INFORMATIONSSÄKERHETS-GUIDE FÖR PERSONALEN

Februari 2014

INNEHÅLLSFÖRTECKNING

Denna informationssäkerhetsguide är i första hand avsedd för personalen vid universiteten. Guiden har utarbetats som ett samarbete mellan universitetens informationssäkerhets-experter och målet har varit att göra den lämplig för användning vid alla universitet.

Arbetsgrupp: Olavi Manninen (Itä-Suomen yliopisto), Mari Karjalainen (Oulun yliopisto), Matti Levänen (Jyväskylän yliopisto), Ulf Pensar (Svenska handelshögskolan), Jan Wennström (Åbo Akademi). Den svenskspråkiga versionen: Urpo Kaila (CSC), Ulf Pensar (Svenska handelshögskolan), Jan Wennström (Åbo Akademi), Kuno Öhrman (Svenska handelshögskolan).
Bilder: Raija Törrönen (Itä-Suomen yliopisto)
Layout: Raija Sassi (Helsingfors universitet)

Arbetsgruppen har utöver denna guide skapat två kompletterande guider: Kortversionen av informationssäkerhetsguiden innehåller en komprimerad uppläggning av de väsentligaste aspekterna. Anvisningar angående användningen av mobila enheter ges i mobilsäkerhetsguiden.

VARFÖR ÄR INFORMATIONSSÄKERHETEN VIKTIG FÖR DIG OCH UNIVERSITETET

- I medierna har du säkert lagt märke till olika slag av nyheter om informationssäkerhet. Har du någonsin tänkt på vilka informationssäkerhetshot som är förknippade med din dagliga it-användning?

- Exempelvis försöker nätfiskare komma åt ditt lösenord, som sedan kan används för att uppnå ekonomisk vinning.

- Sabotageprogram som sprids via nätet och e-posten är också allvarliga hot. De kan exempelvis stjäla eller förstöra filer, förmedla dina användarnamn och lösenord till den som gjort sabotageprogrammet eller göra datanäten långsammare.

- Det är viktigt att du fäster uppmärksamhet vid hur du själv agerar. Då du exempelvis använder molntjänster och e-post kan du av misstag förmedla information som hör till universitetet och ska skyddas.

- Att låta uppgifter som hör till ditt arbete läcka ut i fel händer kan skada universitetets verksamhet och rykte och ge upphov till ekonomiska förluster. Universitetets viktigaste kapital är kunskap – skydda informationen på ett korrekt sätt.

- Alla är skyldiga att sörja för informationssäkerheten genom att följa gällande lagstiftning och universitetets regler och anvisningar om informationssäkerhet.

- Denna informationssäkerhetsguide hjälper dig att skydda de uppgifter du behandlar, arbetsstationen och nätverket mot informationssäkerhetshot.

- Om du misstänker att den dator du använder har utsatts för ett sabotageprogram eller att ditt användarnamn och lösenord hamnat i fel händer, läs anvisningarna i slutet av guiden.

ANVÄND STARKA LÖSENORD OCH HÅLL DEM HEMLIGA

- Du loggar in till universitetets informationssystem med ett personligt användarnamn och lösenord. Ta hand om ditt användarnamn och ditt lösenord lika noggrant som ditt bankkort och din PIN-kod.

- Du ansvarar personligen för användningen av ditt användarnamn. Ge inte ditt lösenord till någon annan. Inte ens administratörerna ska känna till det. Om någon frågar efter ditt lösenord är personen i fråga garanterat ute i skumraskaffärer.

- Byt ditt lösenord tillräckligt ofta enligt universitetets anvisningar och omedelbart om du misstänker att någon annan än du själv känner till det.

- När du får ett nytt lösenord av it-stödet ska du genast byta ut det till ett sådant som endast du känner till.

- Välj ditt lösenord med omsorg. Ett bra lösenord är ett du själv lätt kommer ihåg, men som ingen annan kan knäcka. Använd inte alldagliga ord eller ord som anknyter till dig på något vis som lösenord. Undvik att skriva ner lösenordet som sådant. Bekanta dig med universitetets anvisningar för hur du väljer ett bra lösenord.

- De lösenord du använder för universitetets tjänster skall du inte använda i något system utanför universitetet. Om någon kommer över ditt lösenord i den utomstående tjänsten ska personen inte kunna komma in i universitetets system med samma lösenord.

ANVÄNDNING AV E-POST

- Du ska använda den e-postadress du har fått av universitetet i alla dina arbetsuppgifter. Det är förbjudet att använda e-posttjänster utanför universitetet för dina arbetsuppgifter. Det är även förbjudet att automatiskt styra arbetsplatsens e-post till externa tjänster.

- För tjänster och officiella förvaltningsuppgifter ska du i första hand använda särskilda organisations-e-postadresser, exempelvis registrator@universitet.fi.

- Om du får e-post som tillhör någon annan ska du meddela avsändaren om den felaktiga adressen. Kom ihåg att du har tystnadsplikt om meddelandet du har mottagit. Enligt förvaltningslagen ska ändå ett meddelande som gäller förvaltningsuppgifter i första hand sändas vidare till rätt mottagare, om du känner till denna.

- Sköt hanteringen av e-posten också då du är frånvarande från arbetet. Använd vid behov automatsvar till exempel under din semester för att tala om vem som sköter arbetsuppgifterna då du är frånvarande.

- Skilj klart och tydligt åt dina privata meddelanden, både de du fått och sänt, från dina arbets e-postmeddelanden (i separata e-postmappar).

- Då du skriver meddelanden ska du tänka på att mottagaren kan sända det meddelande du sänt i förtroende vidare till en större krets.

- E-postmeddelanden kan innehålla sabotageprogram eller leda dig vidare till en sida som innehåller sabotageprogram. Öppna inte ett meddelande om du inte är säker på dess ursprung eller om du inte har kommit överens om att ta emot ett meddelande. Be vid behov om närmare information av it-stödet.

- I datanätet sänds e-postmeddelanden i allmänhet i klartext, utan kryptering. Information som måste skyddas ska således krypteras innan meddelandet sänds utanför universitetet.

- Information som ska skyddas är, förutom konfidentiell information som hör till universitetets verksamhet, också exempelvis person- och kontaktuppgifter, bankuppgifter och uppgifter om hälsa.

- Överväg till vem du ger din e-postadress eller var du publicerar den. Undvik att använda universitetets e-postadress på nätforum och sociala nätverkstjänster (t.ex. Facebook) och skaffa dig en separat e-postadress för privatbruk. Då du använder universitetets e-postadress representerar du alltid också universitetet.

SE UPP FÖR NÄTFISKE OCH ANNAN BLUFF

- Var sunt misstänksam mot tillförlitligheten hos e-postmeddelanden. Ett e-postmeddelande kan komma från någon annan än vad som anges i avsändarfältet. Också sabotageprogram kan sända e-post utan att användaren vet om det.

- Akta dig för nätfiskemeddelanden som uppmanar dig att uppge ditt användarnamn och lösenord eller att skriva in dem på en webbsida. Administratörerna frågar aldrig efter ditt lösenord.

- Kontrollera alltid länkens verkliga adress innan du klickar dig vidare. Var speciellt försiktig om du fått länken i ett meddelande.

- Lär dig att skilja mellan seriösa webbadresser och adresser som används av bedragare. Bekanta dig med universitetets anvisningar.

- Reklam och kedjebrev som sänds utan mottagarens tillåtelse är skräppost. Besvara dem inte, utan förstör dem genast. Tro inte på erbjudanden som verkar alltför bra för att vara sanna.

- Universiteten använder sig av olika metoder för att filtrera skräppost och sabotageprogram och detta kan påverka leveransen av e-posten. Ta reda på hur man gör vid ditt universitet.

- Du kan bli utsatt för bedrägeriförsök på annat sätt än via e-post, till exempel per telefon eller i sociala medier. Akta dig för överraskande räkningar, falska meddelanden i it-stödets namn och överraskande uppmaningar som sänds i dina bekantas namn.

- Om du misstänker att du har blivit lurad eller att någon försöker lura dig kan du be om råd av it-stödet eller polisen.

ANVÄND NÄTTJÄNSTER OCH SOCIALA MEDIER MED EFTERTANKE

- Många nättjänster är molntjänster, vilket innebär att den information du matar in i tjänsterna endast lagras på tjänsteleverantörens servrar, ofta utanför Finlands gränser. Redan innan du tar i bruk en tjänst är det skäl att du i användningsvillkoren för tjänsten kontrollerar åtminstone att äganderätten till din information kvarstår och att din information inte överlåts vidare.

- Bekanta dig med universitetets anvisningar om deltagande i sociala medier. Kom ihåg att endast vissa aktörer vid universitetet har rätt att officiellt framträda i universitetets namn i offentliga medier.

- Använd ditt omdöme vid behandlingen av personuppgifter; överväg vilka uppgifter du kan lämna ut och till vem.

När det gäller dina egna uppgifter är det du som har prövningsrätten. För att lämna ut andra personers uppgifter ska du ha tillstånd av personerna i fråga.

- Använd i undervisningen i första hand tjänster som universitetet erbjuder. I allmänhet kan man förutsätta att studerande använder tjänster där man måste logga in endast ifall universitetet officiellt har godkänt tjänsten ifråga.

- Om du överväger att använda molntjänster ska du kontrollera hur tjänsten lämpar sig för användningsändamålet på högskolornas gemensamma webbsidor för utvärdering av molntjänster (länk i slutet av guiden). Om du behandlar konfidentiella uppgifter i molntjänsten ska du endast använda tjänster som anses säkra.

- Utred på förhand hur du, efter kursens slut, kan radera kursmaterial från nätet.

- När du använder olika nättjänster (Facebook, bilddelningstjänster o.d.) ska du överväga vilken slags information tillhörande dig eller någon annan som du laddar upp. Personliga uppgifter såsom en bild eller en hemadress som en gång lagts ut på nätet kan senare vara omöjliga att radera helt och hållet.

- I e-post och nätkommunikation är det klokt att följa så kallad nätetikett. Att i skrift uttrycka sig alltför bitskt i exempelvis diskussionsgrupper kan påverka ditt eget och universitetets rykte.

- Se upp för poppuppfönster och reklam som finns på webbsidorna. Sabotageprogram sprids effektivt i sociala medier och nättjänster – var uppmärksam innan du klickar.

- Kontrollera de inställningar i din användarprofil som påverkar ditt integritetsskydd (dvs. vem som har tillgång

till uppgifter om dig) och justera inställningarna vid behov. Kom ihåg att den som erbjuder tjänsten kan ändra på användarvillkoren rätt ofta.

- I sociala nätverk är det lätt att låtsas vara en annan eller en annorlunda person. Förhåll dig inte alltför blåögt till det du läser.

- Spara inte platsinformation i de bilder du laddar upp till nättjänster. Inaktivera GPS-funktionen i din kamera eller radera platsinformationen från bilderna innan du publicerar dem.

ANVÄND ARBETSGIVARENS DATORER ANSVARSFULLT

- Logga alltid in på datorn med eget användarnamn.

- Om du använder en dator som är i gemensamt bruk vid universitetet ska du radera eventuella temporära filer innan du loggar ut.

- Lås alltid datorn då du avlägsnar dig, också om det bara är för en kort stund (på Windows datorer: Win-L). Det här förhindrar att ditt användarnamn och dina filer missbrukas.

- Spara allt viktigt material på nätskivan eller i din hemkatalog. Då sköter universitetet om att det säkerhetskopieras.

- Spara det du jobbar med med jämna mellanrum (i många Windows-program Ctrl-S) om du jobbar med text eller annat material under en längre tid. På så sätt går du inte miste om ditt arbete vid ett avbrott.

- Om du använder en gemensam skrivare ska du hämta dina papper genast.

- Förstör konfidentiella utskrifter och dokument med en dokumentförstörare eller lägg dem i en låst datasekretessbehållare.

- Att installera program på universitetets datorer är i allmänhet förbjudet och ofta också spärrat. Kontakta it-stödet om du behöver något specifikt program.

- Om du använder universitetets dator som du har administratörsrättigheter till ska du följa nedanstående principer för underhåll av en hemdator.

SE TILL ATT DIN HEMDATOR FUNGERAR VÄL

Du är administratör för din hemdator. Följ med hur din dator fungerar och beakta informationssäkerheten genom att följa nedanstående anvisningar.

- En dator som är ansluten till nätet ska alltid skyddas med brandvägg och skydd mot sabotageprogram.

- Installera endast program som du verkligen behöver. Installera programmens säkerhetsuppdateringar. Radera program du inte längre behöver.

- Skapa personliga användarnamn (utan administratörsrättigheter) för alla användare, även för dig själv. Administratörskonton ska inte användas för annat än underhållsuppgifter (installation av program, skapande av nya användarnamn).

- Ta regelbundet säkerhetskopior av hemdatorns filer. Spara dina säkerhetskopior separat från datorn och om möjligt på ett ställe som kan låsas.

– Datorer, smarttelefoner och minnespinnar som tas ur bruk ska inte slängas bland övriga sopor. Data raderas genom att du skriver över det eller förstör mediet. För pappersmaterial ska du använda en dokumentförstörare.

SKÖT OM DIN MINNESPINNE

– Använd inte din minnespinne som den huvudsakliga eller enda lagringsplatsen för dina filer, trots att den är behändig för att flytta information och för säkerhetskopiering. Din minnespinne kan lätt tappas bort.

– Om du sparar känsligt material på din minnespinne bör du skaffa en minnespinne som krypterar informationen automatiskt eller själv se till att informationen krypteras.

– Var försiktig med andra användares minnespinnar. De kan innehålla sabotageprogram som aktiveras automatiskt och infekterar din dator.

– Om du på universitetet hittar någon annan användares minnespinne ska du lämna in den till universitetets it-stöd utan att granska dess innehåll.

DISTANSANVÄNDNING – ANVÄNDNING AV DATOR UTANFÖR ARBETSPLATSEN (I HEMMET, PÅ RESOR)

– Bekanta dig med universitetets anvisningar (anvisningar för distansarbete, klassificering av information osv.) och utred vilket slags material du får behandla hemma och på resor.

– För att sköta dina arbetsuppgifter ska du i huvudsak använda din arbetsgivares utrustning.

– Din arbetsgivares utrustning är avsedd för endast ditt bruk. Du ska inte låna den ens till dina familjemedlemmar.

– Använd VPN-kontakt som ger dig skyddad kontakt till universitetets tjänster.

– På resor ska du skydda din dator mot stöld. Det rekommenderas att hårddisken skyddas med kryptering.

– Om du hemma behandlar konfidentiellt material i pappersform ska du se till att det förvaras och förstörs på ett korrekt sätt.

SE UPP FÖR ÖPPNA TRÅDLÖSA NÄTVERK OCH DATORER I ALLMÄNT BRUK

– När du använder trådlösa nätverk ska du använda endast sådana e-post- och nättjänster som krypterar datatrafiken (adressen ska börja med https://) eller en skyddad VPN-kontakt.

– Observera att din dator- och programanvändning alltid efterlämnar spår och att information om dig sparas. Ta på förhand reda på hur du tömmer cacheminnet i webbläsaren och hur du raderar de vanligaste spåren av din datoranvändning.

– Lita inte på att datorer i nätcaféer, bibliotek och offentliga rum är säkra. Dessa datorer kan innehålla program som samlar in användaruppgifter. Överväg om det är nödvändigt för dig att exempelvis logga in till e-posten via en sådan dator.

SE OCKSÅ TILL SÄKERHETEN FÖR DINA MOBILA ENHETER

– Telefoner, pekplattor och andra mobila enheter ska skyddas på motsvarande sätt som datorer.

- Öppna inte textmeddelanden som du får från en okänd avsändare eller som annars verkar misstänkta. De kan innehålla sabotageprogram som sänder meddelanden i ditt namn eller annars ger upphov till tilläggskostnader.

- Skydda din mobila enhet mot stöld. Skydda enheten med en låskod (utöver PIN-koden) så att andra inte kommer åt informationen på den. Ta reda på om innehållet i enheten vid behov kan raderas på distans.

- Stäng alltid av trådlös kommunikation (Bluetooth och WLAN) när du inte behöver den.

- Se också till att informationen på de mobila enheterna säkerhetskopieras. Radera informationen i enheten när den tas ur bruk.

- Installera endast program som du verkligen behöver. Ladda ner och installera program endast från officiella webbplatser.

- Utomlands är kostnaderna för datatrafiken höga, använd enheten med eftertanke.

- Överväg om du vill publicera dina platsuppgifter i olika nättjänster.

DÅ ANSTÄLLNINGEN UPPHÖR

– Rätten att använda universitetets it-tjänster är bunden till din anställning.

– Då din anställning upphör, inaktiverar universitetet ditt användarnamn och efter en viss tid raderas också din e-postkatalog och andra filer. Innan ditt användarnamn inaktiveras ska du:

  - Informera dina samarbetspartner om att din e-post-adress ändras.
  - Kom i god tid överens med din chef om överlåtelse av arbetsmaterial till universitetet.
  - Ta till vara dina egna filer som du vill spara och radera dina övriga filer från universitetets servrar.
  - Kopiera dina privata e-postmeddelanden till dig själv eller sända dem vidare till din nya e-postadress.
  - Avinstallera de program från din dator och övriga enheter som du fått via universitetet och som du inte längre har användningsrätt till.

SABOTAGEPROGRAM ELLER DATASÄKERHETSFÖRSEELSE?

– Skyddsprogram kan inte erbjuda fullständigt skydd mot sabotageprogram eftersom de ständigt ökar i antal. Om du misstänker att någon dator du använt är eller har varit infekterad av ett sabotageprogram ska du:

  1. Via en annan dator genast byta lösenorden till alla de konton som du använt från den infekterade datorn. Om du använt samma lösenord för andra tjänster så byt också lösenorden för de tjänsterna. För att reda ut

missbruket ska du kontakta kundtjänsten för de viktigaste tjänsterna du använt. Berätta om din misstanke att ditt användarnamn möjligen blivit kapat.

2. Om det är fråga om din egen dator ska du inte använda den förrän du vet hur du kan avlägsna sabotageprogrammet. Om det är någon annan som äger datorn ska du kontakta personen eller organisationen som ansvarar för datorn och informera om situationen. För att rensa din egen dator kan du få begränsad hjälp av universitetets it-stöd eller via webbsidan för ditt antivirusprogram.

- Om du misstänker en datasäkerhetsförseelse eller missbruk av systemen ska du kontakta den som ansvarar för tjänsten. Om tjänsten är universitetets eller om du använde tjänsten med ett användarnamn du fått av universitetet ska du kontakta universitetets it-stöd. För övriga tjänsters del ska du sända ett meddelande till organisationens abuse-adress (t.ex. abuse@domain) eller ringa organisationens växel och be om att bli förenad till den person som handhar informationssäkerhetsärenden. Berätta tydligt vad du lagt märke till och när det skedde. Uppge också ditt namn och dina kontaktuppgifter så att du vid behov kan kontaktas för närmare information.

NÄRMARE INFORMATION OCH LÄNKAR

- Sidor om informationssäkerhet vid ditt eget universitet
  - » Bekanta dig med säkerhetsanvisningarna vid ditt eget universitet.

- Anvisningar för säker nätanvändning.
  - » http://www.tietoturvaopas.fi/sv

- Information om informationssäkerhetshot och anvisningar för hur man skyddar sig mot dem.
  - » http://www.tietosuoja.fi (även svenska och engelska)

- Nätetikett: God sed vid nätkommunikation.
  - » http://sv.wikipedia.org/wiki/Netikett

- Anvisningar om skydd av kommunikation, meddelanden om hot mot informationssäkerheten.
  - » http://www.cert.fi/sv

- Konsumentverkets anvisningar för att identifiera bedrägeri
  - » http://www.kuluttajavirasto.fi/sv-FI/bedragerier/

- Informationssäkerhetsanvisningar för mobila apparater.
  - » www.fucio.fi/tietoturva/mobilsakerhetsanvisning.pdf

- Högskolornas utvärderingssidor om molntjänster.
  - » http://pilviohje.eduuni.fi (vid tryckläggning endast på finska)

- Upphovsrätt ur lärarens perspektiv
  - » http://www.opettajantekijanoikeus.fi