rätt att föra personuppgifter är Datalagens 28 paragrafer. Ofta krävs det licens från Datainspektionen för att upprätta register. Den som upprättar ett personregister måste också, förutom personernas tillstånd, anmäla det till Datainspektionen eller utse ett personuppgiftsombud och i vissa fall dessutom söka tillstånd (Datainspektionen, 1999).

Största delen av det kursmaterial och de studentarbeten som publiceras på nätet vid nätbaserade utbildningar omfattas även av upphovsrättslagen. Den tidigare lagen har i år uppdaterats för att även inkludera upphovsrättsliga frågor i den digitala miljön. (SFS 1960:729; 2005:359; 2005:360).

2.3.1 Personlig integritet

Skydd för den personliga integriteten är för traditionella medier främst reglerat genom lagar om förtal och förolämpning med mera samt genom pressetiken. När det gäller Internet tillkommer dessutom personuppgiftslagen, PUL. PUL förbjuder att namn och andra personuppgifter offentliggörs på Internet, om inte berörda personer gett sitt otvetydiga samtycke. PUL har kritiserats hårt för att den inskränker yttrandefriheten. Detta har lett till att lagen mjukades upp och från januari år 2000 är det tillåtet att publicera ”harmlösa” personuppgifter på nätet. En annan konsekvens blev att ”ringa brott” inte längre bestraffas. Uppmjukningen berör inte spridningen av känsliga personuppgifter (Datainspektionen, 1999). Det finns ett antal brott som kan definieras som yttrandefrihetsbrott vilket handlar om missbruk av yttrandefriheten. Dessa brott begås genom spridning av viss information. Det kan gälla barnpornografibrott, uppvigling, hets mot folkgrupp, olaga våldsskildring eller förtal och förolämpning (Truedson, 1999).

PUL gäller inte för personuppgifter som uteslutande publiceras för litterära, konstnärliga och journalistiska ändamål. Den gäller inte heller för grundlagsskyddade publikationer. Den gamla datalagen existerar parallellt med PUL fram till oktober år 2001 (a.a.).

För den utbildning som vill publicera namn på personer finns två alternativ. Antingen betraktar man de aktuella uppgifterna som harmlösa och publicerar dem utan hänsyn till PUL, eller också tar man det säkra före det osäkra och ser till att skaffa en underskrift från alla som kan tänkas komma att nämnas vid namn (a.a.).

2.4 Fusk

Ett specifikt säkerhetsproblem som förekommer i utbildningen i samband med inlämningsuppgifter, rapportskrivning och examinationer är fusk, där avsikten är att examinator får en felaktig uppfattning av studentens kunskaper och färdigheter. Ett sådant förfarande kallas för vilseledande i Högskoleförordningen (1993:100):

> ”Disciplinära åtgärder får vidtas mot studenter som
>
> 1. med otillåtna hjälpmedel eller på annat sätt försöker vilseleda vid prov eller när en studieprestation annars skulle bedömas..”
>
> (HF 1993:100, 10:e kap 1§)

Det finns flera olika sätt att försöka vilseleda examinator, Högskoleverket använder i sina dokument en uppdelning i fyra olika kategorier (Högskoleverket, 2003:24R; 2004:17R; 2005:28R)

1) Användning av otillåtna hjälpmedel vid salskrivningar, t.ex. fusklappar, otillåten litteratur, otillåtna elektroniska hjälpmedel
2) Otillåtet samarbete med andra personer t.ex. vid hemtentamen, rapportskrivning
3) Användning av plagiat genom att inhämta och delvis eller helt kopiera andras arbeten (texter, bilder, musik) från Internet, olika databaser och böcker utan att hänvisa till originalkällan
4) Ändring av poäng på tentamen.

Av dessa fyra kategorier är det främst 2) och 3) som har en specifik anknytning till nätbaserad undervisning där största delen av kommunikationen mellan examinator och student sker i skriftligt form. Det är också viktigt att påpeka att enligt upphovsrätten har upphovsmannen alltid ideella rättigheter till sitt verk och man måste således namnge källan när man citerar ur offentliga texter eller använder annat material (SFS 1960:729; 2005:359; 2005:360).

Det kan vara svårt att avgöra ifall en student avsiktligen har kopierat någon annans text och bilder eller om det snarare är frågan om ovana vid att använda citat och att hänvisa till referenser. För att plagiering ska räknas som vilseledande i Högskoleförordningens mening måste den betraktas som en målinriktad aktivitet med direkt uppsåt. Slarv med källhänvisningar eller oavsiktlig parafrasering leder inte till disciplinära åtgärder, (Jareborg, 2002).

Högskoleverket har sedan 2001 kartlagt disciplinärenden vid landets lärosäten och man kan tydligt se en trend av ökande antal upptäckta fall av fusk under tiden 2001-2004, från 127 till 368. Denna undersökning visar även att plagiat är den största

kategorin av fusk och även den kategori som ökar snabbast. (Högskoleverket 2002, 2003:24R,; 2004:17R; 2005:28R)

Att just plagiering upptäcks så ofta kan åtminstone delvis bero på den aktuella debatten om fusk som leder till större uppmärksamhet bland examinatorer. Många lärosäten har även börjat använda olika digitala verktyg för att snabbare kunna jämföra studentarbeten med olika befintliga källor. Det är samtidigt viktigt att påpeka att Högskoleverkets kartläggning visar hur många fall som årligen bedöms, men den ger inte svar på hur utbrett fusket verkligen är vid landets lärosäten. Det kan även påpekas att trots ett ökande antal disciplinfall utgjorde andelen fällande domar år 2004 endast ca 0,1 procent beräknat per det totala antalet studenter (Högskoleverket 2005:28R). Man har inte kunnat påvisa att fusk skulle förekomma oftare vid nätbaserade utbildningar (Gunnarsson m.fl., 2002).

2.4.1 Fusk och informationssäkerhet

Enligt den tidigare uppdelningen av informationssäkerhetens fyra delområden, kommer fusk i form av otillåtet samarbete vid individuella uppgifter och plagiering främst att beröra områdena riktighet och spårbarhet. Om man på ett vilseledande sätt presenterar andra individers kunskaper som ens egna, har man förvanskat information och därmed avsevärt försämrat informationskvaliteten. Lägre informationskvalitet innebär försämrad tillförlitlighet och detta kan allvarligt skada den tillit som finns mellan lärare och studenter och mellan studenter som arbetar i samma grupp. På längre sikt är försämrad informationskvalitet ett betydande hot mot lärosätets akademiska trovärdighet (Wiedersheim-Finn, 2005).

Fusk och plagiat innebär även problem med spårbarhet, om den inlämnade studieprestationen inte kan härledas till rätt person. Eftersom den student som har som avsikt att fuska vid en hemtentamen eller lämnar in plagierade arbeten vanligen är behörig användare och loggar in under sin rätta identitet, kan man inte lösa detta problem på samma sätt som om det var fråga om en obehörig åtkomst. Det finns digitala sökverktyg som examinator kan använda som hjälp vid granskningen av inlämnade dokument. Ett intressant alternativ som tas upp i Gunnarssons m.fl. rapport (2002) skulle vara att i större utsträckning utnyttja muntliga examinationer med hjälp av videokonferenser.

Även det förebyggande arbetet på organisations- och individnivå är viktigt för att uppnå bättre spårbarhet. Nya examinationsformer som fokuserar på feedback och kontinuerligt lärande kan fungera bättre än traditionella examinationer som huvudsakligen används som inlärningskontroller (Gunnarsson m.fl., 2002; Martin, 2004). Studenter och lärare behöver gedigen utbildning i informationshantering, speciellt när det gäller källkritik och hantering av källmaterial (Wiedersheim-Finn, 2005). Likaså bör det etiska användaransvaret kontinuerligt debatteras i utbildningar där IT är ett centralt verktyg.

2.5 Etik och moral

Individens ansvar och frihet att handla på eget initiativ har ökat dels som en följd av att uppgifter delegeras, dels genom informationsteknikens snabba utveckling. Etik och moral uppfattas ibland som synonymer men det går att göra en skillnad. Moral kan avse människors praktiska handlande medan etik avser då den teoretiska reflexionen över moralen och dess grund (Karlsudd, 2001). I ett informationssystem som är öppet mot Internet ställs organisationen inför frågor av etisk och moralisk karaktär. Det är ofta tillgången till kontroversiell information som väcker frågor om värden och normer. Ett annat problem är plagiering, vilket diskuterades i föregående avsnitt. Tillgången till information i största allmänhet har ökat drastiskt och nuförtiden kan man även hitta åtskilliga webbplatser där färdigskrivna rapporter inom olika områden kan hämtas, s.k. papermills (Wiedersheim-Finn, 2005). Olika organisationer har olika åsikter för vad som är acceptabelt och därmed olika strategier för att möta dessa problem.

Ett sätt att möta problemet är att genomföra tekniska åtgärder ett annat kan vara att bättre följa progressionen i studentens skrivande. När det gäller kontroversiell information, använder man mestadels förebyggande åtgärder i form av olika digitala ”vakter” som genom filtrering syftar till att minska den oönskade informationen. Filtreringsprogrammen gör att det blir svårare att komma åt kontroversiellt material och risken för att överraskas minskas. Många anser att censur- och filtreringsprogrammen är allt för grovmaskiga och att de verkar på ett godtyckligt sätt (Truedson, 2000).

Det finns inga tekniska hjälpmedel som direkt kan förhindra fusk, däremot kan de inlämnade arbetena granskas med hjälp av digitala sökverktyg. Det är då möjligt att upptäcka mer eller mindre direkta avskrivningar av andras arbeten. Andra typer av plagiat, t.ex. användning av någon annans idéer som sina egna, kan enbart upptäckas av mänskliga examinatorer och är mycket svårare att urskilja. Digitala ”antiplagiat”-verktyg kan bli värdefulla hjälpmedel, men de måste användas på ett sådant sätt att de inte underminerar förtroendet som finns mellan examinator och student (Martin, 2004).

Regelsystem eller ”användarpolicy” är ett annat sätt att hantera samma problem. Skillnaden mellan regler och policy är att regler oftast fokuserar på vad som inte få göras medan användarpolicy anger vad som får göras. En genomtänkt policy kan ge vägledning för hur personal och studenter ska förhålla sig vid användningen av Internet.

Ett tredje och kanske mest effektivt sätt är att utveckla en etisk och moralisk handlingsberedskap inför den enorma mängden digital information som finns tillgänglig för studenter. Grunden för denna är att personal och studenter diskuterar det som finns att tillgå på nätet. Detta är diskussioner som förs kring organisationens gemensamma värdegrund.

2.6 Användaransvaret

Det svåraste hotet mot informationssäkerheten kommer, som tidigare nämnts, från den egna organisationen. Fel, misstag och slarv som förorsakats av bristande kompetens eller en otydlig ansvarsfördelning i organisationen är relativt vanliga. Det därefter vanligaste hotet och kanske de allvarligaste är avsiktliga interna angrepp. Det är viktigt att

användare känner sig delaktiga i säkerhetsarbetet för att minska riskerna för oavsiktliga fel och avsiktligt missbruk.

Säkerheten i en organisation fungerar bara om användare är medvetna om vad det är man vill skydda och på vilket sätt det ska skyddas. Användare har ett stort ansvar för att en hög säkerhetsnivå upprätthålls. För att skapa denna ska organisationen utarbeta råd och direktiv om hur det dagliga säkerhetsarbetet ska genomföras. När det gäller att bedöma hot som kommer inifrån organisationen måste man arbeta med stort omdöme och kanske mer på ett allmänt plan för att inte kränka enskilda individer (Borg m.fl., 1997).

Att bygga upp ett hundraprocentigt skydd mot hot och risker är inte ekonomiskt försvarbart. Det gäller att väga kostnaden för upprätthållandet av säkerheten mot kostnaden av en förlust när skydd saknas. I riskanalysen lyfter man fram de åtgärder och riktlinjer som är tillämpbara vid t.ex. förluster och intrång. Målet är att finna rutiner och hjälpmedel för att förebygga sannolikheten för och åtgärda effekterna av missöden och angrepp. Det gäller att hantera dessa situationer med minimal störning av verksamheten. Då säkerhetsarbete inte genererar några direkt synliga intäkter är det viktigt att redogöra för de kostnader som går att undvika (a.a.).

När en riskanalys formuleras uppstår ofta en rad positiva sidoeffekter. Fokusering av säkerheten i hela verksamheten på ett strukturerat sätt ökar säkerhetsmedvetandet hos samtliga användare. Sannolikt förbättras dessutom kommunikationen och förståelsen för varandras behov och roller i organisationen.

2.6.1 Utbildning i säkerhet

Utbildning av användare är ett sätt att realisera ett praktiskt säkerhetsarbete i distansutbildning. För att inte äventyra att en säker miljö raseras av ett misstag byggt på okunskap, är det viktigt att ha kontinuerlig utbildning i säkerhet. Alla användare inom organisationen måste ha kunskaper och färdigheter så att de själva kan identifiera ett hot mot säkerheten och informera detta till den säkerhetsansvariga. Det är viktigt att skapa och upprätthålla ett säkerhetsmedvetande i organisationen och se till att regler och rutiner följs. Det gäller att bevaka de datorresurser organisationen förfogar över. Ett säkerhetsmedvetande byggs upp i form av strukturerade kurser, men också genom en mer informell utbildning användare emellan (Allwood, 1998). Ett exempel på detta är att en anställd på institutionen har ett särskilt ansvar för hjälp och handledning kring säkerhetsfrågor.

Bevakning av datorresurserna är allas ansvar men framförallt är det organisationens systemadministratörer som har de största resurserna när det gäller att känna igen onormala förändringar i datorsystemen. Utbildning måste givetvis differentieras då användare och systemansvariga har klart skilda behörigheter, ansvarsområden och kompetenser. Det gäller att samtliga användare har en fullgod helhetsbild och att de känner till de säkerhetsklassningar som gäller för olika typer av information och resurser i organisationen. Att utbilda användarna i de säkerhetsfunktioner som standardprogrammen innehåller är lämpligt och då kanske särskilt att peka på de brister som dessa funktioner många gånger är behäftade med. Det är omöjligt att erbjuda en utbildning som täcker allt detta men det gäller att uppmuntra till kunskapsinhämtning på egen hand (a.a.).

3 SYFTE

I detta arbete definieras IT-säkerhet som en kombination av datorsäkerhet och informationssäkerhet. Undersökningen har som syfte att kartlägga kunskaper, attityder, problem och beteenden rörande IT-säkerhet i vid mening, vid ett urval av Nät-universitetets distansutbildningar. Med studenten i centrum belyses och diskuteras området utifrån fyra huvudområden nämligen*; riktighet, tillgänglighet, sekretess* och *spårbarhet.*

I undersökningen kommer följande att fokuseras:

- Kunskaper, agerande och attityder gällande IT-säkerhet
- Uppföljning och kontroll av administrativ/teknisk säkerhet
- Förekomst och hantering av fusk i samband med inlämningsuppgifter, examination o.dyl.
- Användande av säkerhetssystem och deras pålitlighet
- Framtida möjligheter, hot och risker kring distansutbildning
- Exempel på säkerhetsåtgärder.

4 METOD

Den empiriska undersökningen hade två huvuddelar: inledande intervjuer med två IT-pedagoger, två kursansvariga och en säkerhetsansvarig samt enkätundersökningar bland studenter, kursledare och IT-ansvariga/IT-pedagoger. Intervjuerna kan betraktas som en inledande inventering av säkerhetsproblem i nätbaserade utbildningar och de bidrog således till konstruktionen av enkätens frågematris.

4.1 Inledande probleminventering

För att fånga in aktuella frågeställningar runt IT-säkerhet i distansutbildning utfördes fem intervjuer med personal engagerade i Nätuniversitetets utbildningar. Från ett universitet och en högskola intervjuades två personer med IT-pedagogisk funktion, två kursansvariga för distanskurser och en säkerhetsansvarig. Samtliga intervjuer tog sin utgångspunkt i områden som de intervjuade upplevde som säkerhetsproblem. Till den inledande probleminventeringen adderades ytterligare tre intervjuer med distans-studenter. Då den inledande probleminventeringen var explorativ till sin uppläggning redovisas här nedan respondenternas utsagor utan att kategoriseras.

IT-pedagogerna
I intervjuerna med IT-pedagogerna kom säkerheten kring datorprogram att inledningsvis behandlas. När det gäller dataprogram menar IT-pedagogerna att det finns ett antal stabila program som används frekvent. Det är ordbehandlingsprogram, kalkylprogram, bild- och presentationsprogram, e-postprogram och webbläsare. Dessa program laddar med automatik ner uppdateringar för bättre prestanda och säkerhet. Konsekvenserna av detta kan bli att vissa funktioner slutar att fungera, men IT-pedagogerna anser att det är bättre att rätta till dessa störningar, än att riskera mer omfattande säkerhetsproblem genom att inte tillåta uppdateringar. På kort sikt kan det bli störningar, men på längre sikt blir säkerhetsriskerna mindre, menar de intervjuade. En av IT-pedagogerna tycker att det kan vara positivt att klara ut mindre problem med lärarna. Det ges då ofta tillfälle att prata om andra IT-pedagogiska frågor.

> För mig är störningarna inte helt negativa. När det blir något problem tekniskt pratar vi ofta vidare t.ex. Fick du in det här kursinslaget i din webbkurs? eller hur vi ska jobba vidare med webbsidan. Man försöker göra det negativa till något bra och ibland funkar det.

Det har funnits en del problem att öppna dokument direkt från webben framhåller en av de intervjuade. Det är ordbehandlaren och webbläsaren som inte korresponderar på det sätt man önskar. Några större ansträngningar för att komma till rätta med detta speciella problem har inte gjorts, då de intervjuade anser att det alltid är bäst att ladda ner dokumentet på skrivbordet innan det öppnas.

Det händer att studenter bryter mot de regler som gäller för datorhanteringen på skolan. Vid en institution kopplade en student in sin egen dator på nätverket vilket innebär en ökad risk för att otillåtna program och virus kommer in i nätverket. Studentens otillåtna agerande blev ett disciplinärende och studenten blev avstängd från

datoranvändning under en månad. För övrigt anser IT-pedagogerna att IT-säkerheten är relativt god. Det som tyvärr händer både lärare och studenter är att man glömmer att logga ut sig som användare innan man lämnar datorn. En av de intervjuade utrycker detta på följande sätt:

> Användarna har relativt begränsade möjligheter att ställa till någonting vad det gäller säkerheten. Det som ibland händer är att dem lämnar en dator utan att logga ur och då kan ju vem som helst göra saker. Skriva ut och radera filer och beställa varor och kanske till och med skriva ut prov.

Ett annat problem som IT-pedagogerna belyste var att belastningen på nätet tidvis kunde vara ganska hög och att överbelastningen försvårade arbetet. IT-pedagogerna ansåg vidare att det är viktigt att studenterna får information om vad som orsakar fel som uppkommer. Ett exempel på detta är när man utnyttjat allt lagringsutrymme på sitt konto på högskoleserven. När kvoten är full kan det få oönskade effekter på en rad funktioner. Denna information har inte riktigt fått fäste i studentgruppen.

Ett område som kan orsaka oro hos IT-pedagogerna är säkerhetskopieringen och lagring av data. Studenter har kommit gråtande när de har förlorat hela sitt arbete för att de inte har lagrat och säkerhetskopierat på ett tryggt sätt. Studenterna uppmanas därför att spara på sitt högskolekonto vilket IT-avdelning säkerhetskopierar varje dygn. En av IT-pedagogerna ger exempel på när studenters agerande kring säkerhetskopiering varit otillräckligt.

> En student hade bara jobbat mot en diskett, och hela arbetet gick förlorat. Det borde hon inte ha gjort. Det räcker att man bryter disketten lite så funkar det inte. Vi hade en annan student som hade jobbat hela förra terminen på en återbrännbar cd. Sedan hade den slutat fungera och allt arbete gick förlorat.

Ett problem som tar relativt stort utrymme i intervjun är hur lärare kontrollera ursprunget eller äktheten i studenters inlämningsuppgifter. Det kan t.ex. vara att studenten kopierar text eller låter någon annan utföra uppgiften. När det gäller otillåten kopiering menar en av de intervjuade att det faktiskt är lättare att kontrollera äktheten i elektroniska inlämnade dokument, då man kan matcha den med den text som finns på nätet.

En IT-pedagog menar att distansstudenterna tillsynes har det lättare än campus-studenter att lagra och få struktur på sina inlämningsuppgifter. Distansstudenterna har tydliga instruktioner hur de ska lämna in sina uppgifter antingen via ett forum eller via e-post. Utöver detta sparar huvuddelen av studenterna en kopia av uppgiften på sin dator eller andra lagringsmedia t.ex. ett USB-minne. Många gånger gör campusstudenterna på samma sätt, men det finns lärare som inte tillåter de elektroniska distributionsformerna, utan vill ha dokumentet i pappersform. En av fördelarna med att lämna in uppgifterna elektroniskt uppges vara att man får bekräftelse på att dokumentet kommit fram. En av IT-pedagogerna utryckte sig på följand sätt:

> Alla elektroniska system bekräftar att ditt dokument är uppladdat och är det fel på mottagarens e-post får du bekräftelser på det. Det som händer på skolan ibland, är att elevarbeten försvinner ur facken och då vet man inte var dom tagit vägen eller som en av lärarna som slängde hela högen med inlämningsuppgifter i fel korg nämligen papperskorgen.

Ett problem som diskuteras av IT-pedagogerna är att det ibland kan uppstå konflikter pga. att någon eller några studenter beter sig illa mot varandra. Det kan i vissa diskussionskonferenser utvecklas ett dåligt klimat vilket skapar problem för läraren att hantera. Å andra sidan menar de intervjuade att de elektroniska kanalerna på ett sätt är mycket ”ärligare” då det alltid går att följa ett inlägg till en person.

> Personattacker är ju sånt som kan uppstå, men det går alltid att härleda det till någon person till skillnad från om du skickar ett vanligt brev med vanlig post eller lämnar en lapp i ett fack.

De intervjuade tar upp problematiken kring lösenorden som enligt säkerhetspolicyn borde bytas var tredje månad. Många lärare har haft samma lösenord i flera år. Men de intervjuade menar att det är bättre att användaren minns sitt lösenord än att lärarna pga. av att det regelbundet byts måste ha komihåglappar som ofta blir liggande under skrivbordsunderlägget.

Kursansvariga

Intervjuerna med de kursansvariga kom inledningsvis att gälla studenternas förmåga att hantera datorer och elektronisk kommunikation. Av de båda intervjuade bedömdes datakompetensen bland studenterna vara relativt god. Studenter som anmäler sig till kurserna är oftast vana vid tekniken och de som är ovana lär sig snabbt att hantera tekniken. Några vänder sig till lärcentran för att få hjälp.

Ingen av de intervjuade har varit med om några större driftsstörningar i distanskurserna. Det har hänt att en lärplattform varit ur funktion en helg, vilket vållat irritation bland de studerande. Enligt en kursansvarig kan det vara problem när användarna använder program som inte läraren har installerat på sin dator. Men den intervjuade uttryckte ”det brukar ordna upp sig till slut”. En av de kursansvariga menar att studenten i regel bara kan göra begränsad skada, då de finns ett dygns backup på alla uppgifter.

En kursansvarig menar att det för några studenter kan kännas obehagligt att lägga ut uppgifter, antingen personuppgifter eller text man producerat, men denna känsla försvinner oftast när osäkerheten om tekniken försvinner. Att det många gånger är svårt att få studenterna aktiva i konferensen beror inte på tekniken, det är mer ett pedagogiskt problem menar de intervjuade. Det finns mycket mer att önska när det gäller information och utbildning påpekar de båda respondenterna. Mycket av de inledande teknikfrågorna skulle säkert kunna reduceras.

Säkerhetsansvarig

Den säkerhetsansvariga gör ingen skillnad på IT-säkerheten vid campus- respektive distanskurser. Problematiken är densamma, möjligen får distansstudenten mindre support och det finns inte någon hjälp att tillgå på kvällar och helger. När man ska hjälpa en distansstudent över telefon är det många gånger mer problematiskt då man inte vet hur datorn är konfigurerad och då datorn inte går att fjärrstyra.

När det gäller IT-regler och policy har alla, studenter som lärare, fått informationen men den IT-ansvariga är inte säker på att informationen når fram, vilket nedanstående citat exemplifierar.

> Vi har ett krav att alla ska ta del av reglerna men frågan är vad de läser, har förstått eller kommer ihåg. Detta gäller både lärare och studenter.

Enligt den intervjuade har många lärare låg IT-kompetens. Många har inte klart för sig om man säkerhetskopierar på hårddisken eller servern. Mer utbildning skulle förbättra situationen för både lärare och studenter. Ett annat problem som är vanligt är att man lånar ut användarnamn och lösenorden till varandra. Ofta får det inga allvarliga konsekvenser, men risken finns att det leder till större problem. När det gäller lösenord menar den IT-ansvariga att det är bättre att ha ett bra lösenord som inte byts så ofta. Att byta lösenord varje år kanske skulle vara en bättre rekommendation. Det största hotet mot IT-säkerheten, menar den intervjuade, är att hackers vill komma åt bandbredd genom att ta över högskolans servrar. Ett annat hot är stöld av information vilket mer gäller forskningsmiljöerna och inte i första hand undervisningsmiljöerna.

Studenter
Av de studenter som intervjuades inför frågekonstruktionen var två relativt vana distansstudenter medan en nyligen närmat sig distanstekniken i sin första kurs. Samtliga intervjuade tyckte att de var försiktiga i början, då de inte riktigt litade på tekniken. Men attityden ändrades efter kursens gång då de upptäckte att tekniken fungerade bra. Samtliga av de intervjuade önskade att information, utbildning och support kunde vara bättre. En av studenterna läste två distanskurser parallellt och framförde önskemålet om att de olika utbildningarna använde samma typ av lärplattform. Många av de frågor som diskuterades kom att handla om lärarens insats och agerande. Ett exempel på denna typ av frågor var önskemålet om snabbare respons på inlämningsuppgifter från läraren.

Sammanfattning och konsekvenser för frågekonstruktionen
Av de inledande intervjuerna kom några intressanta säkerhetsaspekter att framträda. Tillförlitlighet och riktighet i datorprogram, problem kring uppdateringar, säkerhetskopiering och otillåten kopiering var några av de områden som behandlades. Förtrogenhet med tekniken, datorsupport, utbildning, tillförlitlighet och dilemmat runt lösenord var ytterligare områden. Problematiken om hot och olämpligt uppträdande utgör ytterligare exempel på problem som genererade frågor i enkätundersökningen. De som avhandlades i intervjuerna gick att härleda till de fyra områden, *riktighet, tillgänglighet, sekretess* och *spårbarhet* vilka utgjorde grunden för frågekonstruktionen.

4.2 Urval och enkätdistribution

En förteckning över Nätuniversitetets kurser och kursansvariga lärare förmedlades genom denna myndighets försorg. Enligt vårt uppdrag delades Nätuniversitetets kursutbud i tre delgrupper: humaniora och samhällsvetenskap (Hum/Sam), medicin och vård (Med/Vård) samt naturvetenskap och teknik (Na/Te). Som urvalskriterium användes NU:s klassificering av kurserna.

Som datainsamlingsverktyg användes ett webbenkätsystem, ”Enkätarkitekten” (Östlund, 2000). De personer som blev utvalda enligt proceduren nedan fick ett missiv (Bilaga 2) som innehöll allmän information om undersökningen och en länk till webbenkäten. Om de valde att delta i enkäten registrerades deras svar i systemet och två

påminnelser skickades automatiskt om svar inte hade erhållits till vissa bestämda datum. Genom att använda ett automatiserat system kunde respondenterna förbli helt anonyma och resultatet kunde inte kopplas till någon enskild individ.

Studenturval
Urvalet av studenter gjordes i två separata steg. I steg ett valdes 15 kurser från delgruppen Na/Te och från vardera gruppen Med/Vård och Hum/Sam 14 kurser och ett program. Valet skedde slumpmässigt inom delgrupperna även om valet av program blev mera styrt eftersom endast få program fanns med i kursutbudet. Därefter skickades en förfrågan till kursansvariga via e-post om de var villiga att ge undersökningen tillträde till kursen och om de hade möjlighet att distribuera enkäten till studenterna. Efter ett visst bortfall bland kurserna, deltog fem kurser från Hum/Sam, tre kurser och ett helt studieprogram från Med/Vård samt fyra kurser från Na/Te i undersökningens andra steg. I steg två distribuerades missivet till alla studenter som var registrerade på de kurser/program som efter bortfallet ovan ingick i undersökningen. I elva av fallen skickades följebrevet via e-post och i två av fallen gjordes missivet och webbenkäten tillgängliga via den aktuella kursens informationsforum. Det totala antalet studenter som på detta sätt fanns med i enkätundersökningen var 896.

Kursledarenkät
I undersökningen valdes slumpmässigt ut 140 kursansvariga lärare, från delgrupperna Hum/Sam, Na/Te kurser och Med/Vård. Därefter skickades ett missiv via e-post till de utvalda lärarna. På samma sätt som vid studentenkäten innehöll missivet allmän information om undersökningen och en länk till webbenkäten.

Enkät till IT-ansvariga IT-pedagoger
Ett e-postbrev skickades till registratorn vid samtliga lärosäten (27 stycken) som ger utbildningar via Nätuniversitet. I brevet ombads att ett följebrev och länk till webbenkäten vidarebefordras till de personer som ansvarar för IT-utbildningarna. I detta fall kan man inte redovisa ett exakt antal av de brev som efter vidarebefordringen kom fram till IT-ansvariga/pedagoger eftersom ett antal brev kan ha stannat vid det första steget utan att vi blev meddelade om detta. Likaså är det möjligt att brevet vidarebefordrades till flera personer vid ett och samma lärosäte.

4.3 Enkätkonstruktion

Utifrån inledande intervjuer, litteraturstudier och teoretiska ställningstaganden formulerades ett 60-tal frågor med stöd av nedanstående modell (tabell 4.1). I modellen används en matris där raderna representerar informationssäkerhetens fyra delområden och kolumnerna beskriver delarna i den process som sker när en nätbaserad kurs genomförs, här benämnt kunskap/attityder, agerande, teknik och kontroll/uppföljning.

Kursens viktigaste och mest dynamiska resurser är de förkunskaper och attityder som kursdeltagare och lärare har med sig. En annan del är den administrativa infrastrukturen som lärosätena och Nätuniversitetet tillhandahåller och som t.ex. ansvarar för registrering av studenter och deras studieprestationer. Den tredje resurs-

relaterade delen är den teknik som är tillgänglig och som i nätbaserade utbildningarna måste inkludera både den tekniska utrustningen, de lärplattformar som erbjuds av lärosätena och den utrustning och program som kursdeltagarna har på sina studieplatser. När kursen genomförs kommer kursdeltagarna och lärare att tillämpa sina kunskaper och färdigheter genom att agera i olika situationer. Både tekniska och mänskliga IT-resurser har självklart en viktig roll även under kursperioden, för att kunna lagra, bearbeta och presentera information och för att möjliggöra kommunikation mellan de personer som är involverade i kursen. Kursens primära resultat blir de studieprestationer som registreras i Ladok, och till viss del det uppföljningsarbete som pågår under hela studieperioden och som kontinuerligt bör ge kursen feedback så att eventuella brister och problem i informationssäkerheten kan åtgärdas i tid.

Tabell 4.1 Några exempel på områdenas koppling till IT-säkerhetens fyra huvudbegrepp

	Kunskap/ Attityder	Agerande	Teknik	Kontroll/ Uppföljning
Riktighet	Finns tillit till uppgifter och information?	Vilka åtgärder vidtas när felaktig information presenteras?	Hur skyddas materialet mot intrång och förvanskning?	Fungerar källkritiken och kontroll av uppgiftslämnare? Finns antiplagiat verktyg?
Tillgänglighet	Finns erforderlig kunskap att tillgå? Finns hjälpfunktioner och support?	Hur hanteras driftavbrott och störningar?	Vilka minimikrav ställs på datorutrustning och Internet-uppkoppling?	Finns rutiner för säkerhetskopiering och versions-hantering?
Sekretess	Finns det tillräcklig säkerhetsutbildning? Vilken är inställning till säkerhetsfrågor?	Hur skyddas lösenord?	I vilken utsträckning krypteras information?	Hur hanteras personuppgifter?
Spårbarhet	Vilken är inställningen till att publicera material i publika konferenser?	Vilka åtgärder vidtas vid obehörig åtkomst?	Hur garanteras autentiseringen?	Hur hanteras fusk vid examination?

De fyra kategorierna, kunskaper och attityder, agerande, teknik samt kontroll och uppföljning, utgjorde grunden i frågekonstruktionen och även i databearbetning och analys. Enkäterna bestod av bakgrundsfrågor, sakfrågor, attitydfrågor och öppna frågor. Bakgrundsfrågorna i student- resp. kursledarenkäten handlade om kön, ålder, utbildningens ämnesområde och vilken typ av uppkoppling respondenten har mot lärosätet. Sakfrågorna i dessa enkäter handlade om säkerhetskopiering och skydd mot datavirus och obehörigt intrång. I enkäten som besvarades av IT-pedagoger och säkerhetsansvariga var bakgrunden fokuserad på vilken typ av tjänst respondenten har. I attitydfrågor förväntades respondent ta ställning till instämmandegraden i påståenden med hjälp av en femgradig skala. I de öppna frågorna hade respondenterna möjlighet att ge ytterligare synpunkter och kommentarer om IT-säkerheten och distansutbildningen.

4.4 Databearbetning

Bakgrundsfrågorna och frågorna med fasta svarsalternativ bearbetades statistiskt medan de öppna svaren analyserades kvalitativt. Båda svarstyperna redovisas tillsammans, kategoriserade enligt frågekonstruktionen.

Bakgrundsfrågor och sakfrågor
Svaren till bakgrundsfrågor och sakfrågor bearbetades deskriptivt och fördelningen av en variabel redovisas antingen i frekvenstabeller eller i diagram.

Attitydfrågor
I attitydfrågorna som har fem svarsalternativ, har alternativen instämmer inte alls och det efterföljande steget översatts till att respondenten inte instämmer eller i låg grad instämmer i påståendet. Alternativen instämmer i hög grad och skalsteg dessförinnan har översatts som att respondenten instämmer i hög grad eller i någon grad. Det är dessa fyra ytterlägen som redovisas i tabeller medan mittvärdet inte finns med i denna redovisning. Genom att presentera resultatet i procent, i kombination med medelvärdet på frågan, anges riktningen i de svarandes ställningstaganden. I de fall där de interna bortfallet eller alternativet vet ej överstiger 20 procent har detta angetts och kommenterats.

Sambandsmått
Sambandet mellan bakgrundsvariabler och valda attitydfrågor studerades med hjälp av chitvåtest (χ^2). I ett χ^2 -test mäter man avvikelsen mellan de observerade frekvenserna (O_i) och de frekvenser man skulle förvänta sig om det inte fanns något samband mellan variablerna (F_i). Värdet på χ^2 beräknas enligt:

$$\chi^2 = \Sigma (O_i - F_i)^2 / F_i$$

När resultatet visar en signifikant skillnad mellan grupperna syftar detta till ett chitvåtest med signifikansnivån α =5%. Grupperna i dessa test definierades enligt bakgrundsvariablerna kön, ålder och ämnesområde. *Kön* hade grupperna män resp. kvinnor; *ålder* delades i två grupper: *yngre* är åldrarna 20–40 år medan *äldre* är 41-70 år. *Ämnesområde* innefattade tre grupper: Humaniora och samhällsvetenskap, medicin och vård samt naturvetenskap och teknik. I chitvåtest användes alla fem svarsalternativ för attitydfrågorna, genom att delas i två grupper. De tre första svarsalternativen fr.o.m *instämmer inte alls* beräknas som en grupp och de två sista alternativen bildar den andra gruppen. I de flesta fallen har svaren *vet ej* uteslutits, eftersom dessa i regel endast är några få av det totala resultatet. Det finns dock några frågor där ovanligt många respondenter har svarat *vet ej*. I dessa fall kan osäkerheten delvis tolkas som bristande kunskap. Här har alla sex svarsalternativ studerat genom att *vet ej* -svaren bildat en separat tredje grupp.

Det som är mycket viktigt att påpeka är att den statistiska analysen används för att söka eventuella signifikanta samband i det insamlade materialet men endast i syfte att generera hypoteser som sedan kan testas i fortsatta undersökningar. Resultatet kan således inte generaliseras för att allmänt gälla Nätuniversitetets utbildningar. Den huvud-

sakliga orsaken till detta är det relativt stora bortfallet, speciellt när det gäller student-enkäten. Bortfallet kommer att analyseras mer detaljerat i nästa avsnitt.

4.5 Tillförlitlighetsfrågor

Studentenkät
Totalt 896 studenter fick missiv och länk till webbenkäten. Vi fick kännedom om att ett antal studenter, 149 stycken, inte var anträffbara vid den adress som användes. Dels hade förteckningen över e-postadresser en viss övertäckning och innehöll adresser till studenter som inte längre var registrerade på distanskurser, dels gick det inte att nå vissa adresser på grund av tekniska problem. Vi kan dock inte se hur detta bortfall var fördelat över de olika ämnesgrupperna. Troligtvis är antalet studenter som aldrig fick missivet högre än 149, men vi kommer att använda denna siffra i fortsatta beräkningar.

Enkätsystemet mottog totalt 291 svar på studentenkäten. Vi beräknar svars-frekvensen genom att ta hänsyn till de kända fallen där mottagaren inte var anträffbar. På detta sätt kan vi få en bättre uppskattning av hur många studenter som valde att inte delta i undersökningen.

$$\text{Svarsfrekvens (studenter)} = 291 * 100\% / (896 - 149) = 39\ \%$$

Denna frekvens är för låg för att det erhållna resultatet ska kunna användas för att dra generella slutsatser angående studentpopulationen, såsom vi redan har påpekat. En annan faktor som kan påverka resultatet är att kvinnliga studenter är överrepresenterade bland dem som svarade på enkäten. Likaså finns en ojämn fördelning bland de tre ämnesområdena, enligt tabell 4.2. Den huvudsakliga anledningen till denna överrepre-sentation kan vara att ett helt studieprogram fanns med i området Med/Vård, vilket även kan tänkas vara ett område där antalet kvinnliga studenter är högt.

Tabell 4.2. Studenters fördelning inom ämnesområden

Humaniora och samhällsvetenskap	21 %
Medicin och Vård	63 %
Naturvetenskap och teknik	16 %

Det är svårt att bedöma vilka studenter som inte svarat på enkäten och hur detta bortfall kan ha påverkat resultatet. Möjligen är det så att de studenter som är särskilt aktiva i kurserna och som besitter god datorvana är de som har svarat. I en nyligen genomförd undersökning (Söderström, 2004) uppmärksammades skillnader i uppfattningar mellan yngre och äldre studenter samt mellan aktiva och mindre aktiva studenter. Äldre studenterna med större studievana visade sig vara mer positiva till distansutbildning. Om så är fallet finns anledning att tro att utfallet hade blivit mer negativt om bortfallet minskat.

Kursledarenkät
Totalt 140 kursansvariga lärare fick missiv och länk till webbenkäten. Vi fick kännedom om 34 lärare som inte arbetade med distansutbildning eller som var oanträffbara på grund av tekniska problem. Enkätsystemet mottog totalt 68 svar på kursledarenkäten. Vi uppskattar den totala svarsfrekvensen på samma sätt som vi gjorde för studentenkäten.

Svarsfrekvens (kursledare) = 68 * 100% / (140 – 34) = 64 %

Denna frekvens var högre än i studentenkäten vilket visas i tabell 4.3 och fördelningen mellan könen och ämnesområdena var mera jämn. Vi har dock valt att även i detta fall inte använda resultatet för att dra generella slutsatser angående populationen, såsom vi redan har påpekat.

Tabell 4.3. Kursledare, frekvensfördelning inom ämnesområden

Humaniora och samhällsvetenskap	36 %
Medicin och Vård	21 %
Naturvetenskap och teknik	43 %

Då enkäten i första hand vände sig till kursansvariga lärare är det sannolikt att svaren är positivare än även om de distanslärare som enbart undervisar i kursen skulle ha ingått. Bakgrunden till denna uppfattning är att det i en aktuell undersökning visat sig att kursansvariga anser att andra lärare som medverkar i kurserna har sämre IT-kunskaper (Westerberg & Mårald, 2004).

Enkät till IT-pedagoger och säkerhetsansvariga
När det gäller enkäten vet man inte hur många missiv som slutligen kom fram till den avsedda målgruppen IT-pedagoger/säkerhetsansvariga. Således är det inte möjligt att uppskatta svarsfrekvensen på samma sätt som gjordes i de två tidigare fallen, och resultatet kommer inte heller användas för att dra generella slutsatser. Enkätsystemet mottog totalt 27 svar på enkäten.

5 RESULTAT

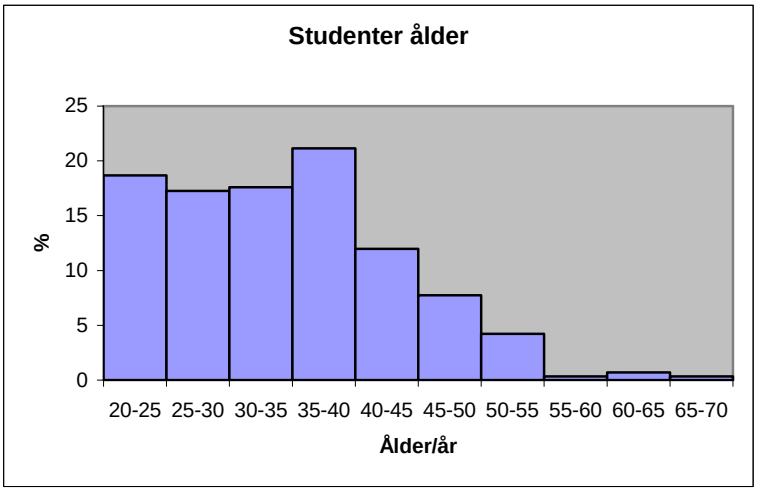
I resultatredovisningens inledning presenteras de bakgrundsvariabler som angetts för studenter, lärare, IT-pedagoger och säkerhetsansvariga. Därefter redovisas svaren i de kategorier som bildat utgångspunkt för frågekonstruktionen nämligen **kunskaper och attityder** (avsnitt 5.4), **agerande** (avsnitt 5.5), **teknik** (avsnitt 5.6) och **kontroll och uppföljning** (avsnitt 5.7). Svaren från öppna frågor och övriga kommentarer, som ställdes i slutet av enkäten, har ordnats och redovisas under de avsnitt som har tydligaste kopplingen till uttalandet.

Efter varje kategori presenteras en sammanfattning och analys. I analysen görs kopplingar mot tidigare forskning

5.1 Enkätundersökningen

Nätuniversitetsstudenterna

Huvuddelen av dem som svarat på enkäten är kvinnor (86 %). Medianåldern för studenterna är 34 år och 50% av dem ligger inom intervallet 26–40 år, dvs. kvartilavståndet (IQR) är 14 år. Åldersfördelningen visas i histogram, se Figur 5.1.



Figur 5.1. Åldersfördelning bland studenter

Hemmet är den i särklass frekventaste stället där datorn används för studierna (84 %) och det är få (10 %) som huvudsakligen använder datorn på universitet/högskola/ lärcentra eller på arbetet och annan plats (7 %). Det kan vara intressant att notera att i det insamlade materialet finns en signifikant skillnad genom att flera kvinnor använder datorn hemma medan männen använder datorn på arbetet. Några alternerar mellan hem och arbete vilket följande citat belyser:

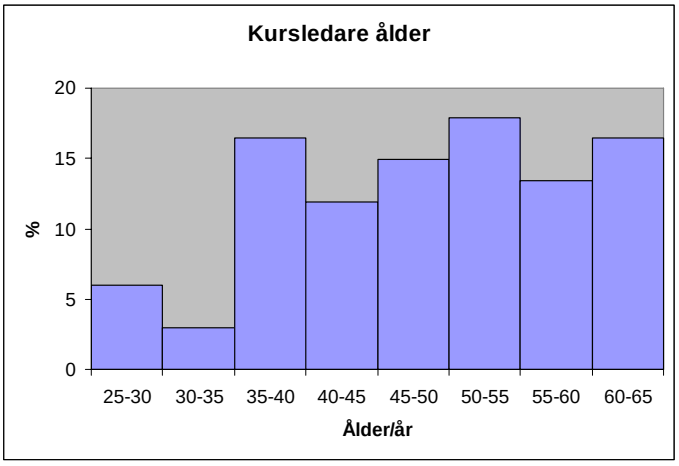
> Jag har modemuppkoppling hemma och bredband på jobbet, så jag stannar ofta kvar på jobbet för att göra sådant som kräver uppkoppling. Jag brukar, av samma anledning, ladda hem pdf-versioner av studiematerialet för att använda dem istället för att vara uppkopplad.

De flesta som svarat på enkäten går programutbildning (68 %) och övriga (32 %) följer fristående kurser.

De studenter som svarat på enkäten förefaller var väl medvetna om vilken typ av Internetuppkoppling de använder. En hög andel av respondenterna (76 %) har bredband i hemmet medan än en femtedel (20 %) använder vanligt telefonmodem.

Distanslärarna

Fördelningen mellan kvinnor (48 %) och män (52 %) är jämn i lärarenkäten. Medianåldern för lärarna är 48 år och 50% av åldrarna ligger inom intervallet 39–56 år, dvs. kvartilavståndet (IQR) är 17 år. Åldersfördelningen visas i histogram, se Figur 5.2.



Figur 5.2. Åldersfördelning bland kursledare

Arbetet som distanslärare sker huvudsakligen på arbetsplatsen (91 %) och endast några få lärare (9 %) arbetar hemifrån.

De flesta som svarat på enkäten (80 %) undervisar på fristående kurser och ungefär hälften på program (40 %). Några (20 %) undervisar således både i fristående kurser och program.

Alla har uppgett vilken typ av Internetuppkoppling de har hemma. I jämförelse med studenterna är det något färre lärare (68 %) som anger att de har bredband hemma. Nästan en tredjedel (30 %) har vanligt telefonmodem i hemmet.

De IT-ansvariga och IT-pedagoger

I den enkät som vände sig till IT-pedagoger och säkerhetsansvariga vid samtliga av Nätuniversitets högskolor och universitet svarade 27 personer. Då enkäten förmedlades genom registratorn vid varje lärosäte kunde tyvärr inga påminnelser skickas ut. Av dem som svarat uppgav 11 att de tjänstgjorde som IT-pedagog eller hade liknande funktion och 21 hade uppgifter som säkerhetsansvarig för IT-säkerheten i distansutbildningen. I

enkätsvaren framkom att 12 tjänstgjorde på central nivå och 12 på avdelningsnivå. Tre respondenter tjänstgjorde på båda nivåerna. I enkätsvaren kunde man utläsa att 18 uppgav att de ansvarade för studenternas utbildning kring IT-relaterade frågor och användning av distansverktyg.

5.2 Kunskaper och attityder

Datorvana och datorkunskap

I en av enkätfrågorna fick respondenterna skatta sin datorvana. Nästan två tredjedelar av distansstudenterna bedömer att den är god. Något mer än en tiondel av studenterna menar att datorvanan inte är tillräcklig (tabell 5.1 Bilaga 1). Bland studenterna finns det en signifikant skillnad mellan kvinnor och män, genom att kvinnor anger sig att ha något mindre datorvana än män. Likaså har studenterna i ämnesgruppen Medicin/Vård något mindre datorvana än de övriga grupperna. Däremot finns det ingen signifikant skillnad i datorvana när det gäller olika ålderskategorier, vilket kan vara ett intressant faktum. I citatet nedan utrycker en student sin osäkerhet inför datorhanteringen.

> Det är min första termin och jag är väl inte helt insatt i detta ännu. Min datavana är inte så god, så det har varit ganska mycket att lära sig, men det börjar klarna nu.

Det är en större andel av lärarna som bedömer sin datorvana som god. Bland lärarna går det inte att se någon signifikant skillnad mellan könen eller mellan olika åldrar. Däremot visar det sig även här att de lärare som tillhör ämnesgruppen Medicin/Vård anser sig ha något lägre datorvana än de övriga grupperna. Endast en lärare har bedömt sin datorvana som mindre god (tabell 5.1 Bil.1).

Nästan hälften av de studenter som deltagit i enkätundersökningen uppger att de tagit del av universitetets/högskolans regler och policy för användning av datorer, distansverktyg och Internet. Nära en fjärdedel markerar att de inte gjort detta (tabell 5.2 Bil.1). Det är fler lärare än studenter som menar att de tagit del av informationen om regler och policy, men nära nog en femtedel av lärarna uppger att de saknat informationen (tabell 5.2 Bil.1).

I den enkät som vände sig till IT-ansvariga menar många att studenterna har fått information om regler och policy (tabell 5.3 Bil.1) men många har inte alltid tagit till sig innebörden i förbindelsen vilket följande citat belyser.

> På vår högskola får alla information om vilka regler som gäller samtidigt som de skriver på en ansvarsförbindelse. Tyvärr är det inte alltid så att studenten läser det som står i avtalet.

När det gäller kunskaper om de regler som gäller för publicering påpekar många studenter och lärare att de är otillräckliga. Mer än en tredjedel av studenterna och en fjärdedel av lärarna uttrycker osäkerhet inom området (tabell 5.4 Bil.1). IT-ansvariga/pedagog bedömer att studenter och lärares kunskaper inte är tillräckliga men anser att lärarna har högre kompetens inom området (tabell 5.5 Bil.1).

Mer än hälften av studenterna och lärarna är relativt säkra på vilka åtgärder de ska vidta om de misstänker att deras dator blivit smittad av ett datorvirus. Här finns en

signifikant skillnad i studentgruppen mellan könen, kvinnorna är mera osäkra när det gäller vilka åtgärder som måste vidtas. Lärarna uttrycker en större säkerhet än studenterna i sina svar (tabell 5.6 Bil.1).

Mer än var fjärde student har inte riktigt klart för sig vart han/hon ska vända sig när tekniska problem inträffar. Lärarna har i en jämförelse med studenterna en klarare bild av var hjälp står att finna (tabell 5.7 Bil.1). IT-ansvariga/pedagoger gör bedömningen att fler av lärarna vet vart man ska söka hjälp när tekniska problem uppkommer (tabell 5.8 Bil.1).

Säkerhetsmedvetande och tillit

Något fler än hälften av studenterna instämmer i att de är medvetna om de säkerhetsrisker som finns förknippade med användningen av datorkommunikation. Ett flertal säger sig inte vara lika medvetna (tabell 5.9 Bil.1). Några studenter ger uttryck för att man inte upplever det som någon problematik vilket följande citat är exempel på.

> Jag upplever det inte som om något vi håller på med är särskilt viktigt, att det är hemligt. Därför bekymrar den delen av säkerhetsproblematiken inte mig.

Lärarna bedömer sitt säkerhetsmedvetande som högre än studenterna och skattar studenternas säkerhetsmedvetande lägre än vad studenterna skattar lärarnas (tabell 5.10 Bil.1). IT-ansvarig/pedagog bedömer studenters och lärares säkerhetsmedvetande likvärdigt men betydligt lägre än studenternas och lärarnas egna skattningar (tabell 5.11 Bil.1). Mer än hälften av studenterna och lärarna känner aldrig oro för att material ska läsas av obehöriga. Det är ett antal, både studenter och lärare som markerar sitt tvivel (tabell 5.12 Bil.1). I citat nedan ger en student uttryck för sin oro.

> Jag undrar hur vi elever kan vara säkra på att inte lärare har ”hemliga rättigheter” att läsa mail som vi skickar mellan våra privata mailboxar i t.ex., First Class? Detta med tanke på att vissa inlämningskonferenser är öppnade speciellt bara för lärare. Alltså…..informationen om lärarnas speciella möjligheter i t.ex.. FC har inte varit tillräcklig tycker jag.

När det gäller oro för att material som skickas med distansverktyg ska försvinna har studenter och lärare en likartad bedömning (tabell 5.13 Bil.1). Studenterna känner dock mer oro då mer än en fjärdedel uttrycker en farhåga för att material som skickas inte når fram på ett korrekt sätt. I citatet nedan ger en student förslag på åtgärder för att minska osäkerheten.

> Det vore också bra om man fick veta om ens e-brev kommit fram direkt med en slags bekräftelse (automatiskt). å behöver man inte oroa sig för datorstrul då man skickar svar på duggor och tentor till lärarna.

Huvuddelen av studenter, lärare och IT-ansvariga/pedagoger instämmer i påståendet att IT-säkerheten som helhet är god i distansutbildning. Här är samstämmigheten i svaren hög (tabell 5.14 Bil.1). Samtidigt är det mer än var femte student och lärare som inte klart ge uttryck för att de uppfattar IT-säkerheten som god.

5.3 Sammanfattning och analys:

Det är en övervägande del kvinnor som svarat på studentenkäten, vilket först och främst beror på att de kvinnodominerade utbildningarna inom medicin- och vård har en stark representation i materialet. Ytterligare en orsak till denna höga andel kan vara att de kvinnliga studenterna är mer välvilliga till att delta i undersökningen.

Studentens frihet i tid och rum ger inte några direkta avtryck när det gäller lärarnas flexibilitet. Mycket få lärare arbetar från hemmet eller någon annan plats. Att lärare inom distansutbildningar skulle arbeta från mer eller mindre spektakulära platser är troligen mer ”önskan” och myt än realitet. Troliga orsaker till att lärarna fysiskt är bundna till sitt lärosäte kan vara att lärare på distanskurser parallellt arbetar med campuskurser. En annan orsak kan vara att många saknar bredband i hemmet.

Med utgångspunkt i studenternas och lärares skattningar kan vi anta att distanslärare och studenter besitter en relativt bra grundkompetens när det gäller datoranvändning. Mindre datorvana är studenter inom medicin och vård. Att ge detta utbildningsområde riktade utbildningsinsatser inom området kunde vara en lämplig åtgärd. Enligt enkäterna har lärarna en något större datorkunskap och datavana än studenterna, vilket bekräftas i någon grad genom IT-ansvariga/pedagogers enkäter. Denna iakttagelse har gjorts i en tidigare rapport om studenternas uppfattning om dator-kommunikation (Söderström, 2004). I Söderströms undersökning indikerar enkätsvaren att tekniken inte i någon större utsträckning utgjort något hinder eller försvårat för studenter. Detta gäller studenter både med och utan förkunskaper. Ingen verkar avbryta studierna pga. av svårigheter med tekniken (a.a.). I ytterligare en rapport (Westerberg & Mårald, 2004) noteras att IT-kompetensen bland studenter på IT-stödda distanskurser är god. Detta förhållande till trots, är det ett betydande antal studenter och lärare som önskar sig mer kompetens inom området. Önskemål från lärare och studenter har uttryckts i en aktuell undersökning om nätburen examination (Österholm, 2005) där det konstateras att det finns ett uttalat behov av kompetensutveckling inom området.

Vad gäller information och kunskap om regler och policy finns det behov av mer information till både lärare och studenter. Här saknas rutiner som kontrollerar om användarna tagit till sig informationen på ett tillfredsställande sätt. Det finns även ett stort behov av undervisning om de regler och lagar som gäller för publicering på nätet. Här är det drygt en tredjedel av studenterna och en fjärdedel av lärarna som menar att de saknar tillräckliga kunskaper inom området. Liknande bedömning gör IT-ansvariga/pedagoger av studenters och lärares kunskaper inom området. På den här specifika frågan är bortfallet hos IT-ansvariga/pedagoger betydande vilket sannolikt beror på att respondenterna saknar information om lärarnas och deltagarnas kunskaper inom området. Om fel begås kring publicering är det inte alltid det görs synligt för IT-ansvariga/pedagoger.

Betryggande kunskaper om och hur man ska agera när datorn blivit smittat av datorvirus saknas också hos studenter och lärare. Åtgärder som tydliggör hur man ska agera och vem man ska kontakta när tekniska problem inträffar efterfrågas från båda grupperna. Det är få studenter som använder datorer på högskola, lärcenter eller annan plats. Detta gör att studenternas datorer inte kan uppdateras och kontrolleras genom lärosätenas försorg. När det gäller lärarna har de lättare att nå och få datorsupport då de oftast arbetar vid lärosätets datorer och har speciella avtal för support.

Många är medvetna om de risker som finns med datoranvändning och datorkommunikation men de finns också dem som är osäkra. Var femte student säger sig inte vara medvetna om riskerna. Det är en betydande del av studenterna som känner oro för att material som skickas ska komma fel, försvinna, eller läsas av obehöriga. Sammanfattningsvis anser huvuddelen av de tillfrågade att IT-säkerheten som helhet är god i distansutbildning. Detta kan upplevas som motsägelsefullt, då många utryckt brister inom området tex. när det gäller regler för publicering på nätet. En orsak till detta kan vara att respondenterna inte koppla denna och andra frågor till IT-säkerhet. Troligen har man en snävare syn på begreppet IT-säkerhet än den som formulerats i undersökningen, det är relativt vanligt att IT-säkerhet uppfattas som ett synonym till datorsäkerhet.

5.4 Agerande

Handhavande av distansverktyg, personuppgifter och lösenord

Mer än tre fjärdedelar av studenter anser att de, utan några större problem, kan handskas med de distansverktyg som utnyttjas i kursen. Dock finns en signifikant skillnad mellan könen, kvinnor anser sig ha något svårare att hantera dessa verktyg. På samma fråga har lärarna något lägre instämmande grad (tabell 5.15 Bil.1). IT-ansvariga/pedagoger gör en lägre bedömning av studenternas förmåga att hantera distansverktygen (tabell 5.16 Bil.1).

När det gäller hanterandet av personuppgifter i kurser menar huvuddelen av lärarna att man gör detta på ett korrekt sätt. Många av de studenter som svarat gör tillsammans med IT-ansvariga/pedagoger en något negativare bedömning (tabell 5.17 Bil.1). Ett flertal studenter avstår från att svara på denna fråga då de troligen anser att de inte har tillräcklig information för att besvara frågan. Några studenter har avvikande åsikter vilket följande citat kan illustrera.

> Jag är inte helt förtjust i att ha mina betyg utlagda på Internet. Det är alltför ofta önskvärt enligt lärarna att man har med sin e-postadress utlagd på sidorna för att andra elever ska kunna skriva till en. Det vore bättre om man fick byta e-postadress med varann via något annat forum, en slags inläggsbox eller nåt. Om man nu vill det.

Huvuddelen av studenterna har aldrig känt sig hotade eller attackerade i en distanskurs (tabell 15.18 Bil.1). Lärarna har i denna jämförelse en liknande bedömning. IT-ansvariga/pedagoger bedömning inom samma område ligger nära den lärarna utfört (tabell 5.19 Bil.1).

Huvuddelen av studenter och lärare anser att de konstruerar sitt lösenord efter det regler som rekommenderas (tabell 5.20 Bil.1). Det är inte många av studenter och lärare som byter ut lösenordet minst en gång per termin. Ungefär två tredjedelar av studenterna och lärarna byter inte lösenord varje termin (tabell 5.21 Bil.1). När det gäller att skydda lösenordet är det mer än hälften som menar att man gör detta på ett betryggande sätt (tabell 5.22 Bil.1). IT-ansvariga/pedagoger syn på studenter och lärares agerande i denna fråga ligger nära den som studenter och lärare själva gjort (tabell 5.23 Bil.1).

Versionshantering och säkerhetskopiering

Det är mer än hälften av studenter och lärare som uttrycker att de sällan har problem med versionshantering (tabell 5.24 Bil.1). IT-ansvariga/pedagoger bedömer att studenter och lärare oftare har problem kring versionshanteringen än vad studenter och lärares egen skattning ger vid handen (tabell 5.25 Bil.1).

Många studenter och lärare säkerhetskopierar i stor utsträckning sina dokument. Nära nog alla studenter och lärare gör någon typ av kopia. På påståendet ”jag gör ofta en säkerhetskopia på mitt arbete” är det en fjärdedel av studenterna och nära nog en femtedel av lärarna som bedömer att de mindre frekvent utför säkerhetskopiering på sina arbeten (tabell 5.26 Bil.1). IT-ansvariga/pedagogers bedömning bekräftar studenter och lärares agerande kring säkerhetskopiering (tabell 5.27 Bil.1).

Virushantering

Två tredjedelar av studenterna uppger att det uppdaterar sina antivirusprogram regelbundet. Av lärarna är det något fler (tabell 5.28 Bil.1). En hel del studenteter markerar att det inte vet om de har antivirusprogram eller om dessa uppdateras, vilket följande studentkommentar är ett exempel på.

> Ingen aning. Jag har antivirusprogram och anser mig inte ha tid att fundera kring detta. Det är en viktig fråga men som sagt jag har inte den tiden att lägga ner på dessa frågor. Familj och hus samt studier på heltid, då vill man att det skall fungera.

IT-ansvariga/pedagoger bedömer att lärarna har ett betydligt aktuellare virusskydd än studenterna (tabell 5.29 Bil.1).

Hanterandet av program och dokument som hämtats från osäkra miljöer förekommer relativt ofta enligt enkätsvaren, men hälften av studenterna och mer än hälften av lärarna uppger att de inte hämtar program från osäkra miljöer (tabell 5.30 Bil.1). I en av studenternas kommentarer spekuleras i troliga orsaker till att man använder program från osäkra/okända miljöer.

> Har en liten utbildning i datasäkerhet. Gäller speciellt dem som inte läser något inom IT och därför inte är vana datoranvändare. Alltför många tror att det inte drabbar dem och antingen uppdaterar de inte mjukvarorna tillräckligt ofta, eller så kollar de inte nerladdade filer alls innan de öppnar dem.

Runt var tredje student och lärare instämmer i påståendet att man inte öppnar eller utnyttjar program som hämtas från okända miljöer (tabell 5.31 Bil.1). Här finns en signifikant skillnad i studentgruppen, männen instämmer i påståendet i högre grad än kvinnorna. I citatet nedan ges ett exempel på hur en student undviker risken att få virus i datorn.

> Jag ”missbrukar” jobbets dataavdelning och företagets oro för virus odyl, så är jag tveksam öppnar jag filerna via jobbdatorn. Upplever inte att utbildningsIT är farofylld jämfört med andra internetuppkopplingar. Snarare förvånansvärt förskonad från t ex spam. Provar ibland att maila till min jobbmail för att se om det blir något viruslarm.

Den bedömning IT-ansvariga/pedagoger gör i denna fråga är att studenterna i högre grad än lärarna öppnar filer som inte är viruskontrollerade (tabell 5.32 Bil.1).

Hälften av studenterna menar att de till avsändaren regelmässigt skulle anmäla om det fått ett datavirus (tabell 5.33 Bil.1). Färre är de studenter som systematiskt anmäler tekniska fel till IT-ansvarig eller kursledare (tabell 5.34 Bil.1). När det gäller lärarna anmäler det tekniska fel mer frekvent. Många studenter anger varför man avstår från anmälan vilket framkommer av nedanstående citat.

> Ang. att hämta saker från osäkra miljöer: skulle jag låta bli det varje gång jag fick en varning skulle jag inte kunna ta del av mycket av kursinnehållet. Min dator godkänner t.ex. inte högskolans bibliotek.

> Jag har tröttnat på att meddela avsändaren om ett virus, för ofta är avsändaren okänd för mig, och troligen är det ett virus som bara tagit ett namn i någons adressbok och därför är det inte den riktige avsändaren av viruset.

IT-ansvariga/pedagogers syn på studenter och lärares agerande vad gäller anmälningar ligger nära den som studenter och lärare själva gjort (tabell 5.35 Bil.1).

5.4.1 Sammanfattning och analys

Studenter och lärare är i hög grad nöjda med de distansverktyg som används. Endast ett fåtal studenter och lärare har problem att hantera de distansverktyg som används vid de olika distansutbildningarna. Av kommentarerna att döma är det mest asynkron kommunikation i textbaserade forum.

Studenterna utgår från att lärarna handskas med personuppgifter på ett korrekt sätt. Endast ett fåtal markerar att man misstror lärarna i denna uppgift (många har avstått från att svara). Lärarna själva anger att de följer de regler som gäller. En undersökning utförd av Westerberg och Mårald (2004) ger en annan bild då det noteras att kunskaper kring lagstiftningen är bristfälliga. Denna uppfattning, att reglerna inte följs, delas i denna undersökning av några IT-ansvariga/pedagoger. Det är inte omöjligt att den bedömning som lärarna gör i denna fråga baseras på felaktiga kunskaper om hur personuppgifter ska hanteras.

Det finns ett antal studenter och lärare som känt sig hotade eller personligt attackerade i distanskurser. De är inte många, men bara det faktum att det förekommer är allvarligt nog. Huvuddelen av studenterna och lärarna konstruerar lösenord enligt de rekommendationer som ges. Det är emellertid få som byter ut lösenordet varje termin. Detta är ett faktum som många IT-ansvariga/pedagoger accepterar, eftersom de anser att alternativet då användare skriver minneslappar skulle innebära ett större problem för säkerhet och support.

Det är många studenter och lärare som menar att de inte har några problem med versionshantering men det är trots allt ett flertal som anger att de har problem att hålla ordning på de olika dokumentversionerna. När det gäller säkerhetskopiering är det förhållandevis många, både lärare och studenter, som anger att de sällan gör någon säkerhetskopiering. En trolig anledning till detta är att användarna sparar sina dokument på skolans server och de är medvetna om att de finns en stabil och kontinuerlig backup

på det som lagras där. Det kan också vara så att det faktiskt inte finns någon aktuell säkerhetskopia. Att studenter och lärare har enkla och bra rutiner för säkerhetskopiering och versionshantering är essentiellt för att trygga undervisning och studier. Särskilt viktigt är detta i uppsatsskrivande och dokumentation av studenternas prestationer.

När det gäller virushantering finns det relativt många studenter som inte uppdaterar sitt virusskydd. Många av studenterna önskar ett ökat stöd inom detta område. Lärarna har oftast ett bra virusskydd som uppdateras med automatik från IT-avdelningarna, vilket IT-ansvarigas/pedagogers svar ger vid handen. Det är däremot inte alltid som lärarna själva vet att deras virusskydd uppdaterats kontinuerlig genom IT-avdelningens försorg.

Att program och dokument från osäkra miljöer hämtas hem och öppnas förekommer både bland studenter och lärare. Enligt IT-ansvariga/pedagoger är detta förhållningssätt vanligare bland studenter. Möjligen är tillförlitligheten i denna fråga något lägre än i andra frågor då viss nedladdning av t.ex. musik och film är populärt men olagligt.

Ett flertal studenter rapporterar inte tekniska fel till kursansvarig eller IT-ansvarig/pedagog. Möjliga förklaringar till detta kan vara att studenter många gånger inte vet vem de ska vända sig till, att problemet är övergående eller att studenter får hjälp att lösa problemet av någon i vänkretsen. När det gäller rapporteringen från lärarna är den betydligt mer frekvent. En orsak till detta är säkert att tillgången till IT-support är bättre och att läraren har ett särskilt ansvar för att reducera olika typer av avbrott och störningar i kursen.

5.5 Teknik

Teknisk prestanda och datalagring

När det gäller skattningen av den tekniska prestandan på de datorer som används i distansstudierna anger näst intill nio av tio studenter att man har tillräckligt bra datorutrustning (tabell 5.36 Bil.1). Motsvarande skattning för lärarna är något lägre. Några studenter markerar att deras utrustning inte riktigt räcker till för alla moment.

> Det har fungerat bättre än jag trodde. Att se filmer och föreläsningar över nätet är svårt via modem.(jag bor i ett område utan möjlighet till bredband). Jag har löst det genom att låna dator hos bekanta vid dessa tillfällen.

Majoriteten av de IT-ansvariga bedömer att distansstudenterna har en god teknisk prestanda på sina datorer och tillräckligt snabb Internetuppkoppling (tabell 5.37 Bil.1). Värt att notera är att var femte student uppger att de faktiskt använder vanligt telefonmodem.

Vanligast bland studenterna är att man lagrar arbetet på hårddisk eller diskett. När det gäller lärarna är det vanligaste sättet att lagrar en säkerhetskopia på lärosätets server och hårddisk (tabell 5.38 Bil.1) Lärarna lagrar sällan arbetet på diskett.

Antivirusprogram och brandvägg

Nästan nio av tio studenter anger att de har antivirusprogram installerat i sina datorer och något färre har brandvägg installerad. När det gäller frågan om hemdatorn har

brandvägg installerad är andelen kvinnor som svarar *vet ej* anmärkningsvärt hög, och just i denna fråga ger således chitvåtest med tre separata kategorier (se avsnitt 4.4) en signifikant skillnad mellan könen. I lärarenkäten är de fler som anger att det har antivirusprogram installerat på dator hemma medan det är färre som har brandvägg installerat i hemdatorn (tabell 5.39, 5.40 Bil.1). Några studenter tar upp problemet att en god datorsäkerhet kan vara förenlig med kännbara utgifter vilket följande citat är exempel på.

> Virusskydd är dyra. Distansstudenter skulle få det gratis eller med ordentligt rabatt. Bättre virusskydd på skolor och studiecenter. Det är för få på skolor/studiecenter som hjälper elever som får problem med datorn/program.

Runt frågor kring virusskydd och brandvägg lämnades många kommentarer från studenterna. I citaten nedan presenteras några.

> Förse alla studenter med antivirusprogram

> Jag har inte Internet på min dator hemma, därav varken brandvägg eller virusskydd

> Min (bristande) datasäkerhet hemma bygger på det faktum att jag är Mac-användare och därför inte drabbas på samma sätt av virus.

Mer än hälften av studenterna instämmer i påståendet att de sällan får oönskade e-meddelande som stör studierna. Av lärarnas skattning kan man utläsa att de besväras mer av skräppost än studenterna (tabell 5.41 Bil.1) Studentkommentaren nedan utgör exempel på att oönskade e-meddelande stör studierna.

> Att ingen kan lämna ut ens e-adress, utan ens kännedom. Här tänker jag på bla. studentkåren. Jag vet inte hur dom gör, men jag blir nerlusad av spam, både från England-Brasilien, sedan jag började studera.

IT-ansvariga/pedagoger menar i större utsträckning att oönskade e-meddelande stör lärare och studenter i distansutbildningar (tabell 5.42 Bil.1)

Hälften av studenterna instämmer i påståendet att det sällan förekommer tekniska driftstörningar i de distansverktyg som används (tabell 5.43 Bil.1). På påståendet att tekniska problem inte stör distansstudierna är det något större andel som instämmer (tabell 5.44). Här finns en signifikant skillnad som är viktig att notera, genom att kvinnorna upplever att tekniska problem kan störa deras studier i högre grad än männen gör. Bedömningen som görs av lärarna på samma fråga och skalsteg är mycket lika. IT-ansvarig/pedagog bedömer driftsäkerheten högre än studenter och lärare (tabell 5.45 Bil.1).

Mer än två tredjedelar av studenterna visar att de är relativt nöjda med distansverktygen som används i utbildningen. Något lägre bedömning gör lärarna i sin enkät där dubbelt så många, i jämförelse med studenterna, uttrycker sitt missnöje (tabell 5.46 Bil.1). Nöjdas är IT-ansvariga/pedagoger (5.47 Bil.1). Några lärare önskar mer information om vilka digitala resurser som finns att tillgå, vilket nedanstående citat är uttryck för.

> Det behövs mera jämförande information om olika distansverktyg.

En hel del studenter har påpekat brister i de verktyg som används i kurserna.

> På 3 olika distanskurser på GU har jag mött 3 olika, samtliga dåliga gränssnitt. Layouten är undermålig och bitvis även funktionaliteten, men man kan fortfarande lära sig mycket och examination etc. funkar bra.

5.5.1 Sammanfattning och analys

Studenter och lärare anser sig ha god teknisk prestanda på de datorer som används vid distansstudier och distansundervisning. Något fler lärare önskar bättre datorer vilket kan bero på att ansvar och administration av kurser kräver mer av utrustning och användare. Det är alltjämt många studenter som använder diskett som lagringsmedia. Detta är inte tillfredsställande då det inte är särskilt tillförlitligt och studenterna riskerar att förlora sina dokument. Få studenter utnyttjar lärosätenas servrar med den kontinuerliga backup som utförs. Lärarna utnyttjar i hög grad denna möjlighet.

Huvuddelen av studenter och lärare har antivirusprogram installerade i datorerna medan flera saknar brandvägg. Många studenter menar att detta är en fråga om kunskap och kostnad och efterfrågar därför hjälp från lärosätet. Många lärare saknar brandvägg hemma men då det är få lärare som använder sin hemdator för distansundervisning utgör detta inget större hot mot säkerheten i distanskurserna.

Oönskade e-meddelande är ett problem för många användare vilket också IT-ansvariga/pedagoger bekräftar. Tekniska problem påverkar nära nog var tionde student. Här förekommer problem som aldrig kommer de IT-ansvariga till kännedom. Studenterna i enkätundersökningen är i hög grad nöjda med de distansverktyg som används. Lärarna har mer att önska vilket säkert förklaras av att det krävs mer av funktionalitet och kapacitet när hela kurser ska administreras och utvärderas.

5.6 Kontroll och uppföljning

När det gäller informationen runt distansverktygen är det knappt hälften som instämmer i påståendet att denna är tillräcklig. I denna fråga är studenter, lärare och IT-ansvariga/pedagoger mycket samstämmiga (tabell 5.48 Bil.1).

I stort sett samma gäller studenternas och lärarnas inställning i frågan om undervisning kring användandet (tabell 5.49 Bil.1). Nästan var fjärde student instämmer inte i påståendet att utbildningen är tillräcklig. Här finns en signifikant skillnad mellan könen, kvinnorna upplever större brister i utbildning än männen gör. Många studenter har utryckt en önskan om mer undervisning i användandet av distansverktyg vilket nedanstående kommentarer illustrerar.

> Kurser för alla distansare kring just IT-säkerhet. Praktiska, handfasta råd och tips. Kanske en hel ”plan” för hur man bör gå tillväga i olika situationer för att vara så säker som möjligt.

> Vi fick aldrig någon riktig genomgång på hur (namn på LMS) fungerar och en del kursansvariga kan inte alls hantera den. Så ibland får vi studiehandling m.m alldeles för sent, alltså efter kursstart.

> Undermåliga förklaringar hur man kommer med i ett webbseminarium. Ett webbseminarium kallas chatt, modemkontakt mm. Adekvata ord måste användas för nybörjare. Information om Marratech borde finnas på svenska.

En lärare önskar en mer kontinuerlig utbildning.

> Kontinuerlig data- och säkerhetsutbildning på universitet och högskolor, varje år. Nu finns inga alls eller enstaka på enskilda individers initiativ.

Den datorsupport som ges till studenterna bedöms högre av lärarna i jämförelse med studenterna (tabell 5.50 Bil.1). Nästan en femtedel av studenterna anses inte ha fått tillräcklig hjälp. Även i detta fall finns det en skillnad mellan könen, kvinnorna anser att datorsupporten inte är tillräcklig i högre grad än männen gör. Flera studenter har synpunkter på datorsupportens kvalitet och omfattning vilket nedanstående exempel visar.

> Har själv fått hjälpt ett antal kurskamrater med teknisk support. Kanske borde kraven vara högre för anmälan alt. tydligare introduktionsmanualer. Vilka program behövs? Hur installerar jag dem? Och då menar jag en manual som verkligen är steg för steg och inte förutsätter några förkunskaper alls. Jag har stött på frågan: -Word säger du. Vad menar du då? Då är det inte lätt att vara student på nätet!

IT-ansvarigas/pedagogers bedömning av datorsupportens omfattning stämmer väl överens med studenternas och lärarnas skattning (tabell 5.51, Bil.1).

Autentiseringen

När det gäller att identifiera avsändaren är det många som instämmer i att man alltid kan se vem som skickar ett inlägg eller lämnar ett inlägg i webbkonferensen (tabell 5.52 Bil.1).

Fusk

Klart mer än hälften av studenterna anser inte att risken för fusk är större vid distansstudier jämfört med traditionell campusutbildning. En mindre andel har markerat instämmer inte. På denna fråga är bortfallet på studentenkäten högre än på övriga frågor (14 %). På frågan skiljer sig lärarnas uppfattning från studenternas då de har klart lägre grad av instämmelse (tabell 5.53 Bil.1)

Hälften av lärarna instämde i lärarenkätens påstående *”jag ägnar inte mer tid åt att förebygga fusk i distansutbildningen i jämförelse med campusutbildning*” (tabell 5.54 Bil.1). Nästa lika många instämmer inte i påståendet att *”vid distansutbildning vidtar jag inga speciella åtgärder för att förhindra fusk”* (tabell 5.55 Bil.1).

Ungefär en fjärdedel av lärarna menar att det kan vara vanskligare att upptäcka fusk vid distansundervisning (tabell 5.56 Bil.1). För att undvika fusk menar några lärare att man

ska kombinera fysiska träffar och låta studenterna lämna in sina arbeten för kontinuerlig bedömning. Användandet av webbkamera är ett annat förslag som nämns.

> Kombination av fysiska träffar. Kontinuerlig inlämning av arbeten för bedömning.
>
> Jobba mera med webbkameror och personlig kontakt via internet.
>
> Man skulle ha möjligheten som lärare att använda olika slags ”prov” om det är osäkert om en student har gjort alla uppgifter själv. 2:a förslag: online-tenta hemma med webkamera och mikrofonen på minskar fuskmöjligheter med en modersmål-talande i närheten.

Utveckling av IT-säkerheten

Av studenterna är det mer än en tredjedel som instämmer i påståendet att de kan bidra till ökad IT-säkerhet i distansutbildningen. En högre andel av lärare instämmer i samma påstående (tabell 5.57 Bil.1). De IT-ansvariga/pedagogerna menar i högre grad att studenter och lärare kan bidra till datorsäkerheten (tabell 5.58 Bil.1).

Att IT-säkerheten kommer att öka i framtiden tror en stor andel av studenterna, lärarna och de IT-ansvariga/pedagogerna (tabell5.59 Bil.1). Få är de studenter och lärare som inte instämmer i påståendet.

5.6.1 Sammanfattning och analys

Många studenter och lärare efterlyser mer information och undervisning kring användandet av distansverktygen. Samma behov finns kring support och stöd. Här har lärarna lättare att få stöd, vilket troligen beror på bättre kontakt och närheten till de IT-ansvariga. Brist på tekniksupport är ett problem som uppmärksammats i Österholms (2005) undersökning om nätburen examination. Denna support bör organiseras på flera nivåer enligt den kartläggning som gjorts.

Det är inte många som har problem med att identifiera de användare som skickar meddelanden och dokument i kurserna. Denna identifiering kan bara gälla det vi benämner legitim autentisering (se sid. 7). Att nå den tredje nivån, den personliga kräver god kännedom om personen eller andra åtgärder.

Det är en mindre andel studenter som anser att det är större risk för fusk vid distansstudier i jämförelse med traditionell campusutbildning. Här är det nästan var fjärde lärare som indikera att risken för fusk är större vid distansstudier. Många lärare vidtar speciella åtgärder för att beivra fusk men om dessa skiljer sig mot den traditionella utbildningen går inte at utläsa på grund av frågeformuleringen. Nästan lika många ägnar mer tid åt att förebygga fusk i distansutbildningen i jämförelse med en campusutbildning. Om man tolkar svaren från dem som anser att risken för fusk är större vid distansstudier finns det anledning att tro att deras examinationssystem bygger på traditionella tentamen. Då uppsatsskrivning, hemtentor, och processprotokoll inte förutsätter personlig närvaro vid ett visst tillfälle och om uppgifterna till sin uppbyggnad inte ställer frågor på detaljnivå är det vår bedömning att det inte bör finnas någon större skillnad mellan campus och distansutbildning vad avser möjligheter till fusk. Om läraren har rutiner för att följa en students skrivprocess är det vår bedömning att risken för fusk inte bör vara större. Möjligen är det så att det som förklarar den ökade tidsåtgången som

några lärare upplevde när det gäller att beivra fusk är att de måste välja examinationsformer som kräver mer tid av läraren och att det inte går att använda sig av traditionella tentor som kanske övervakas och rättas av annan personal.

Många användare inser sitt eget ansvar i säkerhetsarbetet och tror på en ökad säkerhet i framtiden även om säkerheten redan nu bedöms som bra. Denna framtidstro finns också uttryckt i Westerberg, och Måralds undersökning (2004).

6 DISKUSSION

Grunden och utgångspunkten för undersökningen har varit att betrakta problemområdet främst ur fyra delområden nämligen riktighet, tillgänglighet, sekretess och spårbarhet. Detta relativt rymliga sätt att se på området har sannolikt inte bottnat hos alla respondenter, utan många sammankopplar IT-säkerhet med rent tekniska åtgärder. Detta går att skönja i de svar som respondenterna avger på vissa frågor.

Trots uppenbara säkerhetsbrister i flera områden anser studenter och lärare att IT-säkerheten är god. Det verkar finnas en diskrepans mellan respondenternas kunskaper/attityder och deras agerande i verkliga situationer. Några exempel på detta är hantering av personuppgifter samt publicering på nätet. Detta kan delvis förklaras med bristfälliga kunskaper om de lagar som gäller; med andra ord, det kan finnas säkerhetsproblem inom dessa områden som studenter och lärare inte är medvetna om. Om problemen förblir fördolda händer det också att respondenterna i regel bedömer sina kunskaper som goda medan oberoende observatörer, såsom IT-ansvariga/pedagoger kan ha en annan uppfattning. När det gäller problem med säkerhetskopiering och versionshantering eller med spridning av skadlig kod, är det ofta fråga om attityder snarare än bristande kunskaper. Även om användare har kännedom om riskerna händer det likväl att dokument går förlorade på grund av slarvig hantering eller att systemet blir utsatt för virussmitta. Som vi har konstaterat tidigare måste användare ha hög motivation att följa organisationens riktlinjer och att använda befintliga tekniska lösningar. Organisatoriska och tekniska kontrollåtgärder är viktiga delar för att stödja säkerhetsarbetet men de kan aldrig ersätta det individuella användaransvaret.

Det kan därför vara klokt att avslutningsvis rekapitulera de begrepp som ingår i en vidare definition av informationssäkerhet och diskutera resultatet utifrån dessa (avsnitt 6.1). I efterföljande avsnitt (6:2) ges sedan ett antal förslag till hur lärosätena med olika åtgärder kan förbättra IT-säkerheten.

6.1 Riktighet, tillgänglighet, sekretess och spårbarhet

Riktighet

Begreppet riktighet innefattar personintegritet, systemintegritet och informationskvalitet. Med integritet menas att de objekt som är föremål för skyddet ska fredas mot obehörig förändring (sid. 6).

Att känna till regler och policy kring användning av datorer, distansverktyg och Internet är viktigt för riktigheten. Här finns det brister både bland studenter och bland lärare. Många har fått informationen, oftast skriftligt, men inte riktigt tagit den till sig. Ett annat område som är viktigt för riktigheten är kunskaper om de regler som gäller för elektronisk publicering, vilket också påverka sekretessen. Här är studenter och lärare klart osäkra hur de ska hantera det nya publikationssättet.

En illa skött versionshantering är även den ett hot mot riktigheten Det är en betydande andel studenter och lärare som utrycker att de har problem att hålla ordning på de olika versionerna som sparats.

Att hämta program och dokument från osäkra miljöer hotar riktigheten och riskerar därmed utbildningskvalitet. Enligt enkätsvaren förekommer detta relativt ofta.

Området är nära sammankopplat med problematiken kring fusk. Där är det uppenbarligen ett antal lärare som upplever att de har svårare att kontrollera riktigheten i de uppgifter och prov som utförs på distans. Att identifiera den som utför uppgiften är viktig i detta sammanhang och det hänger nära samman med området spårbarhet.

Tillgänglighet

Tillgänglighet innebär möjligheten att för behöriga användare utnyttja resurser efter behov och inom önskad tid (sid. 6).

Att det är god teknisk prestanda på de datorer som används i distansstudierna är viktigt för tillgängligheten. Även tillräcklig bandbredd har stor betydelse. Huvuddelen av respondenterna är nöjda med tekniska prestanda och bandbredd.

När det gäller datorsupport och snabb hjälp är även de viktiga faktorer för god tillgänglighet. Nästan en femtedel av studenterna anser att det inte ha fått tillräcklig hjälp. Även i detta fall finns det en skillnad mellan könen, kvinnorna anser att datorsupporten inte är tillräcklig i högre grad än vad männen gör.

När det gäller informationen runt distansverktygen är studenter, lärare och IT-ansvariga/pedagoger överens om att den måste bli bättre. Bättre information kring handhavandet hör till åtgärder som stärker tillgängligheten. En mycket viktig aspekt av tillgängligheten är användarvänligheten i de distansverktyg som används. Denna bedöms av samtliga respondenter som god men det finns en signifikant skillnad mellan könen, kvinnor anser sig ha något svårare att hantera dessa verktyg.

Datorvanan har betydelse för tillgängligheten och den uppges vara god såväl bland studenter som bland lärare. Kvinnor anser sig att ha något mindre datorvana än män och de studenter som kommer från ämnesgruppen Medicin/Vård bedömer att de har något lägre datorvana än de övriga grupperna.

Många är osäkra på hur de ska agera när det misstänker att datorn blivit smittat av ett virus, vilket kan påverka tillgängligheten. Virus ger ofta betydande driftstörningar för användaren. Här är det viktigt att snabbt kunna nå stöd och hjälp runt tekniska frågor vilket studenterna inte riktigt har klara rutiner och kanaler för. Hjälp med uppdatering av virusskydd samt installation och uppdaterande av brandväggar är också åtgärder som efterfrågas.

Tillgängligheten och säkerhetskopiering är begrepp som är nära kopplade till vartannat. Här finns anledning att uppmuntra åtgärder som stimulerar till en mer frekvent säkerhetskopiering och ett bättre val av lagringsmedia.

Sekretess

Sekretess innebär att känslig information inte får avslöjas för obehöriga. All information ska vara underordnade regler för åtkomst och behörighet (sid. 7).

Det är ett antal, både studenter och lärare som känner oro för att material ska läsas av obehöriga. Särskilt studenterna uttrycker en farhåga för att material som skickas inte når fram på ett korrekt sätt. Om denna oro är grundad på att verkliga brister i sekretess har uppstått framkommer inte ur resultatet. Sannolikt är denna brist på tillit grundad i okunskap om hur systemet fungerar.

När det gäller hanterandet av personuppgifter i kurser menar huvuddelen av lärarna att man gör detta på ett korrekt sätt. Studenter och IT-ansvariga/pedagoger har inte riktigt samma uppfattning. Det finns exempel i materialet som pekar på att felgrepp

förekommer. Att skydda användaridentiteten med lösen är en viktig sekretessfråga som fungerar relativt bra. Här finns det från de IT-ansvariga ett dubbelt budskap, ett explicit byt lösenord var tredje månad och ett implicit, om lösenordsbytet kräver minneslappar är det bättre att avstå. Det kunde därför vara idé att jämka runt kravet att byta lösenord var tredje månad.

Spårbarhet

Oavvislighet är en typ av spårbarhet. Det innebär att användaren inte i efterhand kan förneka att han/hon har skickat eller mottagit ett meddelande. Användaren kan heller inte förneka att han/hon deltagit i eller orsakat en handling (sid. 8).

En betydande del studenter anmäler inte regelmässigt om deras datorer blivit smittade av datavirus. Ännu fler är de studenter som inte anmäler tekniska fel till IT-ansvarig eller kursledare. Dessa rutiner sortera under området spårbarhet och förbättrade rutiner runt detta skulle stärka möjligheten till spårbarhet.

När det gäller att identifiera avsändaren är det många som instämmer i att man alltid kan se vem som skickar ett inlägg i webbkonferensen. Denna spårbarhet kan främst placeras på nivån legitim autentisering.

Beivrande av fusk har i allra högsta grad stor betydelse för spårbarhet. Ungefär en fjärdedel av lärarna menar att det kan vara vanskligare att upptäcka fusk vid distansundervisning i jämförelse med campusutbildning. Uppenbarligen känner ett antal lärare behov av att stärka igenkännandet på den personliga nivån av autentiseringen.

6.2 Pedagogiska implikationer

I det insamlade materialet har det funnits tydliga skillnader i uppfattningen om hur män och kvinnor bedömer sin datorvana. Vi kan dock konstatera att distanslärare och studenter i största allmänhet har en bra grundkompetens när det gäller datoranvändning. Den kunskap och tekniska prestanda som de båda grupperna förfogar över är tillsynes relativt god utifrån de krav som ställs i utbildningen där ofta enkla asynkrona textsystem används. Att använda ”enkel” teknik har varit ett framgångsrecept enligt många distansutbildare (Karlsudd, 2003). Då allt flera användare har både tillräckliga kunskaper och tekniska förutsättningar är det kanske lämpligt att ta ett steg till och börja använda ljud och bild i större utsträckning. Det finns forskningsresultat (Söderström, 2004) som visar att kommunikationen blir mer kontinuerlig om multimedia används synkront och asynkront. Om multimedia, bild- och ljudkommunikation nyttjades i större utsträckning är det i och för sig möjligt att en del av användarna skulle få uppgradera sina kunskaper och teknisk prestanda. Det som fördröjer denna utveckling är att en femtedel av studenterna fortfarande använder telefonmodem.

Support och stöd

Många önskar en utökning av stödfunktionerna runt IT-användning. Att detta är betydelsefullt för att upprätthålla hög kvalitet har framhållits av många forskare bl.a. Holmberg (1998) och Marklund (2002) som markerar vikten av stödjande strukturer för att IT-utbildning ska bli lyckosam. Sådana strukturer innefattar teknisk support och utbildning.

I distansutbildningen är läraren många gånger ensam i uppgiften att stötta studenten i datakommunikation och tekniska frågor. Mycket av den undervisning och det stöd som inkluderas är den enskilda lärarens uppgift, problem och utmaning (Sherer m.fl., 2003). Lärarna får sannolikt även i framtiden vara beredda att ge enklare support och teknisk vägledning men kan också i många delar avlastas från centralt håll. Att pröva en nationell central supportfunktion som komplement, likt den som universitetsbiblioteken prövat, vore ett intressant alternativ. Det kan finnas ett problem att stödja alla de olika lärplattformar som förekommer runt om på landets lärosäten, men i mångt och mycket är de lika till funktion och design, vilket många respondenter i denna undersökning verifierat.

Utbildning

Många i undersökningen anser att IT-säkerheten i distansutbildningen är god men önskar flera insatser för att ytterligare förstärka den. Ett sätt att öka förtroendet för tekniken är att i kursens inledningsskede använda kursverktygen i enkla och frekventa presentationsövningar. Att satsa mer på teknikintroduktionskurser vore en god idé som även Westerberg & Mårald (2004) förslagit i en rapport. Alla former av användarutbildning bör ha en positiv inverkan på IT-säkerheten. Om lärosätet har skickliga kursledare anställda och om studenterna är vana vid att använda IT-resurser, minskar risken för tillbud (Karlsudd, 2001). Adekvat användarutbildning kan tänkas vara speciellt viktig i nätbaserade distansutbildningar av flera skäl. Dessa utbildningar är starkt beroende av välfungerande IT-resurser, och frekventa säkerhetsproblem kan således påverka studieresultatet på ett mycket negativt sätt. Några vanliga problem är förknippade med bristande rutiner gällande säkerhetskopiering och versionshantering, bekymmer som relativt lätt skulle kunna undvikas med riktade utbildningsinsatser. Det är oftast distansstudenten själv som bär det största ansvaret för att den tekniska utrustningen fungerar och är skyddad mot virus och hackerintrång, speciellt när studenten arbetar vid sin dator hemifrån. Att bättre informera och stödja studenterna i programinstallation och programhantering är några angelägna åtgärder som kan vidtas. På de datorer där skolan ansvarar för driften fungerar uppenbarligen virusskydden bra och många gånger uppgraderas dessa automatiskt. En relativt enkel webbaserad säkerhetsutbildning med efterföljande test, kunde vara ett sätt att bättre avgöra vilka som tillgodogör sig säkerhetsinformationen och vilka eventuella hot som finns p.g.a. bristande kunskaper.

Brister i teknik och säkerhet är troligen inte det största hotet mot kvalitén i distansutbildningen. I rapporten, ”Läkare lär på länk”, som utvärderat en distansutbildning för specialistläkare bedöms utbildning och övning kring handhavandet av IT-inslag och kursens pedagogiska design vara betydligt viktigare (Jokela & Karlsudd, 2004).

> Kvaliteten på utbildningen har enligt vår bedömning inte så mycket med den tekniska standarden att göra. Den teknik som krävs är tillgänglig men det behövs mer erfarenhet och övning när det gäller förberedelse och genomförande. Att utbilda och öva kring handhavande av IKT kan därför vara en lämplig åtgärd. Vad som är mer avgörande är kursens design och metodiska vägval. (a.a. s, 79)

På huvuddelen av landets universitet och högskolor finns det adekvat information kring säkerhet på nätet. En åtgärd som sannolikt skulle höja kvaliteten på de informations-

insatser som görs skulle vara att samla de utbildningsansvariga till ett erfarenhetsutbyte och där dela med sig av de informationsmaterial som producerats. En annan åtgärd som ytterligare kan förstärka arbetet är att utse en huvudansvarig på varje institution att ansvara för information och utbildning kring IT-säkerhet.

I detta sammanhang är det väsentligt att lärare och kursdeltagare kan bygga upp förtroende för varandra i den virtuella studiemiljön. Detta kan förmodligen åstadkommas genom en kombination av förebyggande utbildning/information, nya examinationsformer och tekniska hjälpmedel. Det är viktigt att genom olika åtgärder stärka det vi kallar personlig autentisering (se avsnitt spårbarhet).

Det finns ett uttalat behov från respondenterna att lära mer om regler för publicering på nätet. Det finns en hel del material om juridiska frågor runt webbpublicering men det är inte alltid denna information når användarna trots att t.ex. legala handboken finns lätt tillgängligt på nätuniversitetets hemsida.

Åtgärder mot fusk

Det är en del av lärarna som anser sig lägga mer tid på att beivra fusk i distansutbildning och då vidtar åtgärder som de inte använder i campusutbildningen. Vilka dessa åtgärder är framgår dock inte av undersökningen. Här vore det intressant att gå vidare och utröna vilka åtgärderna är och vad som skiljer dessa från övriga insatser. Det problematiska är troligen att försäkra sig om att det är studenten som svarat på uppgiften, personlig autentisering, ett problem som även gäller hemskrivningar och uppsatser i campusutbildningen. Måhända bedömer lärarna att man har en bättre bild av studenten efter fysiska möten. Att det tekniska inslaget inte bör innebära några problem vid examination menar Marklund (2002). Kanske kan problematiken i högre grad vara kopplad till den som examinerar (Westerberg & Mårald, 2004). Med ett kontinuerligt och formativt examinationssystem minskar troligen risken för fusk (Gunnarsson, m.fl. 2002). Att som lärare följa hela arbetsprocessen kan vara en väg att beivra fusk. Studenterna kan t.ex. skriva processdagbok vilket gör det lättare för läraren att följa arbetets fortskridande. Det är också viktigt att försöka formulera uppgifter på ett sådant sätt att det är svårt att finna färdiga lösningar på nätet t.ex. genom att konsekvent välja uppgifter som kräver egen analys och undvika uppgifter som inbjuder till reproduktion. Ett försök att bättre hantera process och dokumentation i uppsatsarbetet prövas för närvarande i ett projekt ”Uppsatsdialogen” som stöds av Nätuniversitetet.

Erfarenheter som utgångspunkt för vidare forskning

Det är särskilt viktigt att beakta de skillnader som har observerats mellan könen och som även återspeglas i ämnesområden där andelen kvinnliga studenter är högre, dvs. Omvårdnad. Det insamlade materialet pekar på att kvinnliga studenter kan känna sig mera osäkra när det gäller hantering av teknisk utrustning och att de skulle vilja ha mera utbildning i datoranvändning samt mera datorsupport.

Återigen vill vi poängtera att denna undersökning inte kan användas för att visa hur de verkliga förhållandena är i hela populationen dels för att det insamlade materialet är för litet, dels för att det är fråga om individens subjektiva bedömning av egna kunskaper och behov av utbildning och datorstöd. Det skulle därför vara av stort intresse att göra en mer detaljerad studie om hur förstärkt användarutbildning och datorsupport kan leda till att kvinnliga distansstudenter känner större tillit gentemot tekniken och –

vilket är än viktigare – att de litar på sina egna kunskaper och färdigheter. Detta resonemang kan stödjas även av det faktum att i denna undersökning är det övervägande kvinnor som bedriver sina distansstudier hemifrån och därför inte alltid har omedelbar tillgång till hjälp i sin närmiljö vid själva studiesituationen. Som vi har konstaterat tidigare måste distansstudenter i regel ta större ansvar för sin egen studiemiljö, vilket ställer högre krav på studenternas förkunskaper och motivation att medverka i utbildningens totala informationssäkerhet.

En av många andra intressanta frågor att gå vidare med är att belysa de presumtiva distansstudenter som valt att inte söka distanskurser pga. att de anser sig sakna det stöd som krävs. Kanske skulle fler studenter söka och påbörja utbildningen om de var medvetna om att deras tekniska kompetens sannolikt räcker för att genomföra utbildningen. Det gäller allmänt att kunna öka tilliten till den grundläggande infrastrukturen som inkluderar IT-resurser och kursadministration. Förmodligen är det allra viktigaste att de som är involverade i nätutbildningar kan känna tillit till sina egna kunskaper och färdigheter.

Det finns en klar framtidstro på webbaserad utbildning och IT-inslaget kommer med all sannolikhet att öka inom den högre utbildningen. Förhoppningsvis kommer utvecklingsstöd och forskning att öka i samma takt.

REFERENSER

Allwood, C. M. (1998). *Människa-datorinteraktion: ett psykologiskt perspektiv.* Lund: Studentlitteratur.

Borg, T., Lozano, A., Löfgren, T., Malmgren, S. & Palicki, J. (1997). *IT-Säkerhet för ditt företag.* Uddevalla: Bonnier DataMedia.

Brandt, P. & Wennberg, L. (2004). *Informatisk forskning om riskanalysprocess applicerad på Apoteket AB:s kundcenterverksamhet. (*Licentiate Dissertation Series No 2004:09). Karlskrona: Blekinge Tekniska Högskola

Dahlin, B. (2000). *Om IKT baserad distansutbildning och "flexibelt lärande": En forskningsöversikt* (Karlstad University Studies 2000:20). Karlstad: Karlstads universitet.

Datainspektionen (1999). *Personuppgifter på Internet: undantag från förbudet i 33 § personuppgiftslagen: rapport till regeringen den 1 mars 1999.* Stockholm: Datainspektionen.

Edenholm, Y. (2000) Om femtio år finns inte skolan kvar längre. *Computer Sweden 12. 8 december*

Gali, P. (1992). *Informationssäkerhet: Hur du skyddar data, text, ljud och bild.* Linköping: Affärslitteratur AB.

Gunnarsson, M., Lingefjärd, T., Mekki-Berrada, T. & Sjöblom, C-A. (2002). *Flexibelt lärande – lärande examination. FLEX".* UFL-rapport 2002:1. Göteborg: Göteborgs universitet.

Hjelm, J. & Sandred, J. (1997). *Framtidens Utbildare.* Uddevalla: Bonnier DataMedia.

Holmberg, C. (1998). *På distans – utbildning, undervisning och lärande.* SOU: 1998:83.

Högskoleverket (2002). *Sammanställning av beslut från disciplinnämnder och domar i disciplinärenden från förvaltningsdomstolar 2001.* Stockholm: Högskoleverket.

Högskoleverket 2003:24R. *Sammanställning av beslut domar i disciplinärenden som rör studerande vid universitet och högskolor 2002.* Stockholm: Högskoleverket.

Högskoleverket 2004:17R. *Sammanställning av beslut domar i disciplinärenden som rör studerande vid universitet och högskolor från 2003.* Stockholm: Högskoleverket.

Högskoleverket 2005:28R. *Disciplinärenden 2004 vid högskolor och universitet med statligt huvudmannaskap.* Stockholm: Högskoleverket.

Högskoleverket: Högskoleförordningen 1993:100

Jandér, K. (2005). *Tillgång till digitala lärresurser inom högskolan – en förstudie*. Nätuniversitetet.

Jareborg, N. (2002). *Disciplinansvar för studenter som fuskar eller stör.* Konferens om disciplinregler anordnad av juridiska avdelningen vid Högskoleverket, 2002.

Karlsudd, P (2003). *Att lära på tunna linor och bred(a) band : e-learning : ambition, mission och vision : en granskning av e-utbildningsföretagens pedagogiska grundsyn*. Kalmar: Högskolan i Kalmar, Inst. för hälso- och beteendevetenskap.

Karlsudd, P. (2001). *Att lära på tunna linor och bred(a) band : IT-säkerhet i utbildning baserad på informations- och kommunikationsteknologi*. Kalmar: Högskolan i Kalmar, Inst. för hälso- och beteendevetenskap.

Legala handboken, Nätuniversitet http://www.legalahandboken.netuniversity.se/ 2005-10-03

Light, G. & Cox, R.(2001). *Learning & teaching in higher education – the reflective professional.* London: SAGE Publications.

Marklund, K. (2002). ”Högskoleläraren är framtidens hjälte” I Borg, Christian (red) *Vetenskapernas visioner. Elva samtal om framtidens studier och undervisning i högskolan*. Distum, Rapport ¤:2002, Härnösand.

Martin, B. (2004). *Plagiarism: Policy against cheating or policy for learning.* Nexus, Vol 16, No 2, pp 15-16.

Mårald, G., & Westerberg, P (2004). IT-stödd distansutbildning inom medicin och vård höstterminen 2003 – ur studenternas perspektiv. Umeå: Centre for Evaluation Research.

SFS 1998:204, Personuppgiftslag (PUL)

Sherer, P, et al. (2003). Online Communities of Practice: A Catalyst for Faculty Development, In: *Innovative Higher Education*, Vol 27, No 3, 2003.

Siponen, M.T., (2000). *Critical analysis of different approaches to minimizing user-related faults in information security: implications for research and practice.* Information Management & Computer Security, 8/5, pp 197-209.

Statskontoret (1997:29). *Handbok i IT-säkerhet. Del III. Skyddsåtgärder.* Stockholm: Statskontoret.

Söderström, T. (2004). *Studenternas uppfattningar om datorkommunikation-inom Nätuniversitetets medicin- och vårdutbildningar.* Umeå Centre for Evaluation Research.

Truedson, L. (2000). *Internett på gott och ont.* Statens skolverk. Stockholm: Liber distribution.

Upphovsrättslagen: SFS 1960:729, SFS 2005:359 och SFS 2005:360.

Westerberg, P. & Mårald, G. (2004). *Nätuniversitet och IT-stödd distansutbildning – Attityder och erfarenheter hos prefekter, kursansvariga och studenter.* Umeå: Centre for Evaluation Research.

Wiedersheim-Finn, F. (2005) *Plagiathandbok.* Uppsala: Uppsala Universitet, Företagsekonomiska institutionen.

Österholm, I. (2005). *Nätburen examination*. Nätuniversitetet.

Östlund, M. (2000). *Skapandet av ett webbaserat enkätverktyg EnkätArkitekten - webb-enkäter för alla.* C-uppsats, informatik. Kalmar: Baltic Business School, Högskolan i Kalmar.

BILAGOR

Bilaga 1

Tabell 5.1

Jag har god datorvana	Instämmer inte	Instämmer	Medelvärde
Studenter	12 %	61 %	3,77
Lärare	1 %	75 %	4,15

Tabell 5.2

Jag har tagit del av universitetets/högskolans regler och policy för användning av datorer, distansverktyg och Internet	Instämmer inte	Instämmer	Medelvärde
Studenter	23 %	47 %	3,49
Lärare	18 %	58 %	3,66

Tabell 5.3

Studenter har tagit del av universitetets /högskolans regler och policy för användning av datorer, distansverktyg och Internet	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	4 %	37 %	3,79

Tabell 5.4

Jag har goda kunskaper om de regler som gäller för publicering på nätet	Instämmer inte	Instämmer	Medelvärde
Studenter	36 %	33 %	2,96
Lärare	25 %	46 %	3,36

Tabell 5.5

Studenter/lärare har goda kunskaper om de regler som gäller för publicering på nätet	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	22 %	7 %	2,69
IT-ansvarig/ pedagog bedömer lärare	30 %	26 %	2,95

Tabell 5.6

Jag vet vilka åtgärder som måste vidtas om jag misstänker att min dator har blivit smittad av ett datavirus	Instämmer inte	Instämmer	Medelvärde
Studenter	26 %	52 %	3,43
Lärare	19 %	57 %	3,76

Tabell 5.7

Jag vet vart jag ska vända mig för att få hjälp när tekniska problem inträffar	Instämmer inte	Instämmer	Medelvärde
Studenter	27 %	49 %	3,44
Lärare	6 %	30 %	4,44

Tabell 5.8

Studenter och lärare vet vart de ska vända sig för att få hjälp när tekniska problem inträffar	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	0 %	78 %	4,15
IT-ansvarig/ pedagog bedömer lärare	0 %	89 %	4,41

Tabell 5.9

Jag är medveten om de säkerhetsrisker som finns förknippade med användning av datorkommunikation	Instämmer inte	Instämmer	Medelvärde
Studenter	18 %	58 %	3,72
Lärare	9 %	70 %	4,05

Tabell 5.10

Kursledarna/studenterna är medvetna om de säkerhetsrisker som finns förknippade med användning av datorkommunikation	Instämmer inte	Instämmer	Medelvärde
Studenter bedömer lärare	9 %	19 %	3,48
Lärare bedömer studenter	15 %	15 %	3,04

Tabell 5.11

Studenter/lärare är medvetna om de säkerhetsrisker som finns förknippade med användning av datorkommunikation	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	18 %	19 %	2,93
IT-ansvarig/ pedagog bedömer lärare	30 %	22 %	2,95

Tabell 5.12

Jag känner aldrig oro för att material som jag skickar med distansverktygen kan läsas av obehöriga	Instämmer inte	Instämmer	Medelvärde
Studenter	19 %	52 %	3,58
Lärare	19 %	57 %	3,54

Tabell 5.13

Jag känner aldrig oro för att material som jag skickar med distansverktygen kan försvinna	Instämmer inte	Instämmer	Medelvärde
Studenter	31 %	42 %	3,10
Lärare	18 %	51 %	3,44

Tabell 5.14

Jag anser att IT-säkerheten som helhet är god i distansutbildning	Instämmer inte	Instämmer	Medelvärde
Studenter	1 %	67 %	4,19
Lärare	1 %	64 %	3,94
IT-ansvarig/ pedagog	0 %	67 %	4,05

Tabell 5.15

Jag kan använda de tillgängliga distansverktygen utan några större problem	Instämmer inte	Instämmer	Medelvärde
Studenter	4 %	78 %	4,21
Lärare	3 %	71 %	4,06

Tabell 5.16

Studenter kan hantera tillgängliga distansverktygen utan några större problem	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	7 %	56 %	3,65

Tabell 5.17

Jag anser att kursledningen/jag hanterar personuppgifter på ett korrekt sätt	Instämmer inte	Instämmer	Medelvärde
Studenter	2 %	34 %	4,17
Lärare	0 %	87 %	4,47
IT-ansvarig/pedagog	4 %	59 %	4,29

Tabell 5.18

Jag har aldrig känt mig hotad eller personligt attackerad i en distanskurs	Instämmer inte	Instämmer	Medelvärde
Studenter	13 %	81 %	4,39
Lärare	21 %	74 %	4,08

Tabell 5.19

Hot och personliga påhopp är ovanliga i distanskurser	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog	18 %	59 %	3,92

Tabell 5.20

Vid valet av ett lösenord följer jag alltid speciella regler när det gäller lösenordets längd och konstruktion. Exempelvis att lösenordet måste vara minst sex tecken långt och innehålla specialtecken.	Instämmer inte	Instämmer	Medelvärde
Studenter	11 %	70 %	4,19
Lärare	21 %	66 %	3,82

Tabell 5.21

Jag byter mitt lösenord minst en gång per termin	Instämmer inte	Instämmer	Medelvärde
Studenter	66 %	20 %	2,03
Lärare	68 %	21 %	2,19

Tabell 5.22

Jag skyddar mitt lösenord på ett betryggande sätt	Instämmer inte	Instämmer	Medelvärde
Studenter	15 %	64 %	3,93
Lärare	13 %	63 %	3,92

Tabell 5.23

Studenter/lärare konstruerar och hanterar sina lösenord på ett korrekt sätt	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	8 %	50 %	3,92
IT-ansvarig/ pedagog bedömer lärare	15 %	52 %	3,94

Tabell 5.24

Jag har sällan problem med versionshantering (med att veta vilket dokument som är det senaste).	Instämmer inte	Instämmer	Medelvärde
Studenter	17 %	54 %	3,69
Lärare	16 %	60 %	3,64

Tabell 5.25

Studenter/lärare har sällan problem med versionshantering	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	9 %	41 %	3,48
IT-ansvarig/ pedagog bedömer lärare	15 %	33 %	3,33

Tabell 5.26

Jag gör ofta en säkerhetskopia på mitt arbete	Instämmer inte	Instämmer	Medelvärde
Studenter	25 %	58 %	3,62
Lärare	19 %	59 %	3,60

Tabell 5.27

Studenter/lärare gör ofta en trygg säkerhets-kopiering på sina dokument	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	19 %	12 %	2,92
IT-ansvarig/ pedagog bedömer lärare	23 %	35 %	3,26

Tabell 5.28

Jag uppdaterar mina antivirusprogram regelbundet	Instämmer inte	Instämmer	Medelvärde
Studenter	14 %	67 %	4,05
Lärare	6 %	82 %	4,34

Tabell 5.29

Studenter och lärare har uppdaterade antivirusprogram och brandväggar på de datorer de använder i distansundervisningen.	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	12 %	0 %	2,71
IT-ansvarig/ pedagog bedömer lärare	0 %	84 %	4,48

Tabell 5.30

Jag utnyttjar inga program som hämtas från osäkra miljöer (exempelvis okontrollerade program från Internet eller andra allmänna källor)	Instämmer inte	Instämmer	Medelvärde
Studenter	15 %	50 %	3,73
Lärare	18 %	66 %	3,88

Tabell 5.31

Jag öppnar inga program eller dokument som hämtas via Internet eller e-post utan viruskontroll	Instämmer inte	Instämmer	Medelvärde
Studenter	10 %	61 %	4,08
Lärare	15 %	66 %	3,89

Tabell 5.32

Studenter/lärare öppnar inga program eller dokument som hämtas via Internet eller e-post utan viruskontroll	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	8 %	8 %	3,00
IT-ansvarig/ pedagog bedömer lärare	8 %	41 %	3,74

Tabell 5.33

Jag informerar avsändaren om jag upptäcker ett datavirus	Instämmer inte	Instämmer	Medelvärde
Studenter	20 %	50 %	3,69
Lärare	26 %	41 %	3,29

Tabell 5.34

Jag rapporterar alltid tekniska problem till den IT-ansvariga och/eller till kursledaren	Instämmer inte	Instämmer	Medelvärde
Studenter	34 %	34 %	3,04
Lärare	6 %	75 %	4,19

Tabell 5.35

Studenter/lärare rapporterar alltid tekniska problem till den IT-ansvariga och/eller till kursledaren	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	15 %	34 %	3,56
IT-ansvarig/ pedagog bedömer lärare	7 %	78 %	4,25

Tabell 5.36

Jag har tillräckligt bra teknisk datautrustning för att kunna klara av mina distansstudier/undervisning	Instämmer inte	Instämmer	Medelvärde
Studenter	3 %	88 %	4,47
Lärare	7 %	75 %	4,28

Tabell 5.37

Distansstudenter har tillgång till en tillräckligt snabb Internetuppkoppling.	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	7 %	63 %	3,68
Distansstudenter har tillräckligt bra datautrustning för att klara av sina studier			
IT-ansvarig/pedagog bedömer student	4 %	53 %	3,74

Tabell 5.38

	diskett	CD	hårddisk	USB-minne	Lärosätets server	Annat medium	Lagrar ingen kopia
Studenter	30 %	16 %	76 %	16 %	13 %	8 %	6 %
Lärare	9 %	21 %	46 %	21 %	72 %	6 %	3 %

Tabell 5.39

Jag har antivirusprogram installerat i den dator som jag använder hemma	ja	Nej	Vet ej
Studenter	88 %	7 %	5 %
Lärare	97 %	3 %	-

Tabell 5.40

Jag har brandvägg installerad i den dator som jag använder hemma	Ja	Nej	Vet ej
Studenter	70 %	14 %	15 %
Lärare	63 %	22 %	15 %

Tabell 5.41

Jag får sällan oönskade e-meddelanden (spam) som stör mina studier/arbete	Instämmer inte	Instämmer	Medelvärde
Studenter	20 %	60 %	3,71
Lärare	39 %	47 %	3,08

Tabell 5.42

Oönskade e-meddelande (spam) stör sällan distansutbildningen	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog	15 %	71 %	4,20

Tabell 5.43

Det förekommer sällan tekniska driftstörningar i de distansverktyg som jag använder	Instämmer inte	Instämmer	Medelvärde
Studenter	16 %	57 %	3,60
Lärare	14 %	61 %	3,69
IT-ansvarig/pedagog	11 %	67 %	3,81

Tabell 5.44

Jag upplever inte att tekniska problem stör mina distansstudier	Instämmer inte	Instämmer	Medelvärde
Studenter	19 %	59 %	3,70
Lärare	11 %	62 %	3,84

Tabell 5.45

De distansverktyg som används på distanskurserna är stabila och säkra med avseende på sekretess, backup och spårbarhet (autentisering)	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog	7 %	56 %	3,96

Tabell 5.46

Jag är nöjd med de verktyg som används i distansutbildning	Instämmer inte	Instämmer	Medelvärde
Studenter	8 %	68 %	3,93
Lärare	16 %	62 %	3,58

Tabell 5.47

Det är funktionella distansverktyg som används i utbildningen	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog	0 %	77 %	4,21

Tabell 5.48

Information kring användandet av distansverktygen är tillräcklig	Instämmer inte	Instämmer	Medelvärde
Studenter	16 %	54 %	3,56
Lärare	16 %	53 %	3,56
IT-ansvarig/pedagog	11 %	51 %	3,57

Tabell 5.49

Undervisning kring användandet av distansverktygen är tillräcklig	Instämmer inte	Instämmer	Medelvärde
Studenter	23 %	43 %	3,34
Lärare	19 %	52 %	3,39
IT-ansvarig/pedagog	7 %	51 %	3,64

Tabell 5.50

Jag har fått tillräckligt mycket datorsupport under mina distansstudier	Instämmer inte	Instämmer	Medelvärde
Studenter	19 %	43 %	3,41
Lärare	13 %	66 %	3,74

Tabell 5.51

Datorsupporten till studenter/lärare som studera inom distansutbildning är tillräcklig	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig/pedagog bedömer student	16 %	69 %	3,68
IT-ansvarig/ pedagog bedömer lärare	15 %	71 %	3,67

Tabell 5.52

Jag kan alltid se vem som skickar ett inlägg eller lämnar ett dokument i kursens webbkonferens	Instämmer inte	Instämmer	Medelvärde
Studenter	7 %	61 %	4,21
Lärare	4 %	73 %	4,22

Tabell 5.53

Jag anser att risk för fusk inte är större vid distansstudier jämfört med traditionell campusutbildning	Instämmer inte	Instämmer	Medelvärde
Studenter	8 %	68 %	4,21
Lärare	24 %	43 %	3,25
IT-ansvarig/ pedagog	23 %	37 %	3,53

Tabell 5.54

Jag ägnar inte mer tid åt att förebygga fusk i distansutbildningen i jämförelse med campusutbildning	Instämmer inte	Instämmer	Medelvärde
Lärare	21 %	51 %	3,44

Tabell 5.55

Vid distansutbildning vidtar jag inga speciella åtgärder för att förhindra fusk	Instämmer inte	Instämmer	Medelvärde
Lärare	42 %	27 %	2,75

Tabell 5.56

Det är inte svårare att upptäcka fusk vid distansundervisning i jämförelse med campusutbildning.	Instämmer inte	Instämmer	Medelvärde
Lärare	26 %	37 %	3,18

Tabell 5.57

Jag anser att jag själv kan bidra till ökad IT-säkerhet i distansutbildning	Instämmer inte	Instämmer	Medelvärde
Studenter	17 %	34 %	3,33
Lärare	14 %	53	3,64

Tabell 5.58

Jag anser att jag lärare/studenter kan bidra till ökad IT-säkerhet i distansutbildning	Instämmer inte	Instämmer	Medelvärde
IT-ansvarig bedömer student	0 %	63 %	4,25
IT-ansvarig bedömer lärare	0 %	67 %	4,18

Tabell 5.59

Jag tror att IT-säkerheten i distansutbildning kommer att bli bättre i framtiden	Instämmer inte	Instämmer	Medelvärde
Studenter	3 %	59 %	4,24
Lärare	1 %	67 %	4,02
IT-ansvarig	0 %	59 %	4,00

BILAGA 2 Exempel på missiv

Till kursansvarig för kurs registrerad vid *Nätuniversitetet*.

På uppdrag av Nätuniversitetet utvärderas nu IT-säkerheten i ett antal Nätuniversitets-kurser. Tyngdpunkten på undersökningen ligger på kunskaper, agerande och attityder kring IT-säkerhet.

Vi har från Nätuniversitetet erhållit e-postadresser till kursansvariga och vi vill nu be dig delta i undersökningen.

Vi hoppas att du har möjlighet att avvara några minuter för att svara på enkäten. Vårt mål är att undersökningen ska bidra till ökad IT-säkerhet i distanskurser.

Medverkan är frivillig och ditt svar är anonymt. Om du inte svarat före den 2005-05-12 kommer du att få högst två påminnelser. Dessa skapas automatiskt av enkätsystemet utan att din e-postadress kopplas till dina svar.

Dokumentationen av hela undersökningen beräknas vara klar i början av augusti och kommer då att presenteras på Nätuniversitetets webbplats.

Klicka på länken längst ned i brevet så kommer du till enkäten.

Vårt mål är att undersökningen ska bidra till ökad IT-säkerhet i distanskurser.

Om du har några frågor kring undersökningen får ni gärna höra av er via e-post eller telefon.

Med vänliga hälsningar

Päivi Jokela Lektor i informatik och fysikalisk kemi

Peter Karlsudd Lektor i informatik och pedagogik

Högskolan i Kalmar

BILAGA 3 Exempel på enkät

UTVÄRDERING AV IT-SÄKERHETEN
Studentenkät

1. Jag är

- ☐ kvinna
- ☐ man

2. Jag är född år

3. Jag bor i

- ☐ tätort
- ☐ mindre samhälle
- ☐ glesbygd

4. När jag är uppkopplad mot högskolan/universitetet är det oftast via

- ☐ Bredband (ADSL, fiber/fast uppkoppling)
- ☐ ISDN
- ☐ Vanligt telefonmodem
- ☐ Vet ej

5. För mina studier använder jag datorn huvudsakligen

- ☐ hemma
- ☐ på Universitet/Högskola eller lärcenter
- ☐ arbetet
- ☐ annan plats

6. Jag deltar i Nätuniversitetsutbildning inom ämnesområdet

- ☐ Humaniora och teologi
- ☐ Juridik och samhällsvetenskap
- ☐ Medicin och odontologi
- ☐ Vård och omsorg
- ☐ Naturvetenskap
- ☐ Teknik

7. Nätuniversitetsutbildningen jag deltar i är

☐ Fristående kurs

☐ Programutbildning

Markera för varje påstående i vilken grad du instämmer med detta

8. Jag har god datorvana

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

9. Jag har tillräckligt bra teknisk datautrustning för att kunna klara av mina distansstudier

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

10. Jag kan använda de tillgängliga distansverktygen utan några större problem

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

11. Information kring användandet av distansverktygen är tillräcklig

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

12. Undervisning kring användandet av distansverktygen är tillräcklig

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

13. Jag har tagit del av universitetets/högskolans regler och policy för användning av datorer, distansverktyg och Internet

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

14. Jag är medveten om de säkerhetsrisker som finns förknippade med användning av datorkommunikation

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

15. Kursledarna är medvetna om de säkerhetsrisker som finns förknippade med användning av datorkommunikation

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

16. Jag anser att kursledningen hanterar mina personuppgifter på ett korrekt sätt

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

17. Jag känner aldrig oro för att material som jag skickar med distansverktygen kan läsas av obehöriga

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

18. Jag känner aldrig oro för att material som jag skickar med distansverktygen kan försvinna

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

19. Jag kan alltid se vem som skickar ett inlägg eller lämnar ett dokument i kursens webbkonferens

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

20. Jag har goda kunskaper om de regler som gäller för publicering på nätet

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

21. Jag har aldrig känt mig hotad eller personligt attackerad i en distanskurs

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

22. Vid valet av ett lösenord följer jag alltid speciella regler när det gäller lösenordets längd och konstruktion. Exempelvis att lösenordet måste vara minst sex tecken långt och innehålla specialtecken.

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

23. Jag byter mitt lösenord minst en gång per termin

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

24. Jag skyddar mitt lösenord på ett betryggande sätt

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

25. Jag har sällan problem med versionshantering (med att veta vilket dokument som är det senaste

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

26. Jag gör ofta en säkerhetskopia på mitt arbete

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

27. Jag lagrar alltid en kopia av mina arbeten på (välj ett eller flera alternativ)

☐ diskett

☐ hårddisk

☐ CD

☐ USB-minne

☐ lärosätets server

☐ annat medium

☐ jag lagrar inga kopior

---

28. Jag har antivirusprogram installerat i den dator som jag använder hemma

☐ Ja

☐ Nej

☐ Vet ej

---

29. Jag har brandvägg installerat i den dator som jag använder hemma

☐ Ja

☐ Nej

☐ Vet ej

---

30. Jag uppdaterar mina antivirusprogram regelbundet

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

31. Jag öppnar inga program eller dokument som hämtas via Internet eller e-post utan viruskontroll

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

32. Jag utnyttjar inga program som hämtas från osäkra miljöer (exempelvis okontrollerade program från Internet eller andra allmänna källor)

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

33. Jag vet vilka åtgärder som måste vidtas om jag misstänker att min dator har blivit smittad av ett datavirus

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

34. Jag informerar avsändaren om jag upptäcker ett datavirus

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

35. Jag får sällan oönskade e-meddelanden (spam) som stör mina studier

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

36. Det förekommer sällan tekniska driftstörningar i de distansverktyg som jag använder

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

37. Jag vet vart jag ska vända mig för att få hjälp när tekniska problem inträffar

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

38. Jag rapporterar alltid tekniska problem till den IT-ansvariga och/eller till kursledaren

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

39. Jag upplever inte att tekniska problem stör mina distansstudier

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

40. Jag anser att risk för fusk inte är större vid distansstudier jämfört med traditionell campusutbildning

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

41. Jag anser att IT-säkerheten som helhet är god i distansutbildning

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

42. Jag är nöjd med de verktyg som används i distansutbildning

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

43. Jag har fått tillräckligt mycket datorsupport under mina distansstudier

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

44. Jag anser att jag själv kan bidra till ökad IT-säkerhet i distansutbildning

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

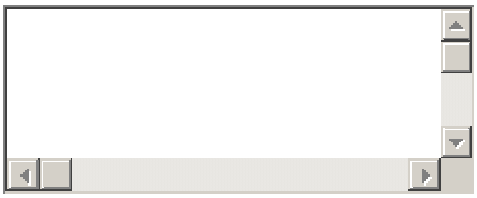
---

45. Jag tror att IT-säkerheten i distansutbildning kommer att bli bättre i framtiden

Inst. inte alls ☐ ☐ ☐ ☐ ☐ Inst. i hög grad ☐ Vet ej

---

46. Så här kan man förbättra IT-säkerheten i distansutbildningen:



---

47. Övriga kommentarer när det gäller distansutbildningen:

Tack för din medverkan!
Päivi Jokela och Peter Karlsudd