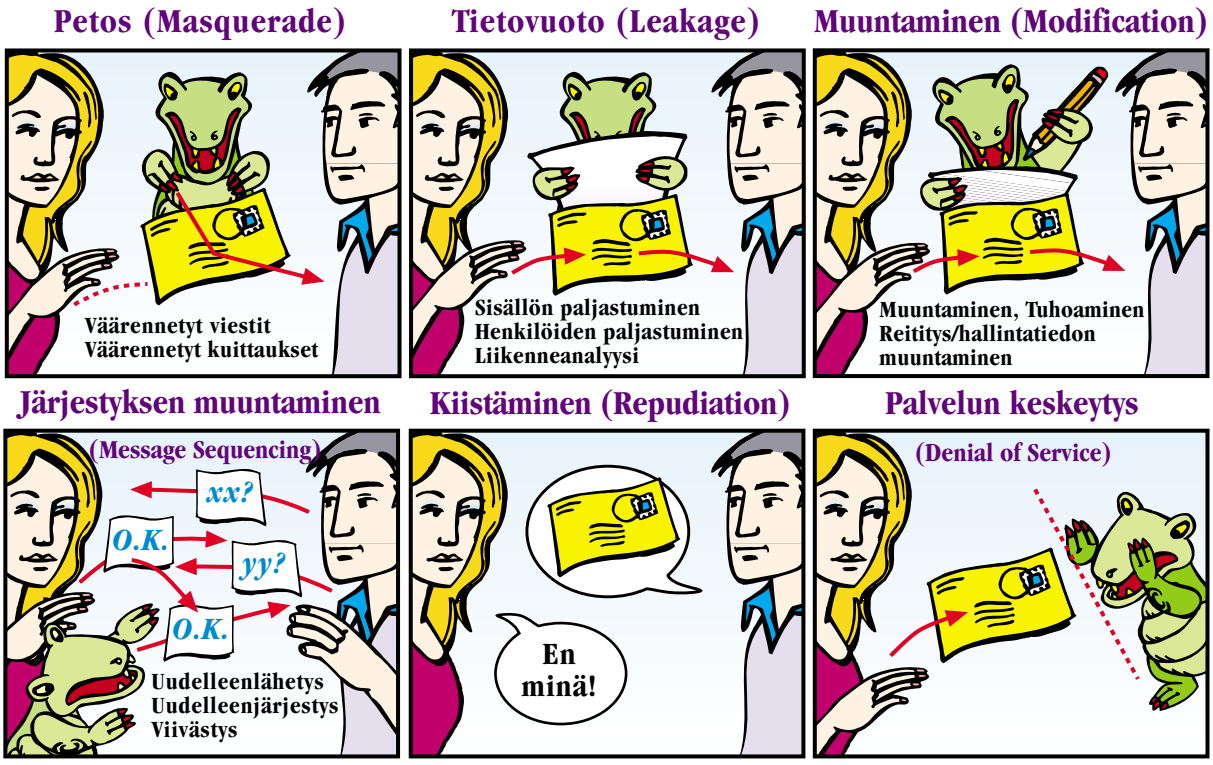
Elektronisen postin turvauhat



Sähköposti oikein hoidettuna on vähintäänkin yhtä turvallista kuin perinteinen paperiposti. Käytännössä läheskään kaikissa yrityksissä turvallisuuteen ei kuitenkaan kiinnitetä asianmukaista huomiota tai tietoturvaan syntyy aukkoja puhtaasti tietämättömyydestä ja sinisilmäisyydestä. Kuvasivulla on kooste tavanomaisimmista elektronista postia uhkaavista tekijöistä.

Petos (masquerade) tarkoittaa väärennettyjä viestejä tai kuittauksia. Postia on erittäin helppo lähettää vaikkapa väärällä nimellä. Suojautumiskeino on ***alkuperän varmistus*** (authentication) tai ***pääsynvalvonta*** (access management).

Tietovuoto (leakage) on mahdollista monella tavalla. Postijärjestelmät ovat luonteeltaan store-and-forward-toiminteisia ja pitkällä matkalla oleva viesti välivarastoituu moneen paikkaan ja/tai saattaa olla siepattavissa suoraan linjalta. ***Luottamuksellisuus*** (confidentiality) saavutetaan tavallisimmin ***salauksella*** (encryption) ja tietojärjestelmien laatua voidaan arvottaa ***turvaluokituksella*** (security labelling).

Postiin voidaan puuttua ***muuntamisella*** (modification) tai ***järjestyksen muuntamisella*** (message sequencing). Näitä vastaan voidaan suojautua ***eheyspalveluilla*** (data integrity) ja ***alkuperän varmistuksella***.

Jos sähköpostille halutaan juridisesti sitovaa statusta, on toteutettava ***kiistämättömyyspalvelut*** (non-repudiation), jotta kommunikoivat osapuolet eivät voi ***kiistää*** lähettäneensä tai vastaanottaneensa sanomia.

Palvelun keskeytys (denial of service) saadaan aikaan esim. ruuhkauttamalla tahallaan kohdejärjestelmä sanomien määrällä tai koolla. Vastalääkkeenä on tavallisimmin oikea ***konfigurointi*** ja ***suodatukset***.