TEMASERIE FRA IT-AVDELINGEN VED UNIVERSITETET I BERGEN / NUMMER 7 / APRIL 2014

DATASIKKERHET

LEDER

Universitetet i Bergen ønsker å være et åpent universitet. Vi ønsker å dele vår kunnskap, og ha mest mulig fri informasjonsutveksling og dialog. Samtidig må vi ta vare på våre data, og spesielt ivareta personvern og beskytte annen sensitiv informasjon. Vi må sikre våre systemer og vår infrastruktur.

Vi merker det samme som andre, at forsøkene på angrep og infiltrering blir mer avanserte og øker i omfang. Derfor må vi fortsette å bygge sikkerhet rundt våre data, våre systemer og vår infrastruktur. Vår spesielle utfordring blir å opprettholde brukervennlighet og universitetets ønske om åpenhet og frihet.

Gjennom dette syvende nummeret av IT-avdelingens temaserie setter vi fokus på datasikkerhet og gir våre lesere konkrete tips. Ta datasikkerhet på alvor.

Tore Burheim
IT-direktør

DATASIKKERHET

DATASIKKERHET - HVA ER DET?

I dette nummeret av temeserien vil vi si noe om hva datasikkerhet* er og hvilken informasjon som kan trenge ekstra beskyttelse. Vi vil også si noe om hvilke farer som lurer og hvordan IT-avdelingen beskytter mot disse. Ikke minst vil vi hjelpe deg med å få oversikt over hva du kan gjøre selv.

* *Med datasikkerhet mener vi informasjonssikkerhet knyttet til informasjon som er lagret elektronisk. (Kilde:Wikipedia)*

Det er altså så enkelt som å ta vare på elektroniske data. Vi må innrømme at det har noen utfordringer, men med litt kunnskap er det likevel mulig å være rimelig trygg på sine data.

Vi forventer gjerne at informasjonen ligger trygt lagret og får riktig behandling. Men vi vet også at det innimellom kan skje noe vi ikke ønsker. Derfor tar vi noen forholdsregler. I hovedsak handler det om at informasjonen er **korrekt**, at den er **tilgjengelig**, og **hvem** som har tilgang. (Se også ordlister på side 11)

ELEKTRONISK INFORMASJON

Elektronisk informasjon er som annen informasjon, men har noen fordeler og noen ulemper.

Innholdet kan være tekst, bilder, lyd eller video som vi bevisst produserer selv. Noe informasjon kan også registreres automatisk eller av andre personer basert på hva vi gjør eller hvem vi er.

På pc-en lagrer vi selv egne dokumenter. På smarttelefonen lagres gjerne bilder og film fra kameraet automatisk. Dette har vi stort sett kontroll på selv. Når vi bruker bankkort i butikken, busskort på bussen, ringer eller sender meldinger, lagres elektronisk informasjon automatisk. Når vi går til legen eller har møte med banken, blir det mer manuell registrering. Både automatisk og manuelt registrert informasjon vil ofte kunne svare på spørsmålene hvem, hva, hvor og når. Det lagres altså mye informasjon om oss selv som vi har liten kontroll over. De ansvarlige er pålagt å håndtere persondata slik at det ikke kommer i hendene på uvedkommende.

Kontakt- og vennelister gir både detaljer om personene i listene og informasjon om våre kontaktnett. Når vi surfer på nettet, kan informasjon bli liggende igjen i elektroniske logger og informasjonskapsler. Informasjonen kan da ligge både på servere et annet sted i verden, og på din egen enhet. Slik informasjon kan si noe om oss som personer. Oppdatering av kontaktlister og nettsurfing er bevisste handlinger, men vi tenker kanskje ikke over dette som persondata.

Om man setter sammen flere informasjonsbolker, kan det sammen gi ny informasjon. Tenk deg at media forteller om en stor pengepremie vunnet i din nærbutikk, du legger ut bilde av din nye sportsbil på Facebook og kort tid etter laster du opp bilder og restaurantanmeldelser fra Thailand?

Systematisk sammenkobling av store mengder data i stor skala ved hjelp av kraftige datamaskiner kalles gjerne «Big data». Dette kan brukes til nyttige ting som for eksempel å sette inn tiltak rettet mot sannsynlige hendelser i trafikk eller innenfor helsevesenet. Både innenfor forskning, næringsliv og samfunnsstyring er mulighetene mange og i stor grad fortsatt ukjente.

HVA ER VIKTIG Å BESKYTTE?

Filer som vi bruker ofte, som har personlig betydning for oss, eller som det ligger mye arbeid bak, passer vi gjerne på at vi har sikkerhetskopi av. Mye av dette kan være vanskelig eller umulig å gjenskape.

Vi sitter alle med privat informasjon som vi holder for oss selv, eller kun deler med familie eller venner. Likevel er mye informasjon om oss lagret elektronisk. For persondata er det strenge regler for hva som kan lagres, hvor lenge, og hvordan dataene håndteres. Datatilsynet har til oppgave å beskytte enkeltpersoner mot misbruk av persondata. UiB har mye forskningsdata og informasjon om både studenter og ansatte som vi må håndtere slik som personvernloven krever.

Økonomisk informasjon er blitt et mer aktuelt tema innen datasikkerhet, etter som penger i stadig større grad håndteres elektronisk. Det blir stadig flere mulige kilder til økonomisk kriminalitet, rettet både mot enkeltpersoner og bedrifter/organisasjoner.

Mye informasjon om bedrifter, institusjoner og organisasjoner trenger beskyttelse på grunn av konkurransehensyn eller renommé. Lover og regler setter også krav til hvordan slik informasjon håndteres.

Informasjon som direkte eller indirekte handler om sikkerhet kan også være viktig å beskytte. De som ønsker å komme forbi hinderne, har nytte av å vite hvilke hinder de må passere. Et eksempel er når IT-selskaper sender ut sikkerhetsoppdateringer. Om noen med uhederlige hensikter sjekker hva oppdateringen gjør, vet de samtidig hvilket sikkerhetshull det tetter. Dermed kan de starte jakten på enheter som ikke er oppdatert, og som kan bli et enkelt «bytte».

FARE NUMMER 1: TAP AV DATA

Harddisker, minnekort og andre lagringsenheter kan bli ødelagt eller mistes. Smarttelefoner, nettbrett og bærbare pc-er kan også bli frastjålet eller gå tapt på andre måter. Da bør viktige data også være lagret andre steder.

Personlig hjemmeområde og avdelingens fellesområder er trygg lagring. På UiBs tjenermaskiner (servere), blir det automatisk tatt sikkerhetskopi hver natt, slik at det er mulig å gjenopprette tapte filer. UiBs bærbare pc-er satt opp av IT-avdelingen kan synkronisere filer mot hjemmeområde når de er på nett. Lagringsplass for sikkerhetskopi av private data kan kjøpes eller leies for stadig lavere priser.

Les mer på it.uib.no/Backup

FARE NUMMER 2: VIRUS OG TROJANERE

Programvare kan brukes på flere måter til å gjøre skadelige eller uønskede ting. Datavirus er dataprogrammer som er programmert slik at de selv prøver å spre seg til andre maskiner. De kan spre seg raskt og til svært mange maskiner om de ikke blir stoppet. Hva virus gjør utenom å spre seg, varierer mye, fra å slette filer til kun å spre seg videre uten å gjøre noen skade. Virus som ikke fjernes kan også være programmert til å gjøre skade senere.

Antivirusprogramvare har mange regnet som en selvfølge på pc-er med Windows. På datamaskiner med Mac og Linux har det derimot ikke vært like påkrevet. En grunn til dette er at virus er en type programvare, og at samme programvare ikke kan installeres på alle typer maskiner. Siden de fleste pc-er har hatt Windows, har dette kunnet gi størst og raskest spredning. Etter som både Mac og Linux er blitt mer vanlig og stadig flere bruker smarttelefoner og nettbrett, åpner det for at disse plattformene også blir mer effektive som virusspredere.

Ulike varianter av uønsket programvare bruker forskjellige metoder for å spre seg. En «trojansk hest» eller «trojaner» er programvare som i utgangspunktet blir installert frivillig av brukeren av maskinen. Programvaren er derimot programmert til gjøre skade etter at den er sluppet «innenfor murene».

Noe programvare kan være så attraktiv at vi frivillig aksepterer den selv om den også gjør ting vi gjerne kunne vært foruten. Dette kan gå på bekostning av personvernet, men om alternativet er å fjerne hele programvaren, lar vi det kanskje likevel være. >>

En «app» er i prinsippet programvare som tradisjonell pc-programvare. Hovedforskjellen er vanligvis at en app har mer begrenset funksjonalitet og er enklere å legge til og fjerne. Dette gjør at vi på smarttelefoner og nettbrett installerer flere små apper i stedet for større programpakker. En utfordring i forhold til å velge de rette appene er at det er så mange utviklere eller utviklerselskaper som lager dem. Dermed er det vanskeligere å forutse hvilke som er gode og hvilke man bør styre unna. Siden det er så enkelt å fjerne en app igjen, blir også terskelen lav for å teste.

Før du installerer en app, får du kanskje opplyst at appen trenger ulike tilganger. Det kan være tilgang til Internett, SMS, personlige kontakter og å lagre og slette innhold på telefonen. Om slikt misbrukes, kan det koste dyrt på flere måter. Noen apper kan for eksempel misbruke tilliten du gir ved å akseptere tilgang til kontaktlisten. Smarttelefoner og nettbrett har mer funksjonalitet enn tradisjonelle pc-er, og er i stor grad med deg alle steder du er. Dette kan også gi større muligheter for misbruk. Om du er usikker på hvorfor en app trenger tilganger den ber om, er usikker på kvaliteten, eller om du mistenker at den kan misbruke tilliten, så bør du gjerne tenke deg om en gang til. Du kan lese mer hos norsis.no

FARE NUMMER 3: PHISHING

Daglig sendes store mengder e-post som prøver å lure informasjon fra mottakerne. Meldingene blir spredd til svært mange, så kun en liten svarprosent kan være nok til at det lønner seg for de som står bak. Oppgir du informasjon som kan gi andre tilgang til en bankkonto, kan saldo plutselig minke.

Ett hakk mer avansert enn sugerør inn i banken, er passord for pålogging til pc eller lignende. Med kontroll over en pc kan man nemlig få tilgang til tjenester man automatisk får tilgang til ved hjelp av lagrede passord. I tillegg brukes ofte samme passord til pålogging flere steder.

ID-tyveri er etter hvert blitt et kjent begrep. Det kan også bli konsekvensen av å bite på kroken i et phishing-angrep. Noe personlig informasjon kan nemlig brukes av andre som kan gi seg ut for å være deg. Dette kan gi deg økonomiske kostnader og andre skader eller ubehageligheter. Du kan lese mer om hvordan du forebygger, oppdager og bekjemper ID-tyveri på datatilsynet.no.

FARE NUMMER 4: CRACKERE

IT-kompetanse kan brukes til å utvikle gode og sikre IT-systemer. Men tilsvarende kunnskap kan også brukes motsatt av såkalte «crackere» til å prøve å komme forbi sikkerhet. Dette brukes på internasjonalt nivå, både økonomisk og politisk. En mer direkte trussel for folk flest er misbruk for privat økonomisk vinning. For noen kan også personlig spenning, utfordring eller anerkjennelse blant likesinnede være motivasjon for å overvinne sikkerheten i IT-systemer.

Internett er en forutsetning for den raske veksten i bruk av informasjonsteknologi, men gjør det også lettere å utnytte IT-svakheter hos andre. Heldigvis bidrar også Internett til raskt å kunne rette opp i svakheter. Men det er et kappløp mellom de som prøver å utnytte sikkerhetshullene og de som prøver å tette dem. Internett gjør det mulig å spre informasjon raskt og i stor skala, også om hvordan sikkerhetshull kan utnyttes før alle har rukket å tette igjen. Personer med relativt lav IT-kompetanse kan dermed også gjøre stor skade, såkalt «script-kiddies». For eksempel har det vært mulig å finne ferdige virus på Internett som enkelt kan endres for å lage en variant som antivirusprogramvare ikke fanger opp før det har rukket å spre seg. Normalt blir de fleste virus likevel raskt stoppet med oppdatert antivirusprogramvare.

FARE NUMMER 5: DEG OG MEG

Uansett hvor sikkert din pc eller smarttelefon er satt opp, vil du ikke kunne gardere deg hundre prosent. Den svakeste lenken kan nemlig være deg selv. Du kan glemme igjen mobiltelefonen eller miste den ut av lommen i full fart mot bussen eller flyet. Du kan i ubetenksomhet klikke på feil lenke på nettet, som ikke fører der du trodde. Du kan i god tro gi fra deg informasjon som du ikke selv tenkte på at det kan misbrukes. Kanskje installerer du en app du ble tipset om at du bare «må» sjekke.

Menneskelige feil klarer vi ikke gardere oss helt imot. Men det er mulig å forebygge noen av feilene, eller å redusere konsekvensene av dem. Det kan gjøres med faste rutiner og gode vaner, men også ved å tenke oss litt ekstra om og bruke sunn fornuft. Litt forståelse av farene som finnes vil også kunne hjelpe deg til å gjenkjenne og unngå dem.

HVA GJØR IT-AVDELINGEN?

Innenfor alle IT-tjenester må sikkerheten vurderes kontinuerlig. Mye av IT-avdelingens fokus handler om høy nok sikkerhet i forhold til ressursbruk og risikovurdering, samtidig som IT-tjenestene må være tilgjengelige og brukervennlige.

Universitetets ulike datamaskiner må ha sikkert oppsett. Dette gjelder både pc-er som studenter og ansatte bruker, og tjenermaskiner (servere) som gir IT-tjenester som lagring, utskrift, nettsider osv. Nødvendige sikkerhetsoppdateringer fra leverandører må installeres etter hvert. Det er et utall av valg og innstillinger som må balanseres mellom brukervennlighet og sikkerhet. Om sikkerheten er for lav, kan konsekvensene bli store. Pc-er driftet av IT-avdelingen skal få oppdateringer automatisk, om de er på nett regelmessig. På de fleste UiB-pc-er har ikke brukeren rettigheter til å installere programvare, så de fleste virus kan dermed heller ikke installeres. Automatisk oppsett for lagring på server er også en viktig del av sikkerheten på pc-er.

Datanett ved UiB er også IT-avdelingens ansvar. Både trådløst og kablet nett må kunne brukes sikkert uten at andre kan «sniffe» til seg informasjon som blir sendt fra en datamaskin til en annen. En av metodene som bidrar til å sikre data som sendes over nettet er kryptering av data, en slags koding med svært kompliserte nøkler. Det er også viktig at internettforbindelsen ikke kuttes helt om datanettet blir rammet av feil ett sted.

Rutiner og dokumentasjon bidrar til at sikkerhet blir i varetatt i daglig drifts- og utviklingsarbeid, og for å redusere driftsstans. Gode arbeidsvaner kan hjelpe med å forutse mulige feil og raskt gjenopprette tjenester når noe går galt. Med fysiske maskiner og kabler vil det nemlig innimellom forekomme feil. Når IT-avdelingen skal gjøre endringer på systemene, eller nye systemer skal inn, vil det også påvirke andre systemer. Da er rutiner og dokumentasjon uvurderlig.

Administrasjon av brukertilganger er også en viktig sikkerhetsoppgave for IT-avdelingen. IT-tjenester skal være tilgjengelige for alle som skal ha tilgang, og ikke for andre. Tilganger kan gis i de enkelte systemer, via tilleggssystemer eller i datanettet. Det sentrale systemet for brukeradministrasjon er SEBRA (https://sebra.uib.no), som er laget og videreutvikles ved IT-avdelingen. Tilgang til IT-tjenester kan du lese mer om i forrige nummer av IT-avdelingens temaserie. Se it.uib.no/temaserien

Informasjon om hvordan IT-tjenestene bør og ikke bør brukes med tanke på sikkerhet er også viktig. IT-avdelingen lager derfor bruksanvisninger og informasjonskampanjer for å fortelle deg som bruker hvordan du bør eller ikke bør bruke IT-tjenestene, og hva du må tenke ekstra på. IT-avdelingen prøver å gjøre sikkerhet lettere for deg ved å sørge for grunnleggende sikkerhet, slik at du i større grad kan fokusere på det du egentlig skal gjøre. Men en del av sikkerhetsansvaret ligger også på deg som bruker.

HVA BØR DU GJØRE SELV?

De fleste anbefalinger her gjelder for alle typer datamaskiner, inkludert smarttelefoner og nettbrett.

OPPSETT OG PROGRAMVARE

- Bruk sikkerhetsprogramvare som finner virus og annen uønsket programvare. IT-avdelingen tar seg av dette på de aller fleste av UiBs pc-er, såkalte «klientdriftede maskiner».
- Pass på at anbefalte sikkerhetsoppdateringer blir installert. Dette gjelder både for operativsystem (Windows, Mac OS X, iOS, Android og andre Linux) og programvare (apper, Java, Flash, Adobe Reader, osv.).
- Bruk administratorrettigheter bare når du trenger det.
- Installer bare apper eller annen programvare du er trygg på. Fjern programvare du ikke bruker eller trenger.
- Pass på at nettverket du bruker hjemme er sikkert satt opp. UiB har VPN som også kan brukes hjemmefra.
- Brannmur følger med i Windows, Linux og Mac, og bør være slått på. Standardoppsett stopper en del av de vanligste truslene.

UNNGÅ TAP AV DATA

- Sørg for at du har sikkerhetskopi av data du ikke vil miste. Se også it.uib.no/Backup
- Lagre på hjemmeområde eller fellesområde når du bruker pc-er driftet av IT-avdelingen og er på universitetet.
- Sørg for sikkerhetskopi eller kopi på hjemmeområde når du er utenfor UiB-nett eller på mobil enhet eller privat pc.

PASSORD

Tilgang til IT-tjenester og utstyr må sikres godt både privat og på UiB. Se også it.uib.no/Passord

- Ikke gi dine passord til noen andre. Bytt passord som andre kan ha fått tilgang til.
- Lag gode passord: minimum ti tegn som du husker, men ikke andre kan gjette.
- Bruk automatisk skjermlås som krever passord eller annen sikker autentisering. Dette gjelder både på pc, nettbrett og smarttelefon.
- Bruk ulike passord til ulike tjenester (forandre i hvert fall noe). Brukernavn og passord fra UiB skal bare brukes til pålogging der UiB krever det.

NETTSIDER

Anbefalinger for Internett gjelder både for privat og UiBs utstyr.

- Ikke klikk på lenker i e-post eller andre meldinger du får tilsendt. Skriv inn nettadressen i stedet.
- For nettsider som krever pålogging, sjekk at nettadresser begynner med https og ikke bare http. S-en står for secure/sikker.
- Er du i tvil om du er på riktig nettside, sjekk spesielt at domenenavnet i nettadressen er korrekt. Husk at UiB-domenet heter uib.no.

MOBILE ENHETER

Smarttelefoner, nettbrett og til dels bærbare pc-er har noen ekstra utfordringer.
Merk at de andre anbefalingene også gjelder for disse. Se it.uib.no/Mobil_trygghet

Mer om hva du kan gjøre selv finner du på it.uib.no/IT-sikkerhet

SJEKKLISTE

- ✓ Er dine viktige data trygt lagret for deg, og beskyttet mot uvedkommende?
- ✓ Har du trygt oppsett på smarttelefon/nettbrett, privat pc og hjemmenett?
- ✓ Har du sikkerhetsprogramvare?
- ✓ Får IT-utstyr du bruker nødvendige sikkerhetsoppdateringer?
- ✓ Har du god passordbeskyttelse?
- ✓ Tenker du deg om før du klikker?
- ✓ Vet du hva du bør passe på alle steder du er på nett?

OFTE STILTE SPØRSMÅL

Hvordan får jeg tak i antivirus til privat maskin?

Det finnes flere gode antivirusprogrammer gratis tilgjengelig på nett. Søk litt på nett for å sikre at du velger programvare som er fra en seriøs utvikler og er testet at den faktisk finner virus som er i omløp. Det finnes også falske antivirusprogrammer, som kan gjøre skade heller enn nytte.

Jeg tror jeg har fått virus. Hva gjør jeg?

Antivirusprogramvaren skal kunne kjøre en manuell sjekk, og trolig kunne fjerne ondsinnet programvare. For sikkerhets skyld anbefaler vi en reinstallasjon av operativsystem og programvare, da viruset for eksempel kan ha endret på oppsettet. Gjelder det en UiB-maskin, kontakt brukerstøtte. Er det en privat maskin, koble maskinen først fra Internett, og pass på at du tar vare på filene du skal ha. Etter reinstallasjon bør antivirus være første program du legger til etter at operativsystemet er installert. Maskiner på UiB som sprer virus, vil raskt kunne bli stengt ute fra nettet.

Er denne e-posten svindel?

De fleste svindelmail har noe mistenkelig ved seg. Virker det for godt til å være sant, er det som regel også det. Om du blir bedt om å gi fra deg personlig informasjon, spesielt bankinformasjon eller passord, så styr unna. Svindelmail bærer ofte preg av dårlig oversetting og har lenker eller ber deg svare på e-posten. Er du i tvil, så ikke klikk på lenkene og ikke svar på e-posten. Du kan også sjekke hvor lenken peker ved å holde musepereren over. Tror du at en e-post er svindelforsøk, kan du videresende den direkte til postnuke@uib.no. >>

Jeg mistenker at noen har fått tilgang til bank- eller påloggingsinformasjon. Hva gjør jeg?

Har andre fått tilgang til ditt UiB-passord, bør du snarest bytte passord på sebra.uib.no. Vurder også om du må bytte passord andre steder. Din bank har informasjon om hva du gjør om du mistenker at bankinformasjon er kommet på avveie.

Kan jeg bruke Windows XP hjemme etter 8. april 2014?

Microsoft har bestemt at etter 8. april 2014 vil de ikke lenger lage sikkerhetsoppdateringer for Windows XP. Dette har vært et mye brukt operativsystem gjennom mange år, så «crackerne» kjenner det godt. Det er derfor ganske sikkert at noen har prøvd målrettet å finne sikkerhetshull som de kan utnytte etter 8. april. Andre programvareleverandører vil nok også slutte å levere oppdateringer til programmer som brukes på Windows XP. Siden du før eller siden må bytte uansett, bør du gjøre det før 8. april, og ikke vente til etterpå. Får du ikke installert et sikkert operativsystem før fristen, bør maskinen tas av nett. Andre operativsystemer uten sikkerhetsoppdateringer bør heller ikke brukes på nett.

OM DU TRENGER HJELP

Brukerstøtteportalen IT-hjelp inneholder en del informasjon om datasikkerhet på nettadressen it.uib.no

Studenter og ansatte kan sende en henvendelse i bs.uib.no

Ansatte kan ringe BRITA på (555) 84700.

Studenter kan også spørre en IT-assistent (tidligere kjent som pc-vakt), som videresender til IT-avdelingen ved behov.

MER OM DATASIKKERHET

it.uib.no/IT-sikkerhet – fra UiB IT-avdelingen

norsis.no – Norsk senter for informasjonssikring

nettvett.no – fra Post- og teletilsynet

datatilsynet.no – statlig personvernmyndighet

securingthehuman.org/ouch – nyhetsbrev oversatt til mange språk

ORDLISTE

HVA ER DATASIKKERHET

informasjonssikkerhet	å sikre at informasjon er sikker med hensyn til konfidensialitet, integritet og tilgjengelighet
datasikkerhet	informasjonssikkerhet knyttet til informasjon som er lagret elektronisk
konfidensialitet	å sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som skal ha tilgang
integritet	å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige
tilgjengelighet	å sikre at informasjon og informasjonssystemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt.

NOEN TRUSLER

hacker	person med god (IT- eller teknisk) kompetanse som søker å finne sikkerhetsmessige svakheter; dette kan brukes til å utbedre eller utnytte svakhetene (se også cracker, sosial hacking)
cracker	hacker som misbruker sin (IT- eller tekniske) kompetanse til å gjøre skade eller skaffe urettmessig tilgang
script-kiddie	person med moderat IT-kompetanse som bruker ferdiglagde programmer eller oppskrifter til å utnytte IT-sårbarheter
datavirus	programkode som sprer seg selv til andre maskiner via datanettverk
orm	en type virus som sprer seg selv uten hjelp av andre programmer
trojaner	uønsket programkode innbakt i apper eller andre dataprogrammer man installerer frivillig
spionprogramvare	programvare som stjeler informasjon, typisk persondata, bankopplysninger og passord
hoax	falsk rykte om virus eller annen trussel; kan ved å skremme folk lure dem til å installere falske antivirusprogrammer o.l.
spam	uønsket masseutsendt e-post eller andre meldinger, ofte bare irriterende og ikke direkte skadelig
phishing	forsøk på å fralure folk informasjon som kan misbrukes, typisk passord eller bankkontoinformasjon (kan være masseutsendt eller målrettet)
id-tyveri	å utgi seg for å være en spesifikk annen person ved hjelp av denne personens identitetsinformasjon
sosial hacking	å lure mennesker til å gi fra seg informasjon eller tilganger, ofte ved å gi seg ut for å være noen man ikke er, og ofte målrettet mot utvalgte enkeltpersoner; kan misbrukes til å skaffe seg urettmessige tilganger. (se også hacker, cracker)

VERKTØY OG TEKNOLOGI SOM KAN HJELPE DEG

antivirusprogramvare	programvare laget for å gjenkjenne og fortrinnsvis uskadeliggjøre datavirus (har ofte også andre sikkerhetsfunksjoner)
brannmur	programvare eller fysisk maskin som kun slipper gjennom godkjent datatrafikk
kryptering	koding for å gjøre informasjon uforståelig for de som ikke kjenner krypteringsnøkkelen
vpn - virtuelt privat datanettverk	teknologi for å hindre at andre kan få tilgang til data sendt mellom to punkter i et nettverk
eduroam	sikkert trådløst datanett som gir tilgang for brukere fra et stort antall samarbeidsinstitusjoner i verden; anbefalt trådløstnett ved UiB

DATASIKKERHET

Grafisk utforming: Kommunikasjonsavdelingen, UiB
Foto og illustrasjoner: Colourbox / Istockphoto

TIDLIGERE NUMMER:

TILGANG TIL IT-TJENESTER
PROGRAMVARE
UTSKRIFTSTJENESTER
PC VED UiB
E-POST VED UiB
LAGRING OG BACKUP

it.uib.no/Temaserien

Adresse: Postboks 7800, 5020 Bergen
Besøksadresse: Nygårdsgaten 5
Telefon: (+47) 55 58 47 00 Faks: 55 58 40 70
Kontakt: post@it.uib.no
Ansvarlig redaktør: IT-direktøren
http://it.uib.no