Savonlinnan Kaimisto

Mikä on SSL-salaus tai TLS-salaus?

SSL-salaus muodostuu sanoista Secure Sockets Layer ja on käytännössä sama asia kuin TLS-salaus (Transport Layer Security). Kyseessä on protokolla, jolla salataan verkon yli tapahtuvaa liikennettä kahden sovelluksen välillä, kuten kotisivujen ja sivuston kävijän selaimen välillä.

HTTPS salaus ja sen merkitys

SSL-salauksen tarkoituksena on hyödyntää suojattua HTTPS yhteyttä sivuston ja kävijän välillä, siten etteivät ulkopuoliset pääse yhteyden väliin. SSL suojaus mahdollistaakin näin esimerkiksi kävijän arkaluontoisten tietojen turvallisen syöttämisen erilaisiin verkkopalveluihin, kuten verkkokauppoihin.

Mistä tunnistan SSL salausta käyttävän sivuston?

Salauksen tunnistaa juurikin HTTPS alkuisesta polusta selaimen osoiterivillä. Salaamattomat sivustot toimivat puolestaan HTTP alkuisina. Hieman selaimesta riippuen, selaimet esittävät myös salatuilla sivustoilla pienen lukon kuvan, usein osoiterivin yhteydessä. Lukkoa painamalla saa useinkin lisätietoja salauksesta ja sen varmenteesta.

Selain saattaa myös herjata, että sivuston salauksessa on puutteita. Tämä johtuu useimmiten siitä, että sivuston toteuttaja ei ole koodissa käyttänyt kaikkiin elementteihin salausta hyödyntävää HTTPS protokollaa, vaan esimerkiksi jokin yksittäinen mediatiedosto ladataan sivustolla suojaamattoman HTTP yhteyden välityksellä.
Tällaisia kuvatiedostoja on myös vielä taimistomme sivuilla. Koodiston päivittäminen uuteen suojattuun muotoon on suuri työ ja teemme sen vähitellen talven aikana. Sivustomme toimii tällaisia tiedostoja avatessa käyttäjän suuntaan, kuten aikaisemminkin http-sivuston aikana. Muutaman selaimet saattavat tästä varoittaa, mutta kuvan avaaminen sivustollamme on käsityksemme mukaan yhtä turvallista, kuin se on ollut jo toistakymmentä vuotta.

SSL-salaus ja SSL Sertifikaatti

SSL-salaus perustuu varmenteisiin, joilla sivustot todistavat olevansa luotettavia toimijoita. Varmenteista käytetään yleisimmin nimitystä SSL Sertifikaatti. Salausta on teknisesti mahdollista käyttää myös ilman varmennetta, mutta tällöin kävijöiden selaimet varoittavat käyttäjiään puuttuvasta sertifikaatista.