

TIETOKONEEN MONET VIHOLLISET

Tietokoneesi toimintaa ja hyvinvointia uhkaavat monet vaarat. Järjestelmä voi mennä jumiin ilman näkyvää syytä, virukset tekevät ilkeää ohjelmille ja hakkerit kaivelevat tietoja kovalevyiltäsi. Onneksi on olemassa keinot tietokoneen turvaksi.

Vaikka sinun ei olisi tähän mennessä koskaan tarvinnut miettiä tietosuojan kaltaisia tylsiä asioita, ei kannata luottaa hyvän tuurin jatkumiseen. Luottamus kohtaloon kostautuu viimeistään sitten, kun huomaat menettäneesi 200-sivuisen asiakirjan, jota olet kirjoittanut puoli vuotta. Tai kun virus sekoittaa kovalevysi, ja huoltoliike laskuttaa sen puhdistamisesta toista tuhatta markkaa.

Uhkaavat katastrofit voidaan kuitenkin torjua oikeilla aseilla. Turvajärjestelmän asentamiseen voi mennä pari tuntia, mutta se vaiva kannattaa nähdä.

Tietoturvan kannalta ensisijainen työkalu on varmuuskopiointi. Se voi kuulostaa selvältä asialta, mutta ylivoimaisesti yleisin tietoturvaongelma on se, että uusi asiakirja talletetaan vanhan päälle. Siksi säännöllisen varmuuskopioiden ottamisen pitäisi olla erottamaton osa työskentelyä, jotta tuntien tai jopa päivien työ ei mene kokonaan hukkaan.

Paras ratkaisu on tietysti ottaa silloin tällöin varmuuskopio koko kovalevyn sisällöstä ohjelmineen kaikkineen. Tällöin voit siirtää tiedostosi uudelle koneelle, jos vaikka murto-

ras sattuisi viemään mennessään koko tietokoneen.

Täydellinen varmuuskopiointi vaatii kuitenkin erityislaitteita. Uudenkaisten tietokoneiden kovalevyt ovat nimittäin niin suuria, että niiden sisältämä tietomäärä täyttää helposti jopa 400-500 levykettä. Jos kovalevyllä on arvokkaita tietoja, kannattaakin harkita erillisen nauha-aseman hankkimista, vaikka se vaatisikin tuhannen markan investointia.

Viruksilta suojaaminen käy helposti

Vaikka varmuuskopiointi olisi kuinka aukoton ja ajan tasalla, ajatus viikonlopun tarväämisestä tietokoneen palauttamiseen entiselleen tuskin houkuttelee. Siksi kannattaa minimoida kaikki tietoturvariskit.

Virukset ovat uhka, jota vastaan on helppo suojautua. Tietokoneesi voi saada virustartunnan levykkeiden, CD-romien, siirrettävien levy- tai nauha-asemien tai Internetistä nouta-

miesi tiedostojen kautta. Tartunta voidaan kuitenkin välttää melko hyvin viruksentorjuntaohjelman avulla. Viruksia syntyy tietysti koko ajan lisää, mutta päivittämällä virussuojan tarpeeksi usein vältät tartunnan suurella todennäköisyydellä.

Tietoturvariski, jota ei pidä väheksyä, ovat itse tietokoneen käyttäjät. Hyvää tarkoittavat ihmiset voivat helposti saada aikaan hyvinkin suuren vahingon muuttaessaan järjestelmän asetuksia esimerkiksi tietokoneohjelmien asennuksen yhteydessä.

Jos haluat estää muita käyttäjiä sotkemasta konettasi, voit estää muita käyttämästä konettasi esimerkiksi salasanan avulla. Voit myös suojata asiakirjasi asiattomien henkilöiden uteliailta katseilta.

Paras neuvomme kuuluukin, varaudu pahimpaan: se kannattaa ja on helpompaa kuin luuletkaan. ■



Tehokkain tietokone on täysin turvaton ilman omistajansa apua. Sen uhkana ovat selittämättömät ohjelmistoviat, virukset ja tumpelot käyttäjät.

SUOJAA KONEESI VIRUKSIA VASTAAN

Tietokonevirukset leviävät vain lähikontaktissa, kuten flussaviruksetkin. Koneesi voi saada tartunnan, kun käytät muilta tulleita tiedostoja tai ohjelmia.

Kaikki virukset eivät ole yhtä vaarallisia. Itse asiassa totaalista tuhoa kylväviä tietokoneviruksia on hyvin vähän. Useimmat aiheuttavat vain suhteellisen pientä kiusaa. Ne voivat estää

ohjelmia suorittamasta tiettyjä toimintoja, tuoda näytölle yllättäen outoja kuvia tai panna tietokoneesi äännelemaan tietyissä tilanteissa. Ne ovat kuitenkin kiusanhenkiä, joita vastaan kannattaa suojautua ennen kuin ne sekoittavat koneesi.

Nykyään tunnetaan n. 10 000 tietokonevirusta, ja uusia ilmestyy jatkuvasti. Tietokonevirus on pieni ohjelmätiedosto, joka kätkeytyy tavallisten tiedostojen sisään. Nämä tiedostot toimivat taudinkantajina, joista virusohjelma siirtyy muihin tiedostoihin, kun se niin päättää.

Onneksi virustartunnalta on helppo suojautua viruksentorjuntaohjelman avulla. Virussuoja tarkistaa kovalevyllä tai levykkeellä olevat tiedostot ja poistaa löytämänsä

virukset. Ohjelma voidaan myös säätää tarkistamaan automaattisesti kaikki koneeseen tulevat tiedostot, ennen kuin ne talletetaan kovalevyllä.

Jokaisen *Kompuuteri Kaikille* -lehden mukana tulee McAfee VirusScan -ohjelma, joka on suunniteltu pitämään silmällä kaikkia mahdollisia viruksia. Se ei kuitenkaan tunnista sellaisia virustyyppisiä, jotka on kehitetty ohjelman valmistumisen jälkeen. McAfee tunnistaa silti useimmat virukset ja estää niitä tartuttamasta tietokonettasi.

Markkinoilla on muitakin tehokkaita viruksentorjuntaohjelmia, mutta mikään niistä ei voi taata 100-prosenttista suojaa. Eri puolilla maailmaa on ilkiöitä, joiden huvina on keksiä uusia tapoja sabotoida muiden ihmisten koneita. Virusnikkarit ovat aina muutaman askeleen edellä niitä, jotka kehittävät torjuntakeinoja viruksia vastaan. Paras taikin hankkia viruksentorjuntaohjelmista aina uusin versio. Näin olet turvassa ainakin tunnetuimmilta taudinaiheuttajilta.

KOHTALOKAS KOSKETUS

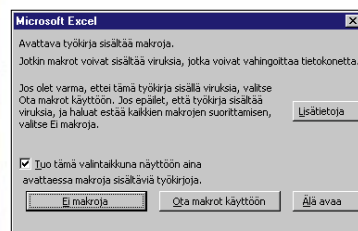
Virustartunnan vaara on olemassa aina, kun tietokoneesi on yhteydessä toiseen koneeseen.

VIRUS VOI TARTTUA, KUN...

- avaat koneellasi dokumentteja, jotka on tehty jossain toisessa tietokoneessa
- käytät muissa koneissa käytettyjä ohjelmia, esimerkiksi laittomia ohjelmakopioita tai shareware-ohjelmia
- koneesi on liitetty lähiverkkoon (varsinkin, jos verkossa ei ole virussuojaa)
- lataat kovalevylläsi ohjelmia tai muita tiedostoja Internetistä.

VIRUS EI TARTU, KUN...

- surfaat Internetissä tai lähetat tai vastaanotat sähköpostia (liitetiedostoissa voi kuitenkin olla viruksia)
- käytät alkuperäislevykeillä asennettuja ohjelmia.



OTA VAROITUKSET TODESTA

Jotkin ohjelmat varoittavat virustartunnan mahdollisuudesta, kun olet suorittamassa tiettyjä toimintoja. Jos toiminto on kuitenkin välttämätön, tarkista dokumentti ensin viruksentorjuntaohjelmalla.

LEVYKKEET JA MAKROT SUURIN VAARA

LEVYKKEET

Ylivoimaisesti suurin osa viruksista leviää levykkeiden mukana. Monet levykkeillä leviävistä kehitetyt virukset tarttuvat koneeseesi, jos levyke on asemassa, kun kone käynnistetään. Tietokone on nimittäin asetettu suorittamaan ensimmäisenä ne komennot, jotka se löytää levykeasemassa olevalta levykkeeltä, vaikka komento olisi esimerkiksi kovalevyn tyhjentäminen. Pidä siis levyke asemassa vain silloin, kun todella käytät sitä.

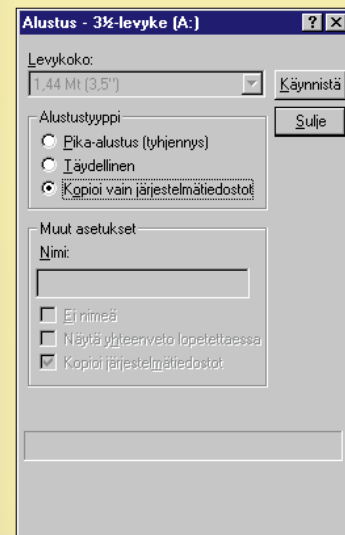
MAKROVIRUKSET

Uusi lisä tietokonevirusten kirjajaan joukkoon ovat ns. makrovirukset. Makro on pieni ohjelma, joka käynnistyy tietyllä näppäinyhdistelmällä. Esimerkiksi tekstinkäsittelyohjelman Etsi- tai Kopioi-toiminnot ovat makroja. Makrovirus toimii samalla tavoin, mutta se voi käskä järjestelmää esimerkiksi poistamaan joitain toimintoja tai estää dokumentin tallentamisen. Paras varokeino on kytkeä ohjelman makrotoiminto pois päältä tai tarkistaa kaikki dokumentit ennen käyttöä.



MCAFEEN ASENNUS HOITUU PUOLESSA TUNNISSA

Tämän kuun K-rompulla saat tehokkaan McAfee-viruksentorjuntaohjelman. Sen asentaminen on helppoa.



1 TEE KÄYNNISTYSLEVYKE

Tee ensiksi käynnistyslevyke. Ohjelma tarvitsee sitä myöhemmin. Pane levykeasemaan levyke. Kaksoisnapsauta Oma tietokone -kuvaketta. Napsauta levykekuva-ketta ja valitse Tiedosto-valikosta Alustus. Valitse Kopioi vain järjestelmätiedostot ja napsauta painiketta Käynnistä.

2 ALOITA ASENNUS

Käynnistä K-romppu ja valitse aloitusvalikosta Aarrearkku. Valitse McAfee ja napsauta Asenna-painiketta. Seuraa näytön ohjeita. Kun ohjelma kysyy asennustapaa, valitse Typical, jota ohjelma ehdottaa. Vastaa kyllä, kun ohjelma kysyy, käynnistetäänkö koneesi.

3 KÄYNNISTÄ TIETOKONE

Ennen kuin käynnistät tietokoneen uudestaan, työnnä käynnistyslevyksen kirjoitus-suojatapin paikalleen. Nyt levykkeeseen ei voi tarttua viruksia. Säilytä käynnistyslevyke varmassa paikassa. Levykettä tarvitaan tietokoneesi käynnistämiseen, jos tietokoneesi järjestelmä menee sekaisin ja kieltäytyy käynnistymästä uudelleen.

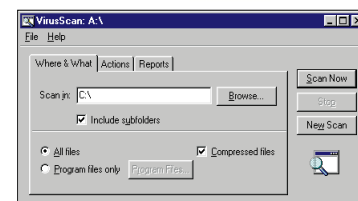


Kun käynnistät viruksentorjuntaohjelman ensimmäisen kerran, se saattaa löytää kovalevyllä viruksen, vaikka koneesi toimii aivan normaalisti. Virus on voinut piileskellä koneessasi hyvinkin pitkän aikaa, joten sen alkuperän selvittäminen voi olla vaikeaa.

MCAFEEN HIENOSÄÄTÖ

McAfee on valmiiksi säädetty niin, että se etsii automaattisesti koko ajan viruksia ja tarkistaa kaikki uudet tiedostot. Jos et muuta perusasetuksia, voit unohtaa koko ohjelman asennuksen jälkeen. McAfee käynnistyy automaattisesti, kun käynnistät Windowsin, ja kertoo, jos jokin on vialla. Tämä ns. taustasuojaus kuitenkin hieman hidastaa tietokoneen toimintaa, koska se vie osan suorittimen tehosta.

Jos haluat käyttää tietokonetta täydellä teholla, voit ottaa taustasuojauksen pois päältä. Tällöin sinun pitää itse tarkistaa kaikki epäilyttävät tiedostot. Käytännössä sinun tulee muistaa tarkistaa kovalevy aina, kun tietokoneesi on ollut yhteydessä vierasiin tiedostoihin. Pääset muuttamaan McAfeen asetuksia valitsemalla Käynnistä-valikon alavalikosta ohjelman McAfee.



LEVYJEN TARKISTUS MANUAALISESTI

Jos saat vieraan CD-romin tai levykkeen tai tietokoneesi käyttäytyä merkittävästi, voi olla hyvä idea tarkistaa epäilyttävä levyke tai koko kovalevy. Valitse Virus Scan ja tarkistettava levyasema. Tarkista, että vaihtoehdot All files on valittuna. Käynnistä ohjelma napsauttamalla painiketta Scan now.

TAUSTA-SUOJAUKSEN ASETUKSET

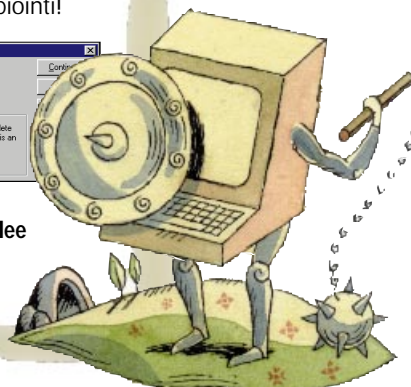
Automaattinen taustasuojaus kytetään päälle ja pois päältä kohdassa Virus Scan Console. Kaksoisnapsauta sinistä palkkia, jonka vasemmalla puolella on kilpi. Taustasuojaus kytetään päälle kohdassa Enable ja pois päältä kohdassa Disable.



JOS VIRUS ISKEE...

Jos McAfee löytää viruksen, ei ole silti mitään syytä paniikkiin. Useimmiten virus ei ole ehtinyt tehdä pahojaan ja se saadaan poistettua, kun seuraat näytölle tulevia ohjeita. Jos ohjelma ei tunnista virusta, hanki ohjelmasta uusin versio ja katso, tuntee se viruksen. Jos sekään ei auta, tuhoa tartunnan saaneet tiedostot. Kaikkein pahimmassa tapauksessa joudut alustamaan koko kovalevyn uudestaan. Eli: muista varmuuskopiointi!

Kun McAfee löytää viruksen, näytölle tulee ohjeita siitä, miten tulee toimia.



TEE KUNNON VARMUUSKOPIOT PAHIMMAN VARALLE

Varmuuskopionnissa on kyse hermoista eli mitkä tiedostot viitsit kopioida. Useimmat tyytyvät kopioimaan vain tärkeimmät tiedot. Jos koko kone rikkoontuu, korjaaminen on kuitenkin sitä helpompaa, mitä laajemmat varmuuskopiot on käytettävissä.

Varmuuskopionnissa on kyse hermoista eli mitkä tiedostot viitsit kopioida. Useimmat tyytyvät kopioimaan vain tärkeimmät tiedot. Jos koko kone rikkoontuu, korjaaminen on kuitenkin sitä helpompaa, mitä laajemmat varmuuskopiot on käytettävissä.

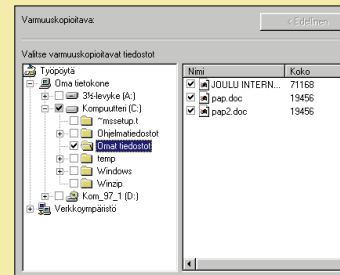
Jos käytät tietokonettasi paljon ja asennat usein uusia ohjelmia, kannattaa ehkä hankkia laitteet, joilla voit ottaa varmuuskopion kaikista tiedostoista. Yksi hyvä vaihtoehto on nauha-asema. Sillä voidaan kopioida koko kovalevyn sisältö kasetille ja tarvittaessa palauttaa tiedostot kasetilta, jos kovalevy vaurioituu. Kannattaa ottaa varmuuskopio koko kovalevystä heti, kun tietokoneeseen on asennettu ohjelmat.

Jos asennat usein ohjelmia koneellesi, kovalevyn varmuuskopio kannattaa päivittää aina, kun tuntuu, että ohjelmien asentaminen uudelleen alkuperäisen "puhtaan" varmuuskopion päälle olisi liian työlästä. Koko kova-

levyn varmuuskopioiminen ei ehkä ole tarpeen, jos olet hankkinut kaikki ohjelmat CD-romeilla. Niiltä uudelleen asentaminen sujuu melko nopeasti. Jos olet muuttanut ohjelmien asetuksia asennuksen jälkeen, kaikkien ohjelmien palauttaminen entiselleen voi kuitenkin olla turhan vaivalloista.

Melko harvoilla on laitteet, joilla koko kovalevy voidaan helposti kopioitua. Useimmat tyytyvät tallentamaan levykkeille tärkeimmät tiedot, kuten omat asiakirjapohjat, osoitehakemistot, ja järjestelmä-

Tärkeät tiedostot samaan kansioon Helpoin tapa pysyä perillä siitä, mistä tiedostoista pitää ottaa varmuuskopiot, on sijoittaa kaikki tärkeät tiedostot samaan kansioon tai hakemistoon. Esimerkiksi Microsoft Office -ohjelmisto luo kovalevyllesi kansion Omat tiedostot (englanniksi My Documents). Kannattaa ottaa tavaksi tallettaa kaikki säilyttämisen arvoiset tiedostot sinne.



Varmuuskopiointi on helpompi hallita, kun kaikki tärkeät tiedot ovat samassa kansiossa.

Varmuuskopiointipäivät on hyvä merkitä kalenteriin. Varsinaisten varmuuskopiointipäivien välilläkin on hyvä pelata varman päälle. Aina kun on saanut valmiiksi suurehkon työn, siitä kannattaa ottaa kopio. Tätä varten ei tarvitse ajaa erillistä varmuuskopiointiohjelmia. Sama asia hoituu tallettamalla dokumentti sekä kovalevylle että levykkeelle. Levykkeen voi ottaa uuteen käyttöön, kun dokumentti on kopioitu seuraavan laajan varmuuskopioinnin yhteydessä.

Joskus Windows 95:ssä varmuuskopiointitoiminto on asennettava erikseen. Se tapahtuu Ohjauspaneelin kohdassa Lisää/poista sovellus.

ASEET TIETOJEN SUOJAAMISEKSI

BIOS-SALASANA: Salasana, jota ilman tietokone ei käynnisty lainkaan. Salasanan hakkerointi vaatii järeät työkalut.

CITADEL SAFSTOR: Tämän lehden mukana saamallasi K-rompulla oleva ohjelma, jolla voit luoda tärkeille tiedostoille tiedostokoh- taiset salasana. Salasanat perustuvat matemaattisiin kaavoihin, joiden avaaminen on käytännöllisesti katsoen mahdotonta.

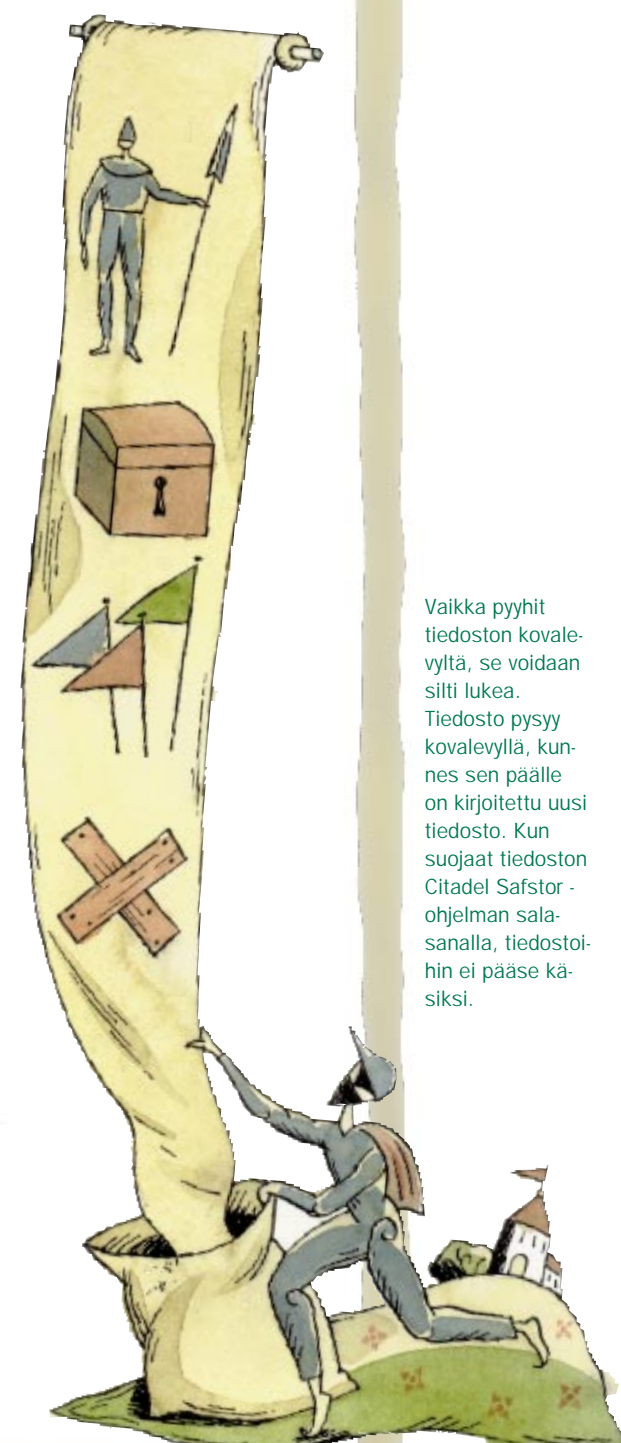
WINDOWS 95:N SALASANA: Windows 95:ssä eri käyttäjille voidaan luoda omat salasanat niin, että kaikki käyttäjät eivät voi käyttää kaikkia tietoja. Pienellä sinnikkyydellä hakkeri pääsee kyllä käsiksi haluamiinsa tietoihin.

NÄYTÖNSÄÄSTÄJÄ: Myös tietokoneen näytönsäästäjään voidaan liittää salasana, joka pitää näytön sisällön piilossa ulkopuolisilta. Tämä toiminto voidaan liittää kaikkiin Windows 95:n mukana tuleviin näytönsäästäjiin. Aukoton tämäkään suojaus ei kuitenkaan ole.

LUKKO: Joissakin tietokoneissa on lukkolaitteisto, joka mahdollistaa koneen käytön vain oikean avaimen haltijalle. Täyttä tietoturvaa lukko ei anna.

NÄPPÄIMISTÖ: Kotioloissa tärkeiden tietojen säilymisen ennallaan voi varmistaa helpoimmin irrottamalla koneesta jonkin osan. Kun näppäimistö puuttuu, lapset eivät pääse sotkemaan tiedostoja.

LEVYKKEET: Jos jotkin tiedostot ovat erityisen tärkeitä, ne kannattaa säilyttää vain levykkeillä ja pyyhkiä pois kovalevyltä. Ennen kuin poistat tiedostot levyltä, suoja ne Citadel Safstor -ohjelmalla.



Vaikka pyyhki tiedoston kovalevyltä, se voidaan silti lukea. Tiedosto pysyy kovalevyllä, kunnes sen päälle on kirjoitettu uusi tiedosto. Kun suojaat tiedoston Citadel Safstor -ohjelman salasanalla, tiedostoihin ei pääse käsiksi.

LAITTEET PIKAKOPIOINTIIN

Varmuuskopiointilaitteen valinta riippuu hinnasta ja tarpeista.

Varmuuskopiointilaitteiden valikoima on niin laaja, että oikean vaihtoehdon löytäminen voi olla vaikeaa. Halvin vaihtoehto on nauha-asema. Kannattaa ehkä kuitenkin hankkia laite, jolla on muitakin käyttömahdollisuuksia kuin varmuuskopiointi.

NAUHA-ASEMA on kätevä tapa kopioida suuria määriä tietoja. Nauha-asema maksaa yleensä noin tuhat markkaa, ja itse nauhat pari sataa markkaa kappale. Yhdelle nauhalle mahtuu 2-3 gigatavua dataa eli parinkin normaalinkokoisen kovalevyn sisältö.

ULKIOINEN KOVALEVY on nopea varmuuskopioituväline, joka on helppo liittää tietokoneeseen. Kapasiteettia ulkoisilla kovalevyillä on 2-4 gigatavua, mikä riittää useimpien tarpeisiin. Hinta tosin voi olla ongelma: noin 4000 markkaa. Se voi monille olla turhan paljon.

CD-ASEMA Nykyisin on saatavilla alle 3 000 markalla kirjoittavia cd-asemia, joilla voit tallentaa tietoja cd-levyille. Lisäksi asema toimii aivan tavallisen cd-rom-aseman tavoin. Muutaman kymmen hintaisille cd-levyille mahtuu 650 megatavua dataa eli monin-kertainen määrä levykkeeseen verrattuna.

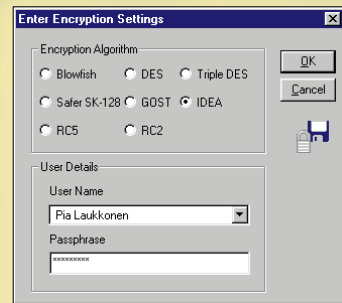
OMA KOVALEVY on halvin ja helpoin varmuuskopiointiväline. Voit pyyhittää tietyn osan levystä varmuuskopiolle ja tallettaa tärkeiden tiedostojen kopiot sinne. Tämä ratkaisu ei suoja tiedostojasi kovalevyn rikkoutumiselta tai viruksilta, jotka tartuttavat levyyn.

ZIP-ASEMA on kohtuuhintainen vaihtoehto, jos sinua ei häiritse se, että koko kovalevyn varmuuskopiointiin tarvitaan yli kymmenen 100 megatavun zip-levyettä. Zip-asemat maksavat hie- man alle 1000 markkaa ja levyt noin 90 markkaa kappale. Jos kovalevysi on suuri, zip-asema voi olla kallis ratkaisu.

YLIMÄÄRÄINEN KOVALEVY on melko edullinen. Reilulla tonnilla saat 2-3 gigatavun kovalevyn, joka asennetaan koneeseen ja liitetään vanhaan kovalevyyn. Ratkaisu suo- jaa tietojen menetykseltä levyn rik- koutuessa, mutta virukset voivat silti tartuttaa kaikki koneen levyt.



Kuva: Ole Raffel



Kuukauden K-rompulla olevalla Citadel Safstor -ohjelmalla voit suojata tiedostosi salasanalla.

SUOJAA TÄRKEÄT TIEDOT TUMPELOILTA

Jos pc:llä on monta käyttäjää, tietyt tiedot kannattaa suojata varmuuden vuoksi.

Vaikka sinulla ei olisikaan koneellasi mitään erityisen salaista tai arkaluontoista tietoa, kaikkien tiedostojen ei silti välttämättä tarvitse olla kaikkien käytettävissä. Erehdyksessä tehdyt pienetkin muutokset esimerkiksi käyttöjärjestelmän tai ohjelmien asetuksissa voivat helposti saada aikaan häiriöitä koneen toiminnassa. Tehokas ja helppo tapa estää "inhimillisistä erehdyksistä" johtuvat häiriöt on pitää asiattomat erossa tärkeistä tiedoista suojaamalla ne salasanalla. Windows 95:ssä on mahdollista luoda eritasoisia käyttöoikeuksia eri käyttäjille. Se on kuitenkin mutkikasta eikä aina täysin turvallista.

Kuukauden K-rompulla on ohjelma nimeltä Citadel Safstor, joka lukitsee tiedostot monimutkaisen matemaattisen kaavan avulla. Tiedostoja pääsee lukemaan vain salasanan tunteva käyttäjä.

BIOS-SALASANA PARAS SUOJA

Useimmissa tietokoneissa salasana voidaan asettaa ns. BIOS-piiriin. BIOS on MS-DOS-käyttöjärjestelmän osa, jonka tehtävänä on sovittaa yhteen

ohjelmat ja tietokoneen eri osat, kuten levyasemat, näppäimistö ja kirjoitin. BIOS ylläpitää kelloaika- ja päivämäärätietoja sekä perustietoja, joita ilman tietokoneen

käynnistäminen ei onnistu. BIOSin suojaaminen salasanalla estää pääsyn kaikkiin tietokoneen tietoihin. BIOS-salasanan luominen on paras antaa ammattihenkilön tehtäväksi, vaikka se on vain muutaman minuutin homma.