5 LIHTSAT NIPPI OMA VEEBILEHE TURVALISUSE TÕSTMISEKS

Kui sa hakkad kohe kasutama neid viite lihtsat nippi, siis **elimineerid** sa tervelt **99%** viirustest, pahavarast ja pahatahtlikest rünnakutest. 100% turvalisust pole kahjuks selles maailmas võimalik garanteerida. See on kui võidurelvastumine külma sõja ajal. Küll on pahad peal, küll head. Ja niimoodi lõputult.

Olen veebilehti valmistanud pea 20 aastat. Tõsisem tegemine algas aga koos WordPressi sünniga. Sellest ajast peale kasutan ma ainult WordPressi.

Nii mõnedki pelgavad seda platvormi just seetõttu, et see on maailma populaarseim sisuhaldussüsteem ning sellele on ehitatud umbes **60% kogu maailma veebilehtedest**, mille sisuhaldussüsteem on teada.

Ja õigusega pelgavad. Sest mida populaarsem on platvorm, seda populaarsem on see ka häkkerite silmis.

Samas pelgavad asjata. Just tänu populaarsusele ja avatud koodile on WordPress ka **kõige turvalisem platvorm** oma veebi loomiseks, kuna abivalmis ja oskajaid meistreid leidub üle maailma kümneid tuhandeid, kes loovad aina uusi võimalusi WordPressi turvalisemaks muutmisel.

Võib ju küsida, et miks peaks mingi häkker huvituma sinu pisikesest ärist. Vastus on lihtne - ega ei huvitugi. Häkkerid on maailma kõige sallivamad inimesed. Nad ei hooli ei sinu nahavärvist, rahvusest ega sellest kas sa oled maskiusku või mitte. Ja samas on nad oporunistid. Iga avatud uks on võimalus oma võrku laiendada ja enda kasuks tööle panna.

Sellegipoolest pead ka **sina, kui veebilehe omanik** ja/või haldur, osalema aktiivselt oma veebi turvaliseks muutmisel.

Õnneks pole selleks vaja olla ei programmeerija ega IT spetsialist.

Piisab, kui järgida viite lihtsat nippi.

Aga enne veel, kui ma neid nippe sinuga jagan, näitan ma sulle, mis võib olla ühe **küberrünnaku hind sinu jaoks**.

Kujuta ette...

… kui **palju tulu jääb sul saamata** tänu sellele, et su veebileht on maas.
… et sinu veebileht on **Google poolt blokeeritud** ja see teatab kõigile külastajatele, et sinu **lehel on pahavara**.
… millist **mainekahju teeb see sinu ettevõttele**.
… kui **palju aega kulub** kõikidele klientidele teavitamisele, et sa oled olukorra peremees ja suudad nende isiklikke andmeid turvaliselt hoida.
… kui **palju ressursse kulub** veebilehe ja maine puhastamisele peale sellist õnnetust.

Rääkimata sinu **magamata öödest**, kulunud närvirakkudest ja neist tulenevatest terviseriskidest.

Niisiis… 5 lihtsat nippi

1. Hoia oma veebileht uuendatuna.

Nii lihtne asi ei saa tegemata jääda. Ära ignoreeri, kui sul on võimalus uuendada WordPressi ennast, pluginaid või teemasid. See on kõigest üks (või paar) hiireklikki.

2. Kasuta tugevaid salasõnu.

Teine äärmiselt lihtne viis pahalasi eemal hoida. Kasuta teiste jaoks keerulisi, samas endale kergelt meelde jäävaid fraase koos numbrite ja muude tähemärkidega. Nõua tugevaid paroole ka teistelt veebilehe haldajatelt ja kasutajatelt.

3. Kasuta kaheastmelist sisse logimist.

Alati, kui võimalik kasuta seda. Esimeses astmes tavalised sisselogimise andmed ning teises astmes eraldi sisestatav turvakood.

4. Tee regulaarseid pahavara skänne.

Mõnikord võib juhtuda, et su veebileht juba sisaldab pahavara. Ise sellest teadmata. Selle vältimiseks tee aeg-ajalt pahavara skänne.

5. Tee veebist tagavarakoopia.

See ei aita küll otseselt turvalisusele kaasa, kuid annab turvatunnet kindlasti. Sest alati on hea teada, et on võimalik taastada viimane töötav versioon.

Mis edasi?

Esimese asjana tee kõik need viis punkti läbi. Et sul oleks lihtsam turvaliselt edasi minna, saadan sulle postkasti täpsemad juhised iga punkti kohta.

Juhuks kui su veebileht on ikkagi rünnaku ohvriks langenud, võta kohe ühendust feliks@veebimeister.com. Teeme selle kiiresti korda.

2020 Feliks Stavitski, veebimeister.com