Mikko Punkari

Huijaussivustot ja web-sivustojen luotettavuus

Tietotekniikan kandidaatin tutkielma

11. joulukuuta 2013

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Mikko Punkari

Yhteystiedot: Ag C233.2, mikko.o.punkari@jyu.fi

Ohjaaja: Ville Isomöttönen

Työn nimi: Huijaussivustot ja web-sivustojen luotettavuus

Title in English: Scam sites and credibilty of websites

Työ: Kandidaatin tutkielma

Suuntautumisvaihtoehto: Tietotekniikan laitos

Sivumäärä: 54+0

Tiivistelmä: Tutkielmassa tarkastellaan, miten käyttäjät käyttävät internetiä, millä perusteella käyttäjät valitsevat käyttämänsä verkkosivuston tai –palvelun, ja kuinka käyttäjät arvioivat sivuston uskottavuutta ja luotettavuutta.

Tutkielma tarkastelee tekijöitä, jotka vaikuttavat käyttäjän arvioon sivuston uskottavuudesta ja luotettavuudesta ja kertoo, miten ja millä menetelmin huijaussivustojen ylläpitäjät käyttävät hyväkseen tätä tietoa.

Avainsanat: internet, tietoturva, uskottavuus, luotettavuus, kalastelu, huijausivustot

Abstract: This document tells how user uses internet and chooses company or service in internet. The Document opens how users evaluate credibility and security of the sites and tells the main factors that have most affect in evaluating prosess. Document also discripes how cybercriminals behind scamsites take advance on this information.

Keywords: internet, kybersecurity, credibility, phsihing, scam sites, corrupted sites

Esipuhe

Kandidaatintutkielman aihe täytyi valita nopeasti. Käytin yli viikon miettiessäni, mikä minua kiinnostaa. Ennen tietotekniikan opiskelujen aloittamista pyrin opiskelemaan psykologiaa. Käytettävyys, havaitseminen ja kognitiivinen psykologia kiehtovat edelleen. Aikaisemmissa opinnoissani olin tehnyt pienen kirjallisuuskatsauksen, jossa arvioitiin erään yhdistyksen web-sivustoa palvelimen lokitietojen pohjalta. Lokitiedostoja oli ihmetelty tietoturvakurssilla ja sain tästä mielleyhtymän ja ajatuksen yhdistää tutkielmassani jotenkin käytettävyyttä ja tietoturvaa.

Tämän jälkeen lopulliseen aihevalinnan selkeytymiseen tarvittiin enää yksi sähköpostiini tullut roskaposti. Ajattelin, että “Joku onneton näihinkin lankeaa. Mikähän siinäkin on.” Seuraavaksi tajusin, että päässäni on kysymys, joka olisi riittävän mielenkiintoinen minulle tutkittavaksi.

Kandityöni kirjoittaminen keskeytyi kandidaattiseminaarin jälkeen, kun minut valittiin vuodeksi Jyväskylän yliopiston ylioppilaskunnan hallitukseen. Haluan kiittää Jyväskylän yliopiston Tietotekniikan laitosta välivuoden jälkeen saamastani hyvästä opintojenohjauksesta sekä keväällä 2012 järjestetystä opinnäytetyöpajasta. Lisäksi haluan kiittää mielenkiintoisen Tietojenkäsittelyalan tutkimusmenetelmät-kurssin vetänyttä Hannakaisa Isomäkeä, kandidaattiseminaarin vetänyttä Jani Kurhista, sekä työni perään katsonutta Ville Isomöttöstä.

Suurimmat kiitokset haluan esittää avopuolisolleni Saana Karnistolle sekä tyttärellemme Enna Punkarille, joka syntyi iloksemme 3.5.2013.

Lisäksi haluan pyytää anteeksi lukion äidinkielen opettajaltani Aulis Tuunalta. Pilkkusäännöt unohtuivat pian ylioppilaskirjoitusten jälkeen.

Jyväskylässä 11. joulukuuta 2013

Kuviot

Sisältö

1 Johdanto

Sähköpostiin kertyy jatkuvasti mainos-, kalastelu- ja huijausviestejä. Monella sivulla kerrotaan selaajan IP-osoitteen lottovoitosta. Facebookissa sovellukset pyytävät jakamaan henkilötietoja. Ajattelemme: “Kuka on niin tyhmä, että uskoo niihin?”

Esimerkiksi vuonna 2003 noin kaksi miljoonaa käyttäjää antoi tietonsa kalastelusivustoille. Tästä aiheutui 1.2 miljoonan tappiot yhdysvaltalaisille pankeille ja luottoyhtiöille (Litan 2004). Vuoden 2012 Norton Cybercrime Report kertoo tietoturvahyökkäysten korjaamisen ja varastetun rahan määrän olevan 114 miljardia dollaria. Näistä tietoturvahyökkäyksistä 11 prosenttia on verkkohuijauksia ja 10 prosenttia phishingiä, eli henkilötietojen tai omaisuuden kalastelua (Symantec 2012). Varsin moni on siis “niin tyhmä, että uskoo niihin.”

Huijatuksi tulleiden ääneen arvostelusta huolimatta tavallinen internetin käyttäjä uskaltaa usein tilata ja maksaa ostoksensa verkossa. Kuvaavampi kysymys olisikin: “Mikä tekee internetsivustosta uskottavan?” Tämä tutkimus pyrkii vastaamaan siihen kysymykseen ja selvittämään, miten huijaussivustojen ylläpitäjät käyttävät hyväksi internetin käyttäjien puutteellista arviointikykyä.

Luku 2 esittelee, miten tavallinen ihminen käyttää internetiä kiirehtien, silmäillen, selaillen ja kelvollistaen. Luvussa käsitellään myös tarkkaavaisuutta ja havaitsemista sekä havaitsemista helpottavia hahmolakeja. Luvussa 3 tarkastellaan, millä perusteella käyttäjä tekee valinnan eri verkkopalveluiden väliltä, ja miten hän arvioi sivuston luotettavuutta. Luvussa 4 käydään läpi luvussa 3 esitellyt, verkkopalvelun valintaan ja luotettavuuteen vaikuttavat tekijät sekä muita luotettavan sivuston rakentamisen kannalta olennaisia asioita. Luvussa 5 paneudutaan huijareiden motiiveihin sekä miten huijaussähköpostien ja -sivustojen tekniikoilla käytetään hyväksi ihmisten tapaa käyttää internetiä sekä näiden puutteellisia tietoja sivustojen turvallisuuden ilmaisimista.

Kirjallisuutta yhdistelevällä tutkimuksella pyritään luomaan pohjaa myöhemmälle tutkimukselle ja osoittamaan, että huijaussivuston erottaminen aidosta voi olla todella vaikeaa, varsinkin jos käyttäjä ei ole keskittynyt ja tarkkaavainen.

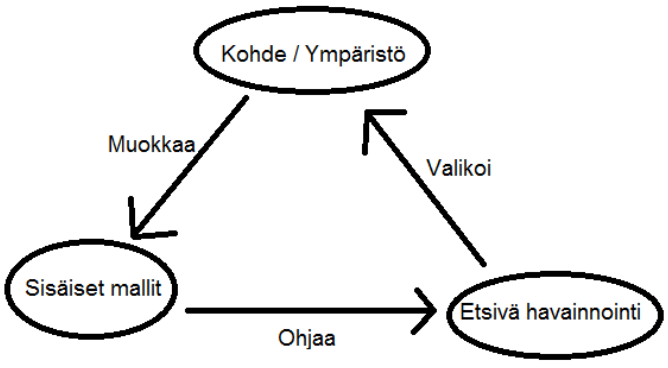
2 Kuinka ihmiset ylipäätänsä käyttävät internetiä?

Tässä luvussa tarkastellaan, miten ihmiset tavallisesti käyttävät internetiä. Selailun, silmäilyn, tarkkaavaisuuden, kelvollistamisen ja käyttämisestä suoriutumisen lisäksi luvussa paneudutaan havaitsemiseen sekä havaitsemista helpottaviin hahmolakeihin.

Kun tiedämme, kuinka ihmiset tavallisesti internetiä käyttävät, olemme valmiimpia ymmärtämään, miten joku voi tulla huijatuksi.

2.1 Selaileminen, silmäily ja havaitseminen

Kognitiivisen psykologian edustajien mukaan internetin käyttöä ohjaa yksi ihmisen monista mielen sisäisistä malleista, eli skeemoista. Tietoisesti tai tiedostamatta ihmiset haluavat säästää aikaa ja löytää etsimänsä nopeasti valtavan informaatiomäärän seasta. Kuviosta 1 näkyy, miten Neisserin havaintokehän mukaan ihmisen skeemat ohjaavat tiedon etsintää ja kiteyttävät ja tiivistävät valtaisaa havaintoinformaation tulvaa (Neisser 1976). Myös käytettävyysasinatuntija Steve Krug (2006, 22) esittää, etteivät ihmiset lue internetsivuja huolella, vaan selaavat ja silmäilevät niitä. Ihminen siis arvio aikaisemmin opittujen tietojensa ja kokemustensa perusteella, mistä ja miten olennaisia asioita tulisi ensimmäisenä etsiä ja valikoi tarjolla olevista havainnoista mielestään olennaisen tiedon. Esimerkiksi sanomalehteä lukiessa katse kiinnittyy ensin otsikoihin ja kuviin. Tämän vuoksi on tärkeää, ettei sivustolle valitut ratkaisut eroa liiaksi muiden sivustojen vastaavista (Krug 2006, 34). Käyttäjä tuskin osaa tai jaksaa etsiä esimerkiksi navigointipalkkia sisällön alareunasta.



Kuvio 1. Neisserin havaintokehä. Muokattu lähteestä (Neisser 1976).

Käyttäjän saadessa uutta tietoa, hän järjestetää sitä edelleen skeemoihinsa. Jean Piaget (1929) on lisäksi tutkinut, että uusi tieto voi joko täydentää ja mukauttaa vanhaa mallia tai korvata sen kokonaan paremmalla. Mikäli käyttäjä on esimerkiksi tulkinnut sivuston idean muutamassa sekunnissa onnistuneesti ja ymmärtänyt, miten sivuston hieman erikoisempi navigaatiovalikko toimii, täydentää tämä uusi tieto luultavasti hänen aiempia navigaatiovalikkoihin liittyviä skeemoja.

Konstruktivistinen havaintoteoria käsittelee havaitsemisprosessia lähes samalla tavalla kuin Neisser. Sen mukaan maailmankuva muodostuu saatavasta informaatiosta, joka yhdistetään henkilön aikaisempiin tietoihin ja asiayhteyteen. Gibsonin ekologisen havaintoteorian mukaan taas havainnoinnin kohteessa, esimerkiksi verkkosivussa, on joukko käyttömahdollisuuksia eli affordansseja. Affordanssi on valikoima mahdollisuuksia, joita ihminen kohteesta havaitsee. Nämä mahdollisuudet kuvaavat niitä toimintoja, joita ihminen kuvittelee kohteella voitavan suorittaa. Gibsonin havaintoteoria eroaa hieman Neisseristä ja konstruktiivisestä havaintoteoriasta, mutta ei kiistä sitä, ettei havainnointia ja affordanssien etsimistä aloitettaisi ensimmäisenä sieltä, missä niiden oletetaan olevan. Kokkonen (2005)

2.2 Tarkkaavaisuus

Tämän osion sisällön lähteenä on käytetty Käyttäjän tarkkaavaisuuden ohjaaminen -esseetä, jonka on kirjoittanut Anne Kettula (2003).

Tiedonkäsittelykykymme on siis rajallinen, ja kuten Neisserin havaintokehä esittää, vain osa ympärillämme tulvivasta informaatiosta pääsee tietoisuutemme asti ja kiinnittää huomiomme muun jäädessä vaimentuneena taustalle.

Tarkkaavaisuuden suuntaamiseen vaikuttavat ulkoiset ja sisäiset tekijät. Ulkoisia tekijöitä ovat mm. erilaiset ärsykkeet, jotka ovat poikkeavia tai suuria intensiteetiltään, äkilliset muutokset sekä varoitusäänet. Mitä selvemmin jokin viesti erottuu muista ärsykkeistä, sitä helpommin kiinnitämme siihen huomiomme. Jos ärsykkeestä on tullut liian tuttu, emme välitä siitä enää. Kuvion 2 havainnollistamaa ulkoiseen ärsykkeeseen reagointia kutsutaan myös suuntautumisrefleksiksi. Liike herättää suuntautumisrefleksimme erityisen tehokkaasti ja sitä tulisikin käyttää verkkosivuilla erityisen harkiten.

Sisäisiä tekijöitä ovat esimerkiksi tunnetilat, vireys, odotukset, tavoitteet ja tarpeet sekä aikaisemmat kokemuksemme. Yleensä huomio kiinnittyy kerrallaan vain yhteen asiaan, jolloin

Kuvio 2. Suuntautumisrefleksi. Kuvion lähde: (Microsoft Clipart).

ihminen ei ole tietoinen muista asioista tai ei välitä niistä. Aikaisemmat kokemukset vaikuttavat siihen, mitä tietoa haluamme käsitellä. Todennäköisimmin huomaamme tiedostettuihin tai tiedostomattomiin tarpeisiimme liittyvät ärsykkeet. Tätä kutsutaan huomion automaattiseksi ohjautumiseksi. Mikäli esimerkiksi internetsivuston valikot toimivat hyvin poikkeuksellisella tavalla, vaatii oman automaattiseksi harjaantuneen toiminnan muuttaminen käyttäjältä enemmän tarkkaavaisuutta ja hänelle aiheutuva kognitiivinen kuorma kasvaa.

Kun käyttäjän huomio kohdistuu yhteen kohteeseen, puhutaan kohdistetusta tarkkaavaisuudesta. Tarkkaavaisuus voi kuitenkin olla myös jaettua tarkkaavaisuutta, jolloin suoritamme useampaa tehtävää samanaikaisesti, kuten kuviossa 3. Mitä harjaantuneempia ihmiset ovat jonkin asian käytössä, sitä vähemmän se vaatii heiltä tarkkaavaisuutta. Esimerkiksi internetsivuston selaaminen hiiren avulla onnistuu tavalliselta käyttäjältä hyvin, vaikkei hän tuijottaisikaan hiiren nappuloita, sillä sen käyttö on pitkälti automatisoitunutta.

Verkkosivujen suunnittelussa tarkkaavaisuuden ohjaaminen on tärkeä huomioida. Sivuston tulee kiinnittää käyttäjän huomio tärkeisiin ja olennaisiin asioihin, jotta työnteko olisi tehokasta ja onnistunutta. Jos käyttäjän tarkkaavaisuus häiriintyy syystä tai toisesta, on sivuston tehtävä saada huomio vangittua takaisin tehtävän suorittamiseen. Tarkkaavaisuuden ohjaamisen apuna voidaan käyttää hahmolakeja, tiedon hierarkisoimista ja sisällön jäsentelyä, tilaan ja aikaan liittyviä vihjeitä, tuttuja metaforia, ikkunointia, värejä, liikettä ja erilaisia varoitustekniikoita. Jos käyttöliittymässä hyödynnetään useampia aisteja, tulee näiden antamien tietojen tukea toisiaan.

Kuvio 3. Jaettu tarkkaavaisuus. Kuvion lähde: (http://www.flickr.com/photos/ryantron/4453018910/ / foter.com / CC BY-ND).

2.3 Kelvollistaminen ja vasteaika

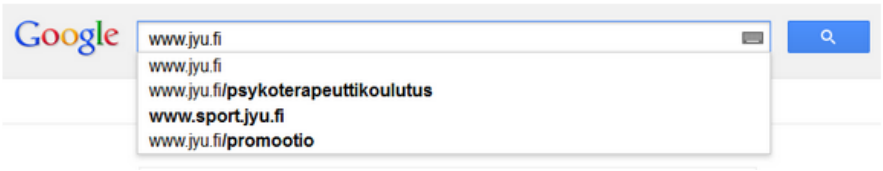
Käyttäjät eivät siis Krugin mukaan lue sivustoja huolella läpi. Näin he eivät myöskään tiedä kaikkia sivuston ja sen sisällön tarjoamia affordansseja. Käyttäjät haluavat löytää etsimänsä kiireellä ja eri vaihtoehtojen optimoiminen on liian aikaa vievää ja vaikeaa. Käyttäjä valitseekin tavallisesti ensimmäinen silmiin osuvan kelvolliselta vaikuttavan vaihtoehdon. Tätä kutsutaan kelvollistamiseksi. Se on tehokkaampaa, varsinkin kun väärästä arvauksesta ei ole paljon haittaa, vaan ongelma ratkeaa selaimen “Edellinen”-painiketta napsauttamalla.

Koska käyttäjien harjoittamaan kelvollistamiseen keskeisimpiä syitä on se, että virheistä ei aiheudu suurta haittaa, järjestelmän pitkä latausaika tai vastaaminen käyttäjän toimenpiteisiin hitaasti turhauttavat käyttäjää, eivätkä anna tyydyttävän nopeasti vastausta kysymykseen “Mitä täällä voi tehdä?” (Krug 2006, 24-25, 95)

2.4 Käyttäjä suoriutuu käyttämisestä

Käyttäjää ei Krugin mukaan kiinnosta selvittää, miten sivusto oikeasti toimii. Riittää, että hän osaa käyttää sitä jollakin toimivalla tavalla, eli suoriutuu sen käyttämisestä. Kuviosta 4 näkyy Krugin kuvailema tyypillinen esimerkki käyttämisestä suoriutumisesta. Hänen mukaansa monet käyttäjät kirjoittavat selaimen aukaistessaan hakukoneeseen haluamansa sivuston koko URL-osoitteen, sen sijaan, että he kirjoittaisivat osoitteen selaimen osoiteriville tai

syöttäisivät hakukoneen kenttään hakusanoja. He toimivat täysin eri tavoin, kuin hakukoneen suunnittelija on tarkoittanut, mutta suoriutuvat silti käyttämisestä heitä itseään tyydyttävällä tehokkuudella. (Krug 2006, 26)



Kuvio 4. Käyttäjä kirjoittaa koko osoitteen hakukoneeseen, eikä käytä hakukonetta hakemiseen. Kuvankaappaus osoitteesta http://google.fi.

2.5 Hahmolait havaitsemisen apuna

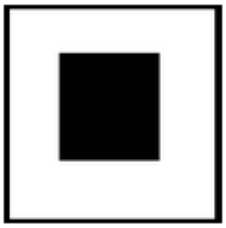
Tämän osion sisällön lähteinä on käytetty Hahmolait käytettävyyden parantajina -tutkielmaa, jonka on kirjoittanut Anna Laine (2004) sekä Visuaalisen havainnoinnin huomioiminen käyttöliittymäsuunnittelussa -esseetä, jonka kirjoittaja on Asko Kokkonen (2005).

Kun käyttäjä saa tietoa näköaistilla kohteesta, siitä muodostetaan aivoissa kokonaiskuva. Käyttäjän odotukset ja kohteen tuttuus vaikuttavat siihen, kuinka nopeasti hän muodostaa kokonaiskuvan ja tunnistaa kohteen. Ennen tunnistusta aivot yhdistelevät havaintoinformaatiota, liittävät sitä yhteen, ryhmittelevät sitä ja muodostavat siitä monimutkaisempia kokonaisuuksia. Näitä eri yhdistelytapoja kuvataan havaintopsykologiassa hahmolaeilla. Oikeastaan ne ovat kuitenkin heurestiikoita, eivät lakeja. Hahmolakien sisältö vaihtelee riippuen lähteestä, mutta yleisimmin mainittuja ovat tuttuus, alueellisuus, sulkeutuvuus, läheisyys, samankaltaisuus, jatkuvuus, valiomuotoisuus ja yhteinen liike.

Kuviossa 5 demonstroitavan tuttuuden lain mukaan tutut kuviot hahmottuvat ensin. Toisin sanoen tarkasteltavat kohteet muodostavat todennäköisemmin ryhmiä, jos näillä on muodostuttuaan kokijalle tuttuja tai merkityksellisiä muotoja. Esimerkiksi ihmishahmo kiinnittää käyttäjän huomion tehokkaasti itseensä.

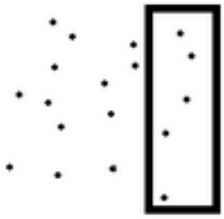
Kuvio 5. Tuttuuden laki. Muokattu lähteestä (Laine 2004).

Alueellisuuden lain mukaan ihminen hahmottaa yleensä pienemmän alueen kuvioksi ja suuremman taustaksi, kuten kuviossa 6.



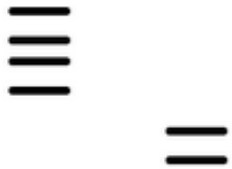
Kuvio 6. Alueellisuuden laki. Muokattu lähteestä (Laine 2004).

Sulkeutuvuuden lain mukaan suljettu, tai lähes suljettu, viiva muodostaa kuvion. Sulkeutuvuus on ehkä yksi yleisimmin käytetyistä hahmolaeista. Jos visuaaliset objektit näyttävät ikään kuin sulkevan sisäänsä jonkin alueen, niin katsoja mieltää tämän alueen erilliseksi kokonaisuudeksi, kuten kuviosta 7 käy ilmi. Onkin tavallinen käytäntö, että verkkosivuilla tiettyyn kokonaisuuteen kuuluvat asiat on suljettu yhteen lohkoon, joka voi puolestaan kuulua johonkin yläkategorian lohkoon, johon kuuluu muitakin lohkoja.



Kuvio 7. Sulkeutuvuuden laki. Muokattu lähteestä (Laine 2004).

Kuviossa 8 havainnollistettavan läheisyyden lain mukaan toisiaan lähellä olevat visuaaliset ärsykkeet mielletään helposti yhteenkuuluviksi. Esimerkiksi painikkeet, jotka liittyvät samaan toimintoon tai tehtävään, asetetaan tämän vuoksi usein lähekkäin.



Kuvio 8. Läheisyyden laki. Muokattu lähteestä (Laine 2004).

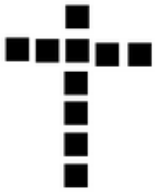
Samankaltaisuuden lain mukaan muodoiltaan, kooltaan tai väreiltään samankaltaiset kohteet katsotaan yhteenkuuluviksi. Esimerkiksi kuvion 9 ympyrät mielletään helposti yhteenkuuluviksi keskenään, kuten kolmiotkin.

Kuvio 9. Samankaltaisuuden laki. Muokattu lähteestä (Laine 2004).

Jatkuvuuden lain mukaan esim. yhteneväinen viiva koetaan kuvioksi. Ihminen kokee esim. kuvion 10 niin, että mustan suorakaiteen takana on ympyrä, vaikka ihminen ei todellisuudessa havaitse suorakaiteen takana viivaa tai mitään muutakaan.

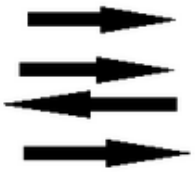
Kuvio 10. Jatkuvuuden laki. Muokattu lähteestä (Laine 2004).

Valiomuotoisuuden laki esittää, miten ihminen pyrkii ymmärtämään kuviot mahdollisimman yksinkertaisina, hyvämuotoisina ja säännönmukaisina. Ihmisellä on siis taipumus havaita yksinkertaisempia kuvioita kuin millaiseksi ne tarkemman tarkastelun jälkeen osoittautuvat. Kuvio 11 koetaan esimerkiksi ristiksi, eikä pieniksi neliöiksi.



Kuvio 11. Valiomuotoisuuden laki. Muokattu lähteestä (Laine 2004).

Yhteisen liikkeen lain mukaan sellaiset kohteet, jotka näyttävät liikkuvan samaan suuntaan samalla nopeudella, mielletään kuuluvan samaan ryhmään. Kuvion 12 kolmannen nuolen koetaan kuuluvan eri ryhmään, kuin kolme oikealle osoittavaa nuolta.



Kuvio 12. Yhdensuuntaisuuden laki. Muokattu lähteestä (Laine 2004).

3 Verkkopalvelun valintaan ja luotettavuuteen vaikuttavia tekijöitä

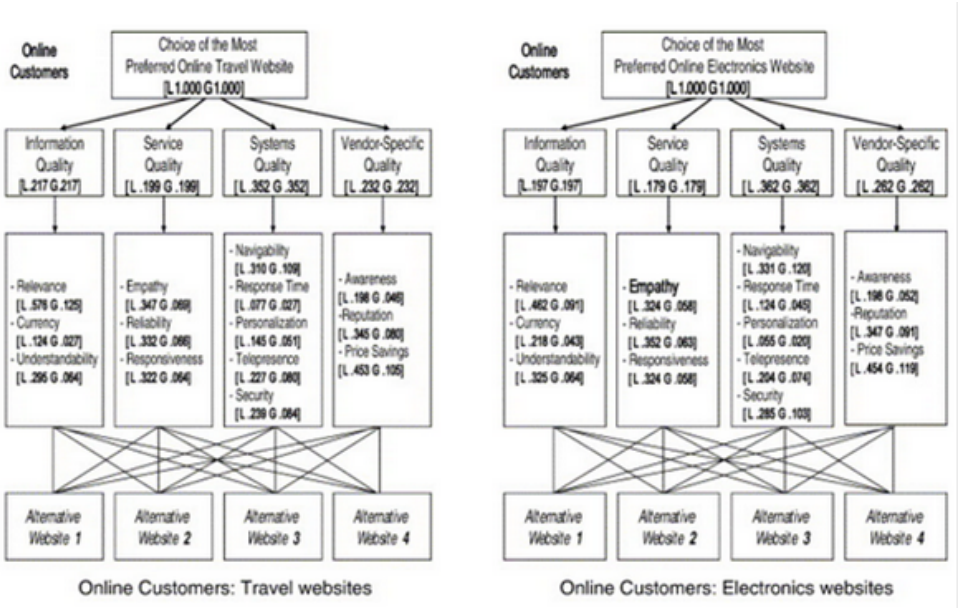
Edellisessä luvussa tarkasteltiin havaitsemista ja tapoja, joilla ihmiset tavallisesti käyttävät internetiä. Tutkimuksessa ei ole kuitenkaan vielä käsitelty lainkaan luotettavuutta. Tässä luvussa esitellään verkkopalvelun valintaan ja luotettavuuteen vaikuttavia tekijöitä kahden eri tutkimuksen tulosten perusteella.

3.1 Tutkimus verkkokaupan ja matkailusivuston valintarperusteista

Kansasin ja Coloradon yliopistojen julkaisemassa tutkimuksessa (Lee & Kozar 2005) pyrittiin selvittämään sivuston laadun vaikutusta verkossa tapahtuvaan liiketoimintaan AHP-menetelmällä (The Analytic Hierarchy Process). Tutkimuksessa selvitettiin, millä perusteella käyttäjät valitsevat käyttämänsä matkatoimistosivuston sekä elektroniikkaa myyvän verkkokaupan. Kuvio 13 vetää tutkimuksen tulokset hyvin yhteen. Siitä käy ilmi, että sekä verkkokauppaa että matkailusivustoa valittaessa käyttäjiin vaikuttivat eniten sivuston ulkoasuun ja rakenteeseen liittyvät seikat, joihin lukeutuvat:

- Sivuston navigoinnin toimivuus
- Sivuston vasteaika
- Sivuston persoonallisuus
- Se miten tuote tai mielikuva siitä oli tuotu sivustolla esille ja
- Sivuston turvallisuus

Kuviosta 13 käy ilmi, että matkatoimistojen kohdalla tärkeäksi nousi myös informaation tarkkuus, ajantasaisuus ja ymmärrettävyys. Sivuston tunnettuus, maine ja hintataso/tarjoukset suhteessa kilpailijoihin olivat toiseksi tärkeimpiä matkatoimistojen kohdalla, ja verkkokauppojen kohdalla niiden merkitys nousi entisestään. Informaation ja palvelun laadulla koettiin sen sijaan olevan vähemmän merkitystä verkkokauppojen kuin matkatoimistojen kohdalla. Kokemuksella palvelun empaattisuudesta, vastavuoroisuudesta ja luotettavuudesta oli vaikutusta valintaan molempien kohdalla, mutta matkailusivustojen kohdalla ne koettiin tärkeämmiksi.



Kuvio 13. AHP-menetelmällä tehdyssä tutkimuksessa ylemmän rivin painoarvoista nähdään, mikä kategoria vaikuttaa päätöksentekoon eniten. Tutkimuksen mukaan sivuston laadulla (engl. Systems Quality) on eniten painoarvoa. Verkkokaupan kohdalla yrityksen maine ja asema kilpailijoihin nähden nousevat suurempaan merkitykseen. Kuvion lähde: (Lee & Kozar 2005).

3.2 Tutkimus sivuston luotettavuudesta

Stanfordin yliopiston julkaisemassa laajassa tutkimuksessa (Fogg ym. 2002) selvitettiin, miten käyttäjät arvioivat internetsivuston luotettavuutta. Tutkimus toteutettiin näyttämällä koehenkilöille eri sivustoja ja keräämällä heiltä kommentteja sivustojen luotettavuudesta. Annetut kommentit käytiin läpi, jonka jälkeen laskettiin, kuinka monessa prosentissa kommenteista oli mainittu jokin tietty luotettavuuteen vaikuttava tekijä.

Kuviosta 14 ilmikäyvien tulosten mukaan eniten painoarvoa oli sivuston ulkoasulla (engl. Design). Myös sivuston visuaalisella rakenteella (engl. Information Design/Structure) ja informaation olennaisuudella (Information Focus) oli tutkimuksen mukaan paljon merkitystä luottamuksen synnyttämiseen. Etenkin sivustolla olevat mainokset vaikuttivat puolestaan negatiivisesti luottamukseen. Mikäli sivuston tarkoitus oli vain myydä tavaraa ja haalia asiakkaiden rahat, koettiin yrityksen motiivit ja sivuston luotettavuus alhaisemmaksi.

	Percent (of 2,440 comments)	Comment Topics (addressing specific credibility issue)
1.	46.1%	Design Look
2.	28.5%	Information Design/Structure
3.	25.1%	Information Focus
4.	15.5%	Company Motive
5.	14.8%	Information Usefulness
6.	14.3%	Information Accuracy
7.	14.1%	Name Recognition and Reputation
8.	13.8%	Advertising
9.	11.6%	Information Bias
10.	9.0%	Writing Tone
11.	8.8%	Identity of Site Operator
12.	8.6%	Site Functionality
13.	6.4%	Customer Service
14.	4.6%	Past Experience with Site
15.	3.7%	Information Clarity
16.	3.6%	Performance on Test by User
17.	3.6%	Readability
18.	3.4%	Affiliations
(Categories with less than 3% incidence are not in this table.)		

Kuvio 14. Vasen sarake kertoo, kuinka suuressa osassa kommenteista oli viitattu oikeassa sarakkeessa olevaan luotettavuuteen vaikuttavaan tekijään. Kuvion lähde: (Fogg ym. 2002).

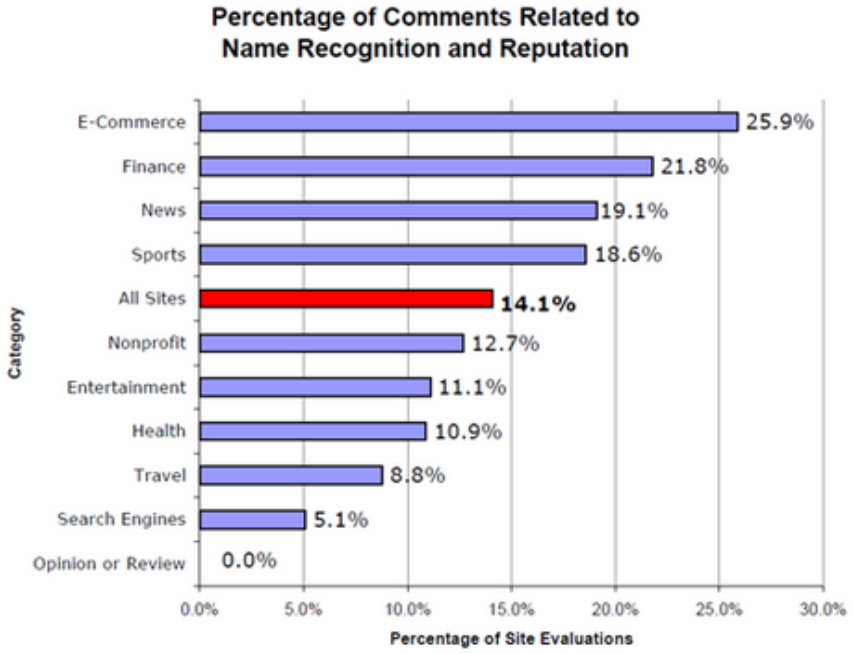
3.2.1 Sivuston tyypillä on väliä

Tutkimuksessa laskettiin myös, miten sivuston tyyppi vaikutti annettuihin kommentteihin. Kyselyssä oli mukana seuraavien kategorioiden sivustoja:

- Hakukoneet
- Verkkokaupat
- Talous- ja sijoitussivustot
- Matkailusivustot
- Terveyspalveluita tarjoavat sivustot

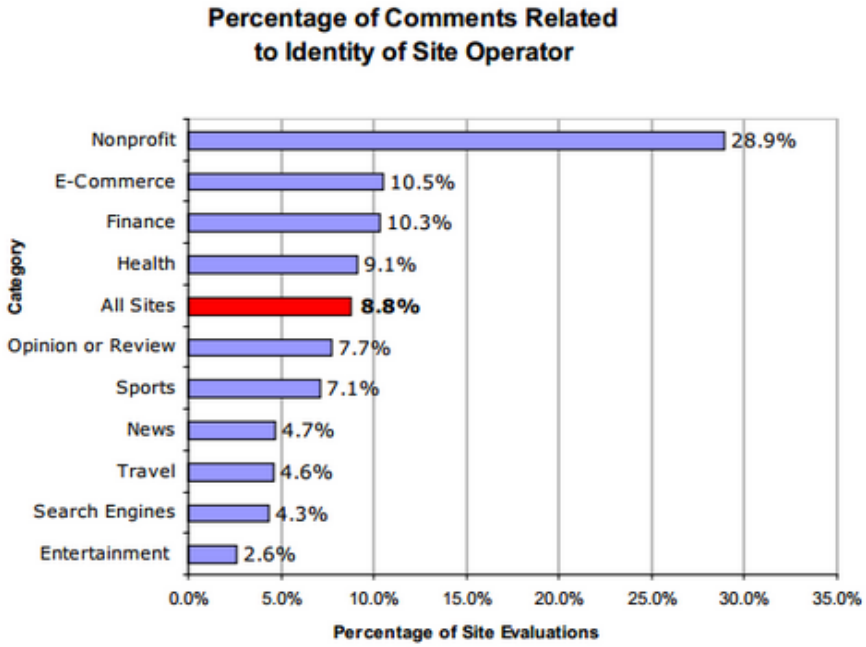
- Voittoa tavoittelemattomat järjestöt
- Uutissivustot
- Viihdesivustot
- Urheilusivustot sekä
- Mielipide- ja arvostelusivustot

Tutkimuksessa kävi ilmi, että sivuston tyyppi vaikutti paljon siihen, millä kriteereillä sivuston luotettavuutta arvioitiin. Kuten Kansasin ja Coloradonkin tutkimuksessa, etenkin verkkokauppojen (engl. E-Commerce) ja sijoitussivustojen (engl. Finance) kohdalla luotettavuuteen vaikutti todella paljon myös yrityksen tai sivuston ennalta tuttu nimi ja maine. Yrityksen tunnettuuden ja maineen vaikutusta luotettavuuteen on havainnollistettu sivustotyypeittäin kuviossa 15. Verkkokauppojen kohdalla koehenkilöt olivat tutkimuksen mukaan muutenkin varovaisempia. He eivät osanneet aina verkkokauppojen kohdalla määritellä, mistä huoli johtuu. Verkkokauppoihin liittyvissä kommenteissa peräti 9,4 prosenttia sisälsivät tällaisia yleisiä epäilyjä. Se on muihin sivutyyppeihin verrattuna huomattavan paljon. Stanfordin tutkimuksessa matkailusivustojen kohdalla asiakaspalvelun saatavuutta pidettiin lukujen perusteella hieman tärkeämpänä kuin Kansasin ja Coloradon tutkimuksessa.



Kuvio 15. Yrityksen tunnettuuden ja maineen vaikutus luotettavuuteen sivustotyypeittäin. Kuvion lähde: (Fogg ym. 2002).

Tutkimuksen tekijät Stanfordin yliopistosta ovat tietoturvan ammattilaisia ja heidät yllätti se, kuinka vähän koehenkilöiden arvioon luotettavuudesta vaikutti varmuus sivustoa ylläpitävän tahon todellisesta identiteetistä (engl. Identity of Site Operator). Luvut on esitetty kuviossa 16. Harvardin yliopistossa 2006 tehty tutkimus tukee tätä havaintoa. Pienemmällä otannalla tehdyssä tutkimuksessa 23 prosenttia koehenkilöistä ei kiinnittänyt mitään huomiota selaimien osoitinpalkkiin tai turvallisuusvihjeisiin. Eniten epäilyä Stanfordin tutkimuksessa herättivät hyväntekeväisyyssivustot ja muiden voittoa tavoittelemattomien tahojen ylläpitämät sivustot (engl. Nonprofit). Verkkokaupat ja sijoitussivustot olivat järjestyksessä toisena ja kolmantena, mutta niiden kohdalla vain hieman yli kymmenen prosenttia luotettavuutta arvioivista kommenteista koski sivuston ylläpitävän tahon identiteettiä.



Kuvio 16. Sivustoa todellisen identiteetin vaikutus luotettavuuteen sivustotyypeittäin. Kuvion lähde: (Fogg ym. 2002).

4 Luotettavan sivuston rakentaminen

Luvussa 3 selvitettiin verkkopalvelun valintaan vaikuttavia asioita. Lisäksi luvussa 3 tarkasteltiin niitä tekijöitä, jotka vaikuttavat käyttäjien arvioon sivuston luotettavuudesta. Tiedämme jo, että moni käyttäjä arvioi sivuston luotettavuutta turvallisuuden kannalta varsin irrelevanttien tekijöiden perusteella.

Tässä luvussa käymme syvällisemmin läpi, miten käytettävyyssuunnittelijat ottavat sivustoja suunnitellessaan huomioon luvussa 3 esitetyt tekijät sekä luvussa 2 esitetyt ihmisille tyypiliset internetin käyttötavat. Toisin sanoen, tässä luvussa perehdymme siihen, miten voidaan rakentaa sivustoja, jotka vaikuttavat monien käyttäjien arviointiperusteiden mukaan hyvin luotettavilta.

4.1 Maine, tunnettuus ja asema suhteessa kilpailijoihin

Kuten Kansasin ja Coloradon (Lee & Kozar 2005) sekä Stanfordin (Fogg ym. 2002) tutkimuksista kävi ilmi, yrityksen maineella, tunnettuudella ja asemalla suhteessa kilpailijoihin on suuri merkitys verkkopalvelun valintaan sekä käyttäjän arvioon sivuston luotettavuudesta. Tyypillisin tapa luoda huijaussivusto on tehdä kopio olemassa olevan hyvämaineisen ja tunnetun yrityksen sivuista. Käsittelemme aihetta syvällisemmin luvussa 5.2.

Täysin uuden sivuston luominen on kuitenkin myös mahdollista. Esimerkiksi huima avajaistarjous saattaa olla hyvä houkutin ja selittää myös sen, miksei huijauksen kohde ole kuullut aikaisemmin yrityksestä. Käyttäjää voidaan yrittää vakuuttaa hyvästä maineesta ja luotettavuudesta myös muilla keinoilla. Näitä ovat mm.

- Sivustolla kerrotaan ulkopuolisista suosittelijoista ja suosituksista
- Sivustolla on kuva yrityksestä sekä yrityksen osoite ja yhteystiedot
- Sivustolla kerrotaan yrityksen työntekijöistä

Mikään ei varmastikaan estä huijareita käyttämästä internetistä löydettyjä kuvia ja tekaisemaan sivustolle muita edellä mainittuja tietoja. Tällä tavoin voidaan luoda myös illuusio toimivasta asiakaspalvelusta. (Fogg ym. 2002)

4.2 Ensivaikutelma sivustosta

Steve Krug (2006, 11) pitää ensimmäisenä ja tärkeimpänä käytettävyyssääntönä sivustojen suunnitellussa ohjetta: “Älä pakota minua ajattelemaan.” Sillä Krug tarkoittaa, että sivuston ratkaisujen on oltava itsestään selviä, eivätkä ne saa aiheuttaa käyttäjälle kognitiivista kuormaa tai pakottaa häntä arvioimaan, mitä sivuston suunnittelijat ja ylläpitäjät ovat milläkin asialla tarkoittaneet. Krugin mukaan yrityksen kotisivun tulee vastata neljään kysymykseen mahdollisimman nopeasti, kun käyttäjä saapuu sivulle ensimmäistä kertaa. Kysymykset ovat:

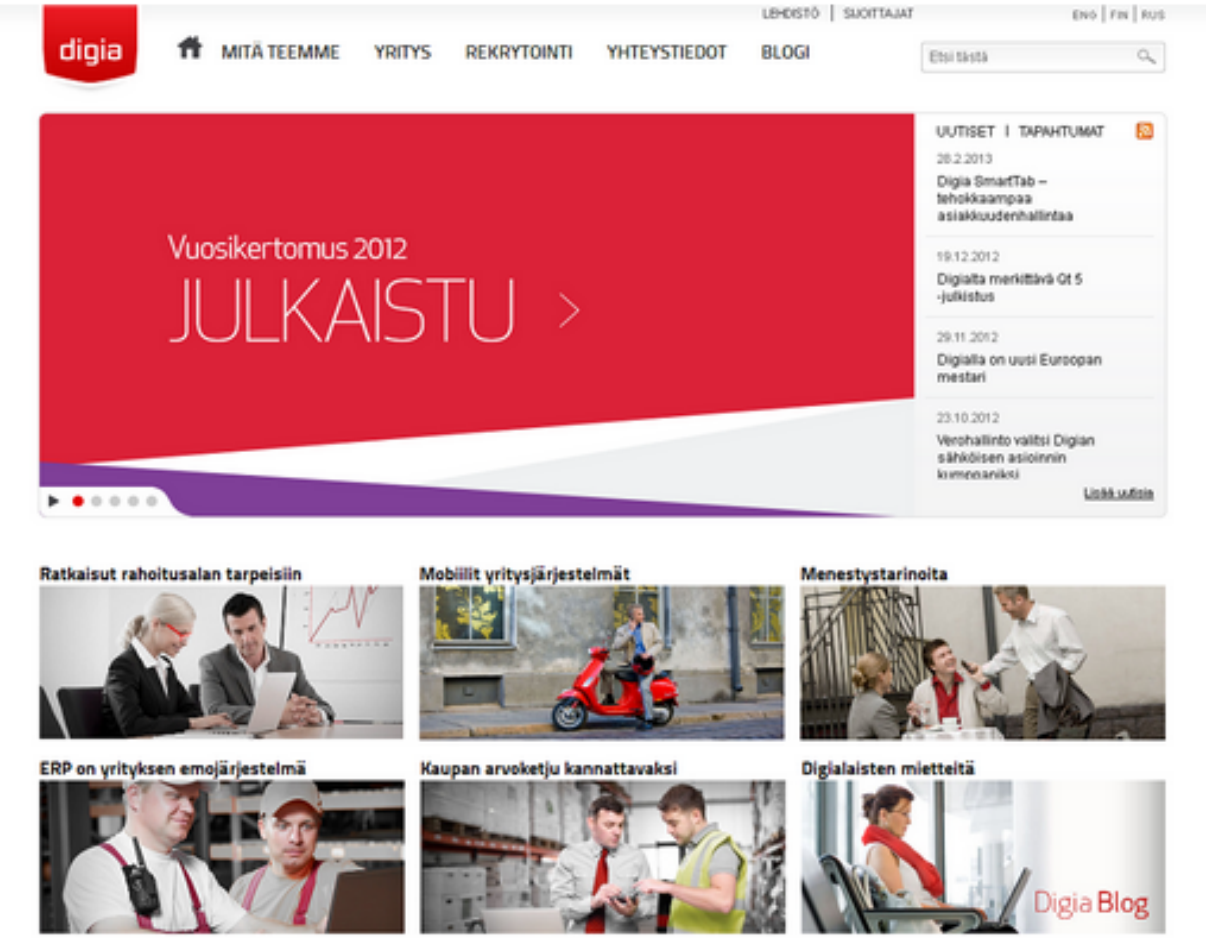
- “Mikä tämä on?”
- “Mitä täältä löytyy?”
- “Mitä täällä voi tehdä?”
- “Miksi minun pitäisi olla täällä eikä jossain muualla?”

Hänen mukaansa käyttäjä turhautuu suurella todennäköisyydellä, jos käyttäjä ei tajua muutaman sekunnin kuluessa, mitä katselee. Mikäli käyttäjä taas tulkitsee sivuston sisällön oikein, tulee käyttökokemuksesta miellyttävä ja onnistunut. (Krug 2006, 95, 99)

4.3 Visuaalinen rakenne

Sivuston visuaalisella rakenteella tarkoitetaan sitä, miten sivuston tiedot ja toiminnot on jaettu selainikkunaan. Länsimaissa lukeminen aloitetaan vasemmalta oikealle ja ylhäältä alas. Käyttäjän katse suuntautuu ensimmäisenä näytön vasempaan yläneljännekseen, ellei mikään muu sivuston osa sieppaa huomiota. Tämän vuoksi sivuston käytön kannalta oleellisimmat tiedot ja toiminnot sijoitetaan ylös ja vasemmalle (Sinkkonen 2002, 120). Sijoittaminen ylävasemmalle kannattaa myös siksi, että näyttöjen ja selainikkunoiden koot vaihtelevat paljon. Myös Krug (2006, 31) kehoittaa noudattamaan yleisiä käytäntöjä ja sijoittamaan tärkeät asiat keskeisille paikoille.

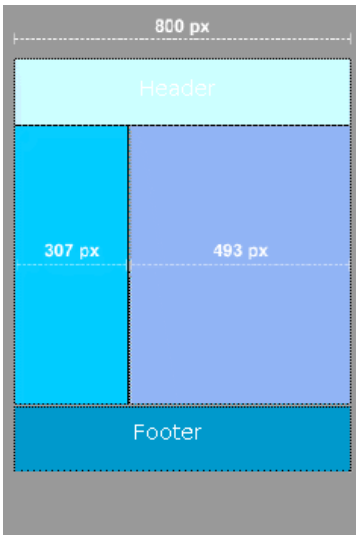
Sivuston tunnus ja navigointivälineet lukeutuvat niihin keskeisiin asioihin, jotka tulee sijoittaa ylös tai vasemmalle. Kuviossa 17 näkyvät Digian kotisivut tarjoavat tästä selkeän esimerkin. Turhia esittelytekstejä ja pitkiä kuvailuja Krug (2006, 45-47) pitää mm. Jacob Nielsenin tutkimuksiin vedoten (Nielsen 2000, 100-103) turhana sanahelinänä. Kysymykseen ”Mikä tämä on?” pitäisi pystyä vastaamaan logon oikealle puolelle sijoitettavalla selkeällä ja informatiiviisella tunnuksella tai iskulauseella (Krug 2006, 101).



Kuvio 17. Digian sivuilla logo ja navigointivälineet löytyvät ylhäältä, josta niitä ensimmäisenä etsisi. Slogania ei löydy, mutta etusivu onnistunee muuten kertomaan, mitä yritys tekee. Käyttäjän katse kiinnittynee ensimmäisenä liikkuvaan uutiskaruselliin tai ihmisten kuviin. Kuvankaappaus osoitteeta http://www.digia.com. Poimittu 3.4.2013.

Ensivaikutelman osalta kysymyksiin ”Mitä täältä löytyy?” ja ”Mitä täällä voi tehdä?” vastaavat Krugin mukaan pysyvät navigointivälineet ja etsintäpalkki. Sivuston on annettava niiden avulla nopeasti hyvä yleiskuva siitä, mitä tarjottavaa sivustolla on sisällön ja toimintojen osalta sekä siitä, miten kaikki on järjestetty. Käyttäjän tulisi löytää niiden avulla nopeasti etsimänsä ja saada tietoa myös sellaisesta, mitä hän ei ole tullut edes ajatelleeksi sivustolta löytyvän. Mikäli tätä kuvaa ei synny tai navigointivälinein tehdyt kokeilut eivät tuota tulosta, käyttäjä ei löydä etsimäänsä ja poistuu suurella todennäköisyydellä sivustolta. Tämän vuoksi sivuston informaatiorakenteen tulisi olla mahdollisimman looginen ja navigointivälineiden kertoa, mistä lähteä liikkeelle, jotta käyttäjän etsimä asia löytyy. (Krug 2006, luku 6)

Tasapainoinen sommittelu syntyy kultaisen leikkauksen avulla, jossa tärkeimmät asiat sijoitetaan näytölle painopistekohtiin. Kultainen leikkaus syntyy, kun jana jaetaan kahteen osaan siten, että pidemmän osan suhde lyhyempään osaan on sama kuin koko janan suhde pidempään osaan. (Beaird 2007) Kuviossa 18 on yksi esimerkki kultaisen leikkauksen avulla toteutetusta sivupohjasta.



Kuvio 18. Esimerkki kultaista leikkausta noudattavasta elementtien jaosta. Muokattu lähteestä (Gervasio 2009).

4.4 Visuaalinen hierarkia

Krug kehoitaa suunnittelijoita vähentämään käyttäjille aiheutuvaa kognitiivista kuormaa 1. jakamalla sivut selkeästi eroteltuihin alueisiin, 2. sijoittamalla loogisesti yhteenkuuluvat asiat yhteen myös visuaalisesti sekä 3. sisäkkäistämään asiat visuaalisesti niin, että osien ja kokonaisuuden suhde näkyy selvästi. Jotta käyttäjä ymmärtää, mikä on tärkeää ja mikä vähemmän tärkeää, on elementtien hierarkian oltava itsestään selvä. Tätä kutsutaan visuaalisen hierarkian rakentamiseksi. (Krug 2006, 31-33) Se onnistuu suunnittelijalta helposti, kun tämä ymmärtää etenkin alueellisuuden, sulkeutuvuuden ja samankaltaisuuden lakeja.

Esimerkiksi kuviossa näkyvällä Suomen amerikkalaisen jalkapallon liiton sivustolla visuaaliset rakenne ja hierarkia on toteutettu seuraavia hahmolakeja hyödyntäen:

- Kirjaimella A merkitty osa on selvästi sivuston tausta ja loput sivustosta sen päällä (alueellisuus).

Kuvio 19. Suomen amerikkalaisen jalkapallon liitto ry:n etusivu. Kuvankaappaus osoitteeta http://www.sajl.fi. Poimittu 3.4.2013.

- Kirjaimilla B, C ja D-merkityt lohkot muodostavat selvästi omat suljetut kokonaisuutensa (alueellisuus ja sulkeutuvuus).
- Kirjaimilla C ja D merkittyjen lohkojen sisältö on myös eroteltu viivoilla toisistaan, joten sisältö on helppo lajitella omiksi suljetuiksi kokonaisuuksikseen (sulkeutuvuus). Vaakaviivat koostuvat itseasiassa pienistä pisteistä, mutta näyttävät viivoilta (jatkuvuus ja valiomuotoisuus).
- Kuvasta näkyy lisäksi, että kaikki valikon B alla oleva kuuluu omaan suljettuun kokonaisuuteensa, jonka valkoinen taustaväri ylettää aina valikon ensimmäiseen välilehteen asti, ja vihjaa, että sen sisältö on osa etusivua (alueellisuus, sulkeutuvuus, samankaltaisuus).
- Valikon B linkit eivät sekoitu keskenään, koska niissä on käytetty riittävää etäisyyttä toisiinsa nähden (läheisyys). Ne erottuvat myös muusta sivustosta omaksi kokonaisuudekseen (samankaltaisuus).
- Ylhäällä oikealla oleva etsintäpalkki ja sen viereinen nappula liittyvät selvästi toisiinsa läheisyyden vuoksi (läheisyys).

4.5 Sivuston värit

Sivuston värit-osion sisällön lähteinä on käytetty kirjoittamaa Käytettävyyden psykologia -kirjaa, jonka ovat kirjoittaneet Irmeli Sinkkonen (2002) ynnä muut sekä Helsingin palvelualojen oppilaitoksen 2007 tekemää Värien merkitys -oppimisaihiota (Helpa 2007).

Värit vaikuttavat ympäristötekijöinä ihmisten mielialaan, tunnelmiin, vireyteen ja viihtyvyyteen. Niillä on merkittävä osa käyttäjän saaman ensivaikutelman ja käyttökokemuksen kannalta ja niiden valinta riippuu hyvin paljon sivuston tarkoituksesta ja kohderyhmästä. Värien kokemisen tavat ja värimieltymykset ovat kuitenkin myös yksilöllisiä. Niihin vaikuttavat aiemmat kokemukset ja värielämykset. Lisäksi eri kulttuureissa värit koetaan eri tavoin niiden vuosisataisen perinteen ja symboliikan mukaan. Sivun 21 taulukossa on esitetty länsimaisen kulttuurin mukaiset väriassosiaatiot.

4.5.1 Kylmät ja lämpimät värit

Kylmät värit ovat värisävyjä, jotka kokemukseen perustuen voivat ilmaista kylmyyttä, kuten siniseen ja sinivihreään vivahtavat värisävyt. Kylmiä värejä pidetään rauhoittavina ja niiden koetaan vetäytyvän taustalle katsojasta päin. Kylmiä värejä käytetäänkin usein web-sivuilla taustaväreinä.

Lämpimät värit ovat värisävyjä, jotka kokemusperäisesti voivat ilmaista lämpimyyttä. Tällaisia ovat esimerkiksi punaisen ja oranssin värisävyt. Lämpimät värit koetaan nousevan kuvapinnalta katsojaa kohti ja ne vetävät tarkkaavaisuuden puoleensa tehokkaasti. Tämän vuoksi lämpimät värit sopivat hyvin niihin sivun osiin, joihin käyttäjän tarkkaavaisuus halutaan kiinnittää.

Väri	Assosiaatiot
Punainen	seis, vaara, kuuma, tuli, impulsiivisuus, ulospäin suuntautuneisuus, lämpö, hämmennys, paine, veri, aggressiivisuus, suuttumus, viha, ptimistinen, rohkea, stimuloiva, eloisa, aggressiivinen, antaa tehokkaan ja toimeliaan vaikutelman, intohimoa ja huomiota herättävä väri, kommunismin ja vasemmiston väri.
Oranssi	ystävällisyys, vieraanvaraisuus, ylpeys, mielen selkeys, voitto, hyväntuulen ja onnellisuuden väri, joka yhdistetään aurinkoon ja lämpöön.
Keltainen	huomio, varoitus, lämpö, aktiivisuus, aurinko, uusi, idealismi, sairaus, pelokkuus. Keltainen on väreistä valovoimaisin, se on onnellinen, toiveikas, rehellinen ilon, kullan, auringon ja lämpimän väri. Keltainen on myös voittajan väri ja keisarillinen väri, mutta sillä ilmaistaan myös varoitusta.
Vihreä	saa edetä, turvallisuus, rauhallisuus, luonto, tuoreus, toivo, kateellisuus, myrkky, terveys, raha, varakkuus, elämä, kasvu, parantuminen, hulluus, paluu.
Turkoosi	vaaleana viileä, rauhoittava, herkkä ja etäisyyttä luova. Turkoosi on jäätä ja merta.
Sininen	kylmyys, vesi, taivas, jää, vetäytyvä, viileä, tosi, rauhallisuus, viattomuus, epäilys, uneksiminen, alakuloisuus. Tummansininen on auktoriteettien väri, se ilmaisee myös luotettavuutta, voimaa ja suoritusta.
Purppura/Violetti	turhuus, rikkaus, voitto, kuninkaallisuus, hienostuneisuus, nostalgia, hengellisyys, katumus, ylhäisyys, arvoituksellisuus, melankolisuus. Violetti on luonteeltaan mystinen ja juhlallinen väri.
Musta	pimeys, yö, kuolema, paheellisuus, viisaus, valta, murhe, synkkyys, epätoivo, arvokkuus, synti, kielteisyys, kaiken loppu, tuska, machous, urbaanius. Musta tuo vaaleiden ja värikylläisten värien sävyt entistä loistokkaammin esille.
Valkoinen	viattomuus, kunnollisuus, rehellisyys, kylmyys, totuus, puhtaus, valoisuus, viisaus, voima, kohtalo, talvi, lumi. Valkoinen on hyvä tausta muille väreille ja se antaa sommittelulle ilmavuutta valovoimaisuutensa vuoksi.
Harmaa	arkisuus, karuus, yhtenäisyys, toiveikkuus, rajoittavuus, vakavuus, konservatiivisuus, turvallisuus, menestys, tyyneys, kypsyys. Laajana ja tasaisena kenttänä harmaa muodostaa vaaleille ja tummille väreille neutraalin taustan.
Ruskea	luotettavuus, voimakkuus, arkisuus ja maanläheisyys, korkeat moraaliset arvot, velvollisuus, vanhahtavuus, köyhyys, yksinkertaisuus, pitkäveteisyys ja ennustettavuus.

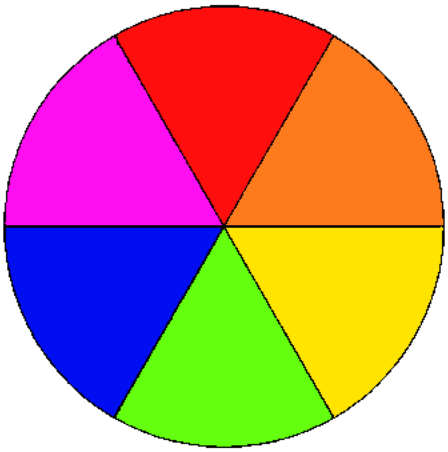
4.5.2 Värien kontrastit

Kontrasti yleensä tarkoittaa vastakohtaa tai jyrkkää erilaisuutta. Värien kontrastilla tarkoitetaan, miten havaittu väri voimistuu tai heikkenee, kun sen rinnalla esiintyy toinen tai useampi väri. Värien keskinäinen käyttäytyminen on tärkeä tiedostaa sivustoja suunnitellessa tavoitellun käyttökokemuksen vuoksi. Esimerkiksi tekstin on erotuttava taustastaan selvästi, eli kontrasti tekstin ja sen taustan välillä tulee olla suuri. Kontrasteja on seitsemää eri tyyppiä.

Kuviossa 20 näkyvä sävykontrasti, eli kirkkaiden ja puhtaiden värien kontrasti, on yksinkertaisin värikontrasti. Esimerkiksi liikenteessä käytettävissä varoitusmerkeissä sekä pienille lapsille suunnitelluissa kuvissa käytetään usein sävykontrastia. Sommitelmana kirkkaiden ja puhtaiden värien kontrasti on värikäs, mutta usein se on myös hyvin kova.

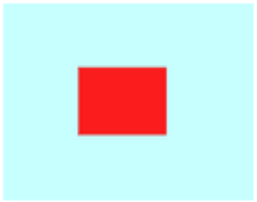
Kuvio 20. Sävykontrasti

Komplementtikontrasti syntyy pääväristä ja sille vastakkaisesta väliväristä. Vastavärit on helppo nähdä kuvion 21 väriympyrästä. Vastavärit muodostavat oudon parin. Ne ovat vastakohtia, jotka vetävät toisiaan puoleensa. Vastavärisommitelmassa ne saavat toisensa loistamaan. Ne korostavat ja täydentävät toisiaan. Jos esim. yhtä kirkas punainen ja vihreä asetetaan keskenään vierekkäin, silmissä alkaa välkkyä.



Kuvio 21. Vastavärit on helppo nähdä väriympyrästä. Muokattu lähteestä (Helpa 2007).

Kulöörikontrasti on lämpimän ja kylmän värin kontrasti. Yleisesti ajatellaan, että keltainen, punainen ja oranssi ovat lämpimiä värejä ja sininen, vihreä ja lila kylmiä. Kaikista väreistä löytyy kuitenkin kylmiä ja lämpimiä sävyjä. Mikäli esimerkiksi vihreän sekoituksessa on käytetty paljon enemmän keltaista kuin sinistä, alkaa se lähestyä lämmintä väriä. Lämpimät värit tulevat katsojaa kohti ja kylmät värit loittonevat. Esimerkiksi kuviossa 22 punainen tulee katsojaa kohti ja turkoosi loittonee. Kylmä ja lämmin väri rinnakkain tuovat toistensa ominaisuudet paremmin esille. Värit alkavat hehkua. Jos ne ovat lisäksi vastavärejä, saavutetaan maksimaalinen kirkkaus. Kaksi kylmää väriä rinnakkain lämmittävät toisiaan. Kaksi lämmintä väriä rinnakkain viilentävät toisiaan.



Kuvio 22. Kulöörikontrasti. Lämmin punainen erottuu hyvin kylmästä turkoosista. Muokattu lähteestä (Helpa 2007).

Valöörikontrastilla tarkoitetaan värin tummuus- ja vaaleusasteen vaihtelusta syntyviä kontrasteja esim. kuvion 23 tumma sininen – vaalea sininen. Tummat ja vaaleat värit korostuvat rinnastettuina, eli vaalea näyttää tumman rinnalla vaaleammalta kuin vaalean vieressä. Voimakkain kontrastipari on musta-valkoinen.

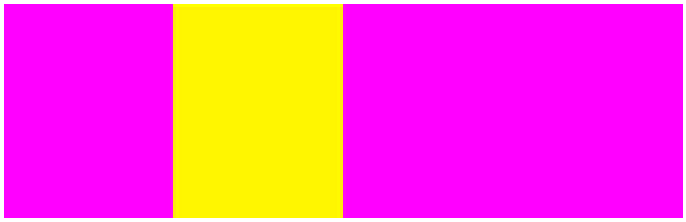
Kuvio 23. Valöörikontrasti. Muokattu lähteestä (Helpa 2007).

Mikä tahansa väri sävyttyy näköhavainnossa vierekkäisen värin vastakkaisvärillä. Jos esim. harmaa väri asetetaan eri taustoille, se näyttää aina eri sävyiseltä. Näin ollen harmaa väri punaisella pohjalla näyttää vihertävältä. Väri pyrkii lisäämään sitä lähellä olevaan väriin vastaväriään. Ilmiö näkyy hyvin kuviossa 24 ja sitä kutsutaan simultaanikontrastiksi.

Kuvio 24. Sama harmaan sävy näyttää eri värilillä pohjilla eri sävyiseltä. Muokattu lähteestä (Helpa 2007).

Kirkkaan ja tumman värin kontrastissa, eli kvantiteettikontrastissa kirkkaat pinnat näyttävät suhteellisesti suuremmilta kuin tummat. Tämä johtuu siitä, että kirkas väri on voimakkaampi kuin tumma. Esim. kuviossa 25 violettia tarvitaan kolme kertaa suurempi määrä kuin keltaista, jotta värien vaikutus olisi yhtä suuri. Tämän vuoksi kvantiteettikontrastia kutsutaan myös pinta-alakontrastiksi.

Kvaliteettikontrasti perustuu puolestaan värien kylläisyysasteiden tuottamiin vastakohtaisuuksiin. Puhdas, runsaspigmenttinen väri tulee aina esiin sameampien värien joukosta. Tämän vuoksi puhdasta väriä käytetään usein sommittelussa korostamaan haluttuja paikkoja. Kuviossa 26 puhdas turkoosi erottuu hyvin sameammasta sävystä.



Kuvio 25. Kvantiteettikontrasti. Kirkas keltainen näyttää kokoaan suuremmalta. Muokattu lähteestä (Helpa 2007).

Kuvio 26. Kvaliteettikontrasti. Puhdas väri erottuu hyvin murretusta. Muokattu lähteestä (Helpa 2007).

4.5.3 Väriharmoniat

Tavallisesti sivustoa suunnitellessa valitaan 2-3 väriä sekä mustaa, valkoista ja harmaata. Näiden lisäksi voidaan kuitenkin käyttää edellä mainittujen eri sävyjä. Värien keskinäistä yhteensopivuutta ja sopusointua kutsutaan väriharmoniaksi. Niitä on olemassa neljää eri tyyppiä.

Valööriharmonia tarkoittaa yhden värin vaaleusasteilla luotavaa harmoniaa esim. kuvion 27 liukuma mustasta valkoiseen. Siitä syntyvä vaikutelma on rauhallinen ja hillitty. Sommitelman mielenkiinto syntyy, kun käytetään erilaisia valoisuusasteita, eli tummia ja vaaleita sävyjä. Joko tummien tai vaaleiden sävyjen olisi oltava sommitelmassa hallitsevassa asemassa.

Kuvio 27. Valööriharmonia. Muokattu lähteestä (Helpa 2007).

Yksiväriharmonialla tarkoitetaan yhdestä väristä saatavaa vivahdussarjaa, jossa perusväriin lisätään vaihtelevia määriä mustaa tai valkoista. Esimerkiksi kuvion 28 punaisessa mustan määrä kasvaa, mitä oikeammalle siirrytään. Yksiväriharmonialla saadaan hillittyjä yhdistelmiä, jonka vuoksi se on turvallinen tapa yhdistellä värejä.

Kuvio 28. Yksiväriharmonia. Muokattu lähteestä (Helpa 2007).

Vastaväriharmonia syntyy yhdisteltäessä värejä tai väriryhmiä väriympyrän vastakkaisilta puolilta. Vaihtelemalla värien voimakkuuksia tai murtamalla värejä mustalla saadaan aikaan lukuisia eri vaihtoehtoja. Sommitelmassa kannattaa rajoittaa värejä esimerkiksi ottamalla useita sinisiä ja vain harvoja oranssin sävyjä. Mitä puhtaampi ja voimakkaampi toinen väri on, sitä vähemmän sitä tulee käyttää vastavärinsä kanssa. Kuviossa 29 vastavärit sininen ja oranssi kohtaavat.

Kuvio 29. Vastaväriharmonia. Muokattu lähteestä (Helpa 2007).

Lähivärisessä harmoniassa värit valitaan väriympyrästä läheltä toisiaan. Valitaan esimerkiksi oranssinkeltainen ja keltainen, tai punainen ja oranssi kuten kuviossa 30.

Kuvio 30. Lähiväriharmonia. Muokattu lähteestä (Helpa 2007).

Värien puoleensavetävyys, assosiaatiot, kontrastit ja harmoniat on siis syytä tuntea, jotta käyttäjä saa sivustosta toivotun vaikutelman, ja jotta sivuston värit tukevat tehokasta ja miellyttävää käyttökokemusta.

4.6 Sivuston fontit

Fontit jaetaan kahteen pääryhmään: päätteellisiin ja päätteettömiin. Päätteellisissä on kaarevat viivat eli päätteet, päätteettömissä ei. Näytön alhaisen tarkkuuden vuoksi päätteettömät fontit sopivat paremmin web-sivulle kuin päätteelliset. Päätteellisiä fontteja voi kuitenkin käyttää otsikoihin. Koska otsikot ovat tavallisesti hieman suurempia, luettavuus ei kärsi olennaisesti. (Sinkkonen 2002, 144-145)

Fontin koon tulee olla tarpeeksi suuri leipätekstissäkin. Kokoina 8 - 10 pistettä ovat liian pieniä varsinkin ikäihmisille. Tekstin värivalinnalla voidaan luoda hyvä kontrasti taustaan nähden. Tekstiä voidaan elävöittää valitsemalla toinen väri linkkeihin ja otsikoihin. Turhaa tekstin muotoilua tulee kuitenkin välttää ja linkit ovat ainoa tekstin osa, joissa voi käyttää alleviivauksia. (Sinkkonen 2002, 144-145) Muutenkin käyttäjälle tulisi osoittaa selvästi, mitä sivulla on mahdollista napsauttaa ja mitä ei (Krug 2006, 37).

4.7 Informaation olennaisuus

Krug (2006, luku 5) katsoo, että kohinaa ja kognitiivista kuormaa tulee vähentää myös karsimalla turhat sanat pois tekstistä. Hänen oma nyrkkisääntönsä on, että vähennä ensin puolet tekstistä ja sen jälkeen vielä puolet jäljelle jääneestä tekstistä. Joissakin tapauksissa, kuten matkatoimiston sivujen tunnelmaa luovissa matkakuvauksissa, pidemmät tarinat voivat olla paikallaan, mutta yleensä tekstin määrä vain hidastaa käyttäjää selaamisessa ja estää tätä löytämästä tietoa, jota hän etsii.

Tekstin tulisi siis olla erittäin tiivistä ja ytimekästä, ja välittää käyttäjälle tehokkaasti relevantti ja olennainen informaatio. Teksti ei saa olla liian korkealentoista vaan käyttäjien tai ainakin kohderyhmän tulee ymmärtää, mitä teksti tarkoittaa. Informaation ajantasaisuus on myös tärkeä asia. Mikäli käyttäjä joutuu pohtimaan, onko tieto enää ajantasalla ja pitääkö se enää paikkansa, aiheutuu hänelle turhaa ajatustyötä. Sivustoa tulisi siis päivittää, jotta käyttäjä tietää sisällön pitävän yhä paikkansa. (Krug 2006, 96)

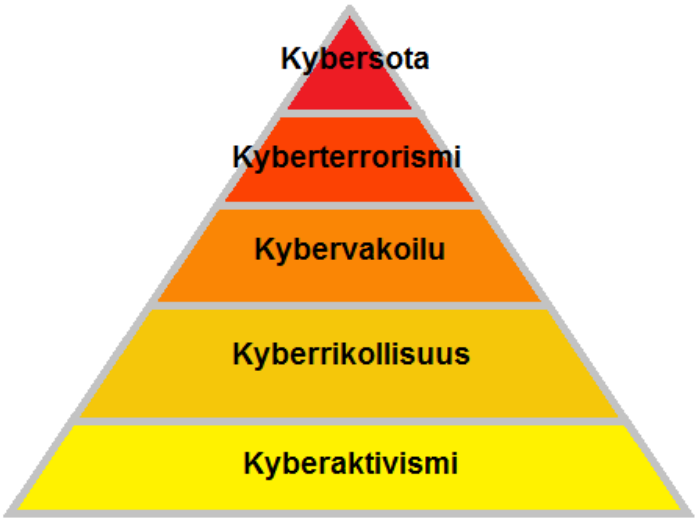
Informaatiolla on myös mahdollista lisätä asiakaslähtöisyyden tunnetta. Sillä on merkitystä, että käyttäjä tuntee yrityksen ymmärtävän hänen tarpeensa. Sama pätee turvallisuuden tunteen luomiseen. Muiden käyttäjien kertomat kokemukset sekä yrityksen yhteystiedot ovat oleellista tietoa. Kansasin ja Coloradon (Lee & Kozar 2005) sekä Stanfordin (Fogg ym. 2002) yliopistojen tutkimukset vahvistavat myös sen, että informaation ajantasaisuudella on merkitystä palvelun valinnassa ja arviossa sivuston luotettavuudesta.

5 Huijaukset

Luvuissa 2-4 on käsitelty monia verkkopalvelun valintaan, luotettavuuteen ja sivuston rakentamiseen liittyviä asioita, joiden tiedostaminen on tärkeää myös täysin rehellisille websuunnittelijoille ja -kehittäjille. Luvussa 5 käsitellään erityisesti, miten käyttäjä arvioi sivustojen turvallisuutta. Lisäksi käsitellään huijareiden motiiveja, käyttäjän manipulointia sekä erilaisia huijauksiin liittyvää tekniikoita.

5.1 Internetrikollisten motiivit

Tietoturvauhkatyypit, eli kyberuhkatyypit voidaan jakaa (Dunn Cavelty 2010) viiteen eri kerrokseen toimijoiden motiivien mukaan, kuten kuviosta 31 käy ilmi. Kolme alinta tasoa ovat kyberaktivismi, kyberrikollisuus ja kybervakoilu. Tässä tutkimuksessa keskitytään huijauksiin, jotka liittyvät lähinnä näihin kolmeen kerrokseen. Kyberterrorismia ja kybersotaa ei käsitellä tässä tutkielmassa.



Kuvio 31. Kyberuhkien jaottelu. Muokattu lähteestä (Lehto 2013).

Debra Shinder (2002, luku 3) kertoo kirjassaan, että kyberaltivismin, -rikosten ja -vakoilun harjoittajien motiiveina tai pyrkimyksenä ovat yleensä jokin tai jotkin seuraavista:

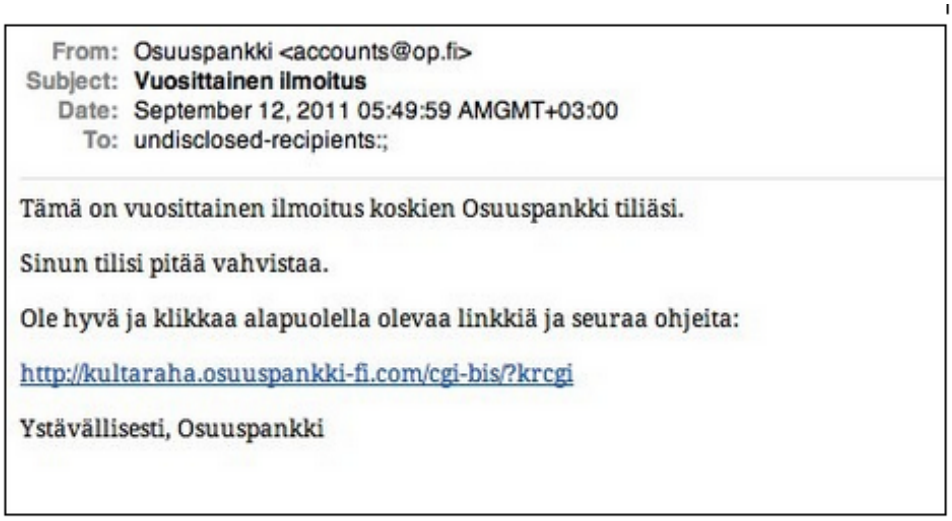
- Käyttäjän tunnusten tai identiteetin varastaminen. Kun tunnukset tai identiteetti on varastettu, niiden avulla voidaan esimerkiksi nostaa rahaa tai tehdä ostoksia käyttäjän nimissä.
- Suora rahan huijaaminen käyttäjältä. Eroaa edellisestä siinä, ettei tunnuksia tai identiteettiä varasteta, vaan huijataan käyttäjä siirtämään rahaa suoraan huijarin tilille tai lähettämään sitä postitse.
- Tietokoneen kaappaus kolmatta tietojärjestelmää vastaan tehtävää hyökkäystä tai roskapostin levitystä varten. Kaappareilla saattaa olla käytössään tuhansia koneita tai sähköpostitilejä, joita käytetään palvelunestohyökkäysten toteuttamiseen ja huijauspostien levittämiseen.
- Tietokoneen kaappaus koneen omistajan tai yrityksen vakoilua varten. Tietokone saatetaan kaapata myös siksi, että sen arvellaan sisältävän jotakin rahan arvoista tietoa. Myös koneen käyttäjää saatetaan vakoilla. Kameran kaappamisen ja vakoilun motiivina saattaa olla rahanarvoinen tieto tai esimerkiksi kaapparin tuntema seksuaalinen mielenkiinto koneen käyttäjää kohtaan.
- Kiusanteko, vandalismi, kosto, näyttämisenhalu ja aktivismi. Aina kyseessä ei ole kuitenkaan välttämättä rahan tai muun taloudellisen hyödyn tavoittelu. Ihmiset tekevät kiusaa ja vandalismia kanssaeläjilleen myös internetissä. Internet tarjoaa taitavalle koneenkäyttäjälle myös turhan hyvän mahdollisuuden kostaa jonkin kokemansa vääryyden anonyymisti ja pienellä kiinnijäämisen riskillä. Monet crackerit tekevät tietoturvarikoksia myös kokeilun ja näyttämisen halusta. Anarkisteimmat haluavat näyttää olevansa järjestäytynyttä systeemiä ja tietoturva-ammattilaisia parempia, toiset kaipaavat vain viihdytystä ja haastetta itselleen, ja jotkut haluavat kasvattaa nimeään ja mainettaan muiden crackerien silmissä. Sivuja kaappaamalla tai roskapostia lähettämällä saatetaan myös hakea näkyvyyttä jollekin poliittiselle kysymykselle tai tilanteelle.

Tässä tutkielmassa ei esitellä yritysten sivustoihin ja tietojärjestelmiin kohdistuvia murtautumistekniikoita, palvelunestohyökkäyksiä ym. yritysten järjestelmien heikkouksiin perustuvia tunkeutumisia, vaan keskitytään internetin huijaussivustoihin, -tekniikoihin ja -uskottavuuteen.

5.2 Käyttäjän manipulointi

Tämän osion sisältö perustuu Handbook of information and Communication -teokseen (Stavroulakis & Stamp 2010).

Käyttäjän manipulointi on toimintaa, jonka tarkoituksena on saada käyttäjä paljastamaan tai antamaan pääsy salattuihin tietoihin. Sosiaalinen manipulointi voi olla huijaus tai yritys saada uhri luottamaan hyökkääjään tarpeeksi. Luottamusta voidaan kerätä esiintymällä jonain luotettava tahona. Esimerkiksi kuviossa 32 tähän on pyritty sähköpostin sisällöllä ja lähettäjätietoja muuttamalla (Sullivan 2011). Käyttäjää voidaan huijata tekosyyllä, eli keksityllä perustelulla, jonka verukkeella yritetään saada kohde esimerkiksi asentamaan haittaohjelma koneelleen tai paljastamaan haluttuja tietoja. (Hadnagy 2011)

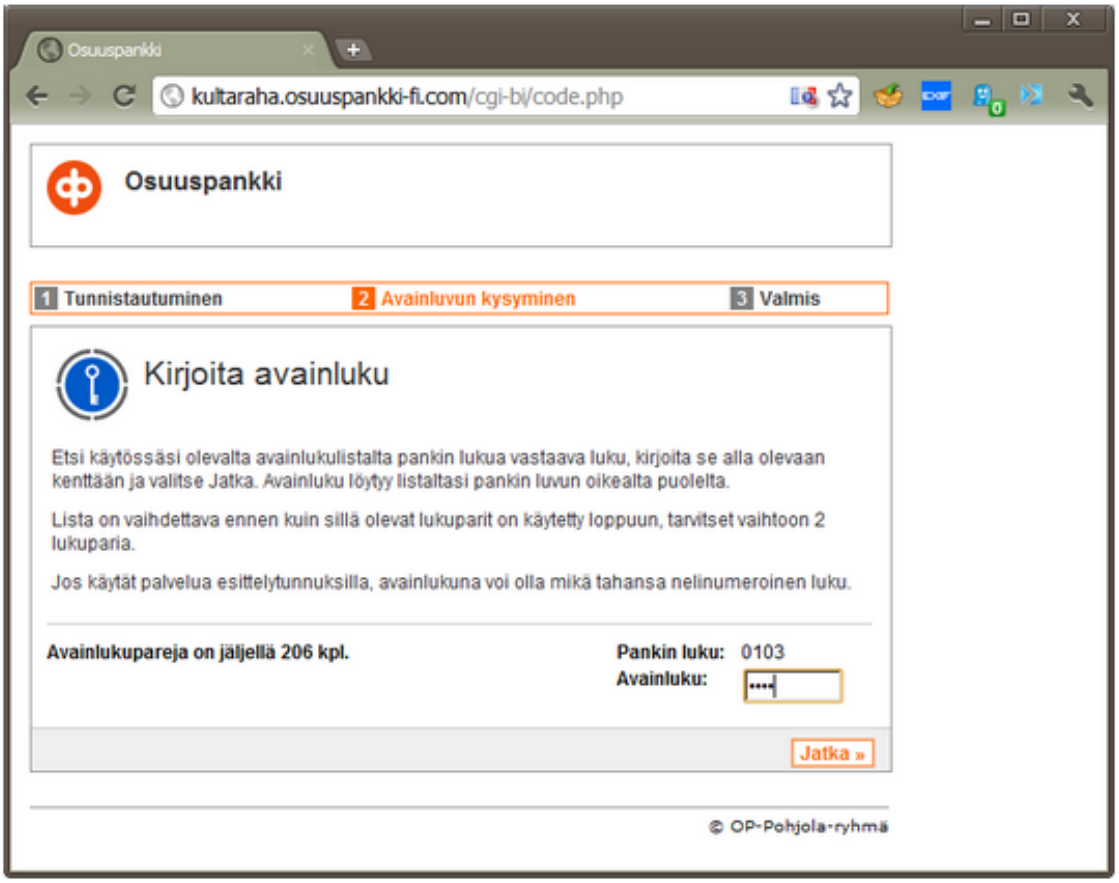


Kuvio 32. Suomen kielinen huijausposti, jonka lähettäjätiedot vaikuttavat luotettavilta. Kuvankaappaus lähteestä: (Sullivan 2011).

Tietojen kalastelua (engl. Phishing) tai suoraa rahan huijausta voi tapahtua myös muun kuin tekosyyn verukkeella. Roskapostina tunnetut sähköpostiviestit vetoavat usein kohteen omatuntoon ja haluun auttaa, ja pyytävät lahjoittamaan rahaa hyvään tarkoitukseen. Köyhän nigerialaisen sijaan salainen tili kuuluu kuitenkin huijareille. Roskapostit sisältävät usein myös tarjouksia tai mainoksia, ja linkin huijaussivustolle, jossa käyttäjä huijataan:

- antamaan luottokortin numero, pankkitunnukset, sosiaaliturvatunnus tai muuta arkaluontoista tietoa. Esimerkiksi kuvion 33 sivusto vaikuttaa varsin aidolta, mutta se on todellisuudessa huijaussivusto, jolla kalastellaan pankkitunnuksia (Sullivan 2011).
- asentamaan koneelle haitta- tai vakoiluohjelma, joista kerrotaan enemmän osiossa 5.5. tai
- maksamaan salaiselle tilille tuotteesta tai palvelusta, jota hän ei tule koskaan saamaan.

Yksinkertainen tapa saada tietoonsa tunnukset on myös katsoa kohteen olan yli, kun hän



Kuvio 33. Aidolta vaikuttava sivusto, jolla kalastellaan pankkitunnuksia. Kuvankaappaus lähteestä: (Sullivan 2011).

käyttää niitä, mutta tässä tutkielmassa ei paneuduta fyysistä läsnäoloa vaativiin tai puhelinmen välityksellä tehtäviin huijaustekniikoihin, vaan keskitytään internetin huijaussivustoihin, -tekniikoihin ja internetin uskottavuuteen.

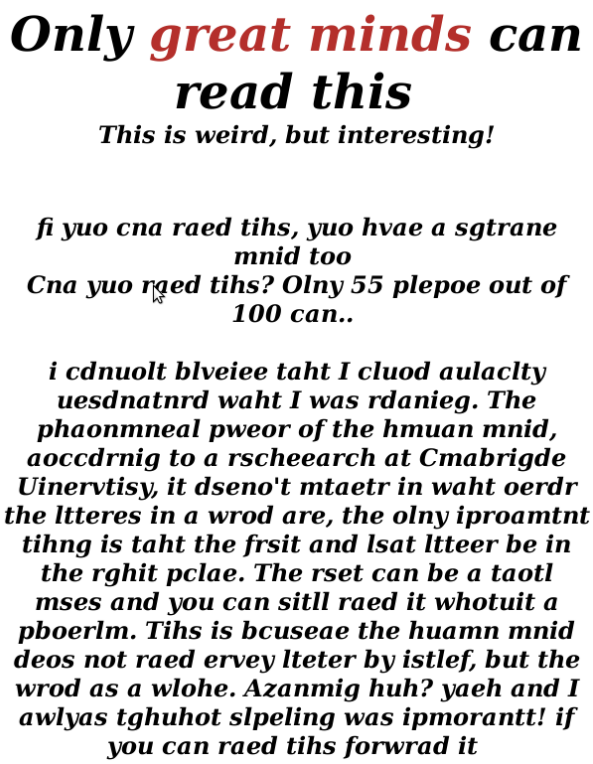
5.3 Sähköpostien huijaustekniikat

Sähköpostin lähettäjätietoja on mahdollista muuttaa sekä lähettäjän nimen että sähköpostiosoitteen osalta. Luotettavana tahona esiintyminen sähköpostilla ei siis ole teknisesti kovin hankalaa. Tätä voi verrata siihen, että huijari merkitsisi kirjekuoreen lähettäjäksi jonkun muun kuin itsensä. Käyttäjän ei siis kannata luottaa sähköpostin lähettäjätietoihin.

Mikäli käyttäjän sähköposti tukee HTML-muodossa olevia viestejä, on linkkien käyttäminen sähköposteissa mahdollista. Tällöin käyttäjän tulisi ennen linkin painamista, tai viimeistään

heti sivustolla, tarkistaa mihin osoitteeseen linkki vie. Usein sähköpostit ovat kuitenkin tekstimuotoisia, jolloin ne sisältävät linkin sijasta osoitteen sivustolle. Osoite saattaa hyvinkin sisältää luotettavan ja hyvämaineisen yrityksen nimen tai muistuttaa aidon sivuston osoitetta suuresti. Jo tämä riittää huijaamaan niitä käyttäjiä, jotka eivät tiedä, miten URL-osoitteen syntaksi muodustuu. (Pandove ym. 2010)

Onnistunut osoitehuijaus saattaa kuitenkin tepsiä myös niihin, jotka tuntevat tietotekniikkaa hyvin ja käyttävät paljon internetiä. Varsinkin kiireellä tai heikosti kohdennetulla tarkkaavaisuudella toimiva käyttäjä saattaa lukea osoitteen päässään eri tavoin kuin se on kirjoitettu. Esimerkiksi osoitteen “www.bankofthevvest.com” kiireinen tai tarkkaamaton käyttäjä lukee helposti “bank of the west”, vaikka osoitteessa on “west”-sanan alussa “w”-merkin sijaan kaksi peräkkäistä “v”-merkkiä (Dhamija ym. 2006). Näin kokenutkin käyttäjä voi päätyä täysin oikeaa sivustoa muistuttavalle huijaussivustolle. Toista merkkiä muistuttavien merkkien lisäksi käyttäjältä saattaa jäädä lukiessa huomaamatta väärin kirjoitettu sana, koska ihminen lukee sanat kokonaisina, eikä merkki kerrallaan. Kuvio 34 on hyvä esimerkki siitä, kuinka tehokkasti aivomme tulkitsevat sekavia merkkijonoja muotoon, jonka ymmärrämme.



Kuvio 34. Aivot toimivat ajoittain niin tehokkaasti, ettemme ehdi huomata kirjoitusvirheitä tai -huijauksia. Kuvankaappaus http://www.lagag.com -sivustolta.

Tietoturvayhtiö Trusteerin arvioiden mukaan miljoonaa roskaposti- ja kalasteluviestiä kohden menee lankaan vain n. 5 vastaanottajaa. Huijaussivustolle sähköpostin kautta tai muulla tavoin päätynyt käyttäjä tulee kuitenkin huijatuksi yllättävän herkästi. Trusteerin arvioiden mukaan joka toinen käyttäjä, ja Harvardin tutkimuksen mukaan 40 prosenttia käyttäjistä ei erota aitoa sivustoa huijaussivustosta (Tietokone 2009) (Dhamija ym. 2006).

5.4 Web-sivustojen huijaustekniikat

Tämän osion sisältö perustuu Harvardissa tehtyyn Why Phishing Works -tutkimuksen yhteenvetoon (Dhamija ym. 2006).

5.4.1 Turvallisuuden arviointi

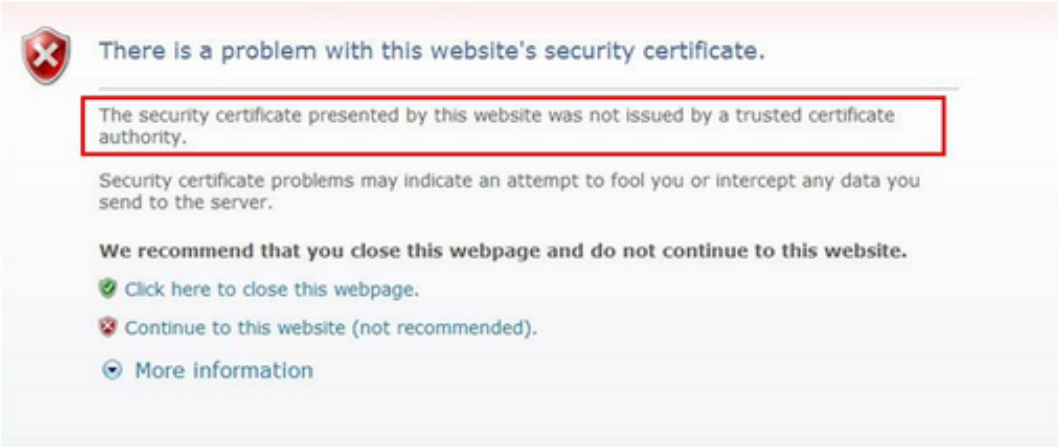
Käyttäjien tietämys sivustojen turvallisuuden ilmaisimista viiteen eri ryhmään.

- Tietämättömimmät arvioivat sivuston luotettavuutta ainoastaan sisällön perusteella
- Seuraava ryhmä arvioi sivuston luotettavuutta sisällön ja osoitteen perusteella
- Kolmas ryhmä toimii kuten edellinen, mutta luottaa sivustoon vain, jos osoitteessa on “https://”-alku
- Neljäs ryhmä toimii kuten edellinen, mutta arvioi luotettavuutta myös riippulukkoikonin perusteella
- Valveutunein ryhmä toimii kuten edellinen, mutta arvioi luotettavuutta myös varmenteiden perusteella

5.4.2 Kuinka käyttäjiä huijataan

Sisältöön on mahdollista tehdä muutoksia tavallisilla html- ja css-tekniikoilla. Sisällön perusteella turvallisuutta arvioivia on siis mahdollista huijata tavallisilla www-tekniikoilla. Toisen ryhmän huijaamista voidaan yrittää esimerkiksi valitsemalla sivuston URL-osoite, kuten Sähköpostien huijaustekniikat-osiossa esiteltiin. Suojatun SSL-yhteyden luominen sivustolle on täysin mahdollista kenelle tahansa web-kehittäjälle. SSL perustuu varmenteisiin, joilla sivusto todistaa olevansa se taho, joksi se itseään väittää. Varmeinteita myöntävät luotettavat yritykset (engl. Certificate Authority, CA), jotka takaavat varmenteen hakijan identiteetin. Selainvalmistajat puolestaan pitävät listaa luotetuista varmenteiden myöntäjistä. Mikäli sivuston varmenteen myöntäjää ei löydy selaimen tiedoista, ilmoittaa selain siitä käyttäjälle,

kuten kuviossa 35.



Kuvio 35. Selain varoittaa mikäli varmenteen myöntäjää ei löydy sen rekisteristä. Kuvankaappaus Internet Explorer -selaimesta.

Pelkkä “https://”-alku osoitteessa ei siis riitä varmentamaan sivuston luotettavuutta. Pelkästään riippulukko-ikoneihin luottaminenkaan ei ole turvallista. Lukon kuva voidaan laittaa tavallisilla www-tekniikoilla osaksi sivuston sisältöä tai selaimen faviconiksi. Sivuston sisältö voidaan myös rakentaa niin, että se näyttäisi olevan osa selainta, jolloin käyttäjä luulee selaimen kertovan sivuston olevan turvallinen. Harvardin tutkimuksessa ryhmien neljä ja viisi käyttäjät menestyivät aitojen ja huijaussivustoiden tunnistamisessa parhaiten. Kuitenkin parhaiten toteutettu huijaussivusto vakuutti 90 prosenttia kokeeseen osallistujista. Kuvion 36 taulukko esittelee Harvardin tutkimuksen yhteenvedon. Ensimmäinen sarake kertoo, mikä sivusto oli kyseessä, toinen oliko se aito (engl. Real) vai huijaussivusto (engl. Spoof). Kolmas sarake kertoo, mitä turvallisuuden osoittimia tai huijaustaktiikoita sivustolla käytettiin. Neljäs ja viides sarake kertovat, kuinka moni oli oikeassa sivuston aitoudesta ja kuinka moni väärässä.

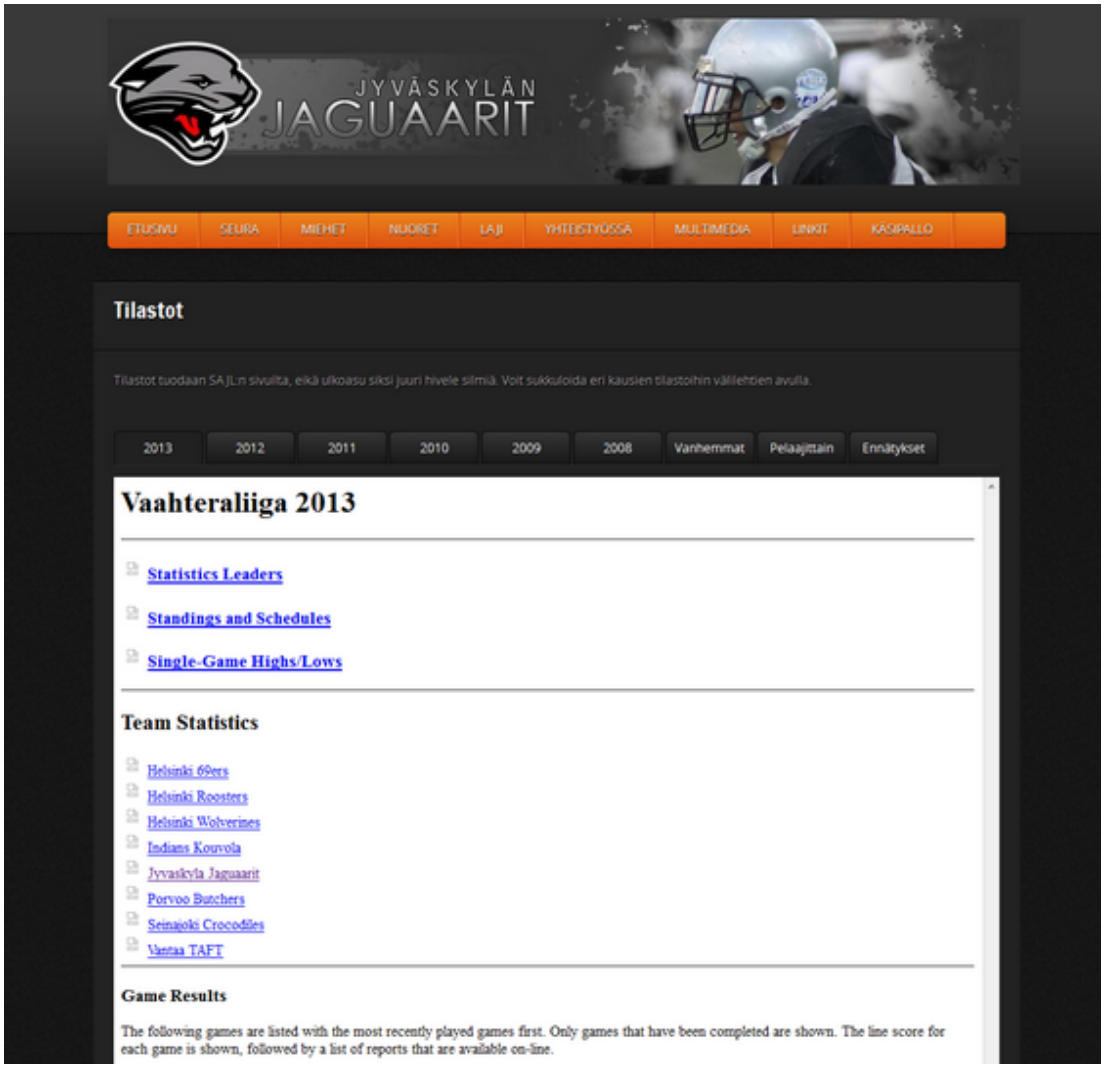
Website	Real or Spoof	Phishing or Security Tactic Used (Partial List)	% Right (avg conf)	% Wrong (avg conf)
Bank Of the West	Spoof	URL (bankofthevvest.com), padlock in content, Verisign logo and certificate validation seal, consumer alert warning	9 (3.0)	91 (4.2)
PayPal	Spoof	Uses Mozilla XML User Interface Language (XUL) to simulate browser chrome w/ fake address bar, status bar and SSL indicators	18 (3.0)	81 (4.5)
Etrade	Real	3rd party URL (etrade.everypath.com), SSL, simple design, no graphics for mobile users	23 (4.6)	77 (4.2)
PayPal	Spoof	URL (paypal-signin03.com), padlock in content	41 (4.0)	59 (3.7)
PayPal	Spoof	URL (IP address), padlock in content	41 (3.9)	59 (4.5)
Capital One	Real	3rd party URL (cib.ibanking-services.com), SSL, dedicated login page, simple design	50 (3.9)	50 (3.5)
Paypal	Spoof	Screenshot of legitimate SSL protected Paypal page within a rogue webpage	50 (4.7)	50 (4.3)
Ameritrade	Spoof	URL (ameritrading.net)	50 (4.2)	50 (3.9)
Bank of America	Spoof	Rogue popup window on top of legitimate BOFA homepage, padlock in content	64 (4.2)	36 (4.4)
Bank Of The West	Spoof	URL (IP address), urgent anti-fraud warnings (requests large amount of personal data)	68 (4.8)	32 (4.4)
USBank	Spoof	URL (IP address), padlock in content, security warnings, identity verification (requests large amount of personal data)	68 (4.1)	32 (4.3)
Ebay	Spoof	URL (IP address), account verification (requests large amount of personal data)	68 (4.4)	32 (4.0)
Yahoo	Spoof	URL (center.yahoo-security.net), account verification (requests large amount of personal data)	77 (3.0)	23 (4.2)
NCUA	Spoof	URL (IP address), padlock in content, account verification (requests large amount of personal data)	82 (4.5)	18 (4.3)
Ebay	Real	SSL protected login page, TRUSTe logo	86 (4.4)	14 (4.0)
Bank Of America	Real	Login page on non-SSL homepage, padlock in content	86 (4.4)	14 (3.3)
Tele-Bears (Student Accounts)	Real	SSL protected login page	91 (4.7)	9 (4.5)
PayPal	Real	Login page on non-SSL homepage, padlock in content	91 (4.6)	9 (3.0)
Bank One	Real	Login page on non-SSL homepage, padlock in content	100 (4.0)	0 (N/A)

Table 2: Security or spoofing strategy employed by each site (spoof sites shown with white background, real sites gray).

Kuvio 36. Harvardin tutkimus osoitti, että taitavasti tehtyä huijaussivustoa on vaikea erottaa aidosta. Kuvion lähde: (Dhamija ym. 2006).

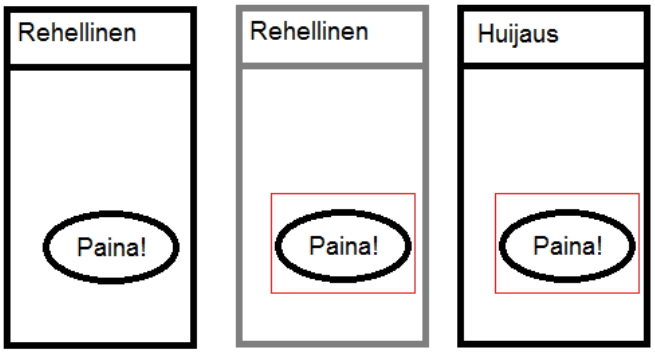
5.4.3 Kehykset ja clickjacking

HTML-kielen <iframe> -ominaisuus mahdollistaa verkkosivun upottamisen osaksi toista verkkosivua (w3school.com). Oikeassa käyttötarkoituksessa tekniikka on kätevä ja sillä voidaan mm. vähentää päällekkäisen työn määrää. Kuviosta 37 käy ilmi esimerkki, missä amerikkalaisen jalkapallon Vaahteraliigassa viikottain päivittyvät pelaajatilastot upotetaan Jyväskylän seudun Jaguaarien kotisivuille suoraan lajiliiton sivuilta. Seuran sivuston vapaaehtoisen ylläpitäjän ei näin tarvitse tehdä viikoittain päivitysurakkaa, vaan riittää, että tilastojen päivitys hoidetaan kertaalleen lajiliiton palkatun työntekijän toimesta.



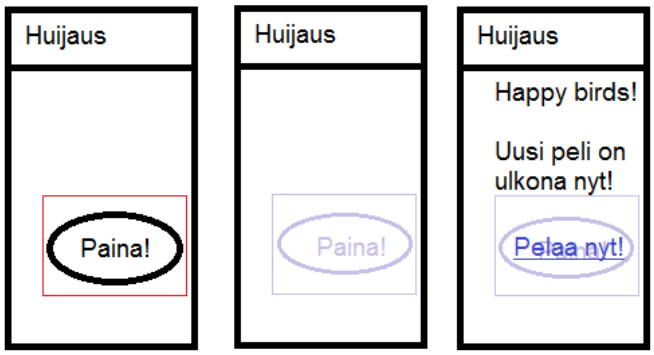
Kuvio 37. Jyväskylän seudun Jaguaarit ry:n kotisivujen tilasto-sivu. Kuvankaappaus osoitteesta: http://jaguaarit.com/index/miehet/tilastot/. Poimittu 28.7.2013.

Huijareille kehystekniikka tarjoaa kuitenkin lisää mahdollisuuksia. Ne mahdollistavat muiden, luotettavien verkkosivustojen, käytön osana oman huijaussivuston rakentamista. Huijari voi myös rajata kehyksen siten, että upotetusta sivusta näkyy vain pieni osa – esimerkiksi painike. Kuvio 38 havainnollistaa, miten painike näyttää tällöin kuuluvan huijaussivustolle, mutta sen painaminen käynnistää toiminnon toisella sivustolla (Assemblix 2008).



Kuvio 38. Kehyksillä voidaan rajata tietty osa luotettavasta sivustosta ja upottaa se osaksi huijaussivustoa. Muokattu lähteestä: (Assemblix 2008).

Kun kehystekniikkaan yhdistetään tyylitiedostojen tarjoama mahdollisuus tehdä elementeistä läpinäkyviä, voidaan toisella sivustolla olevan painikkeen sisältämä kehys muuttaa läpinäkyväksi ja sijoittaa sen alle esimerkiksi jokin houkuttelevan näköinen klikattava painikke tai linkki, kuten kuviossa 39 on tehty (Assemblix 2008).



Kuvio 39. Huijaussivustolle siirretty kehys voidaan vielä muuttaa näkymättömäksi ja sen alle voidaan laittaa houkuttelevalta vaikuttava linkki. Muokattu lähteestä: (Assemblix 2008).

Huijauksen tehoa voidaan pahentaa entisestään esimerkiksi JavaScriptiä käyttämällä. Läpinäkyvä elementti voidaan laittaa seuraamaan hiirtä, jolloin klikkaus osuu siihen varmasti. JavaScriptillä voi myös luoda harmittoman kohteen, joka katoaa hetkeksi klikattaessa, läpinäkyvän kehyksen päälle.

Tavallisimpia tekniikan sovelluskohteita ovat olleet kameran asetusten muuttaminen Flash playerin kautta sekä tietojen ja pääsylupien antaminen huijarien Facebook-sovelluksille. Kuvioissa 40 ja 41 on esitetty, miten kehyksiä ja läpinäkyvyyttä yhdistelemällä käyttäjä huija-

taan antamaan Facebook-sovellukselle pääsy käyttäjän tietoihin (ZDNet 2010).

Kuvio 40. Käyttäjä näkee yllä olevan linkin. Kuvankaappaus lähteestä: (ZDNet 2010).

Kuvio 41. Mutta painaa todellisuudessa jotakin aivan muuta. Kuvankaappaus lähteestä: (ZDNet 2010).

5.5 Haittaohjelmat

Osion sisältö perustuu Cryptography and Network Security -kirjan viidenteen painokseen (Stalling, 2011, luku 21).

Käyttäjä voidaan yrittää saada asentamaan koneelleen sähköpostin liitetiedostona tai huijaussivustolta ladattavissa oleva haittaohjelma. Käyttäjä luulee asentavansa koneelle jonkin hyödyllisen ohjelman tai päivityksen, mutta päästääkin haittaohjelman tietokoneelleen, kuten troijalaiset päästivät puuhevosen muuriensa ohitse. Haittaohjelmista tunnetuimpia ovat

virukset ja madot, jotka pyrkivät yleensä käyttäjän koneen sekoittamiseen. On kuitenkin olemassa myös muunlaisia haittaohjelmia, joista alla on esitelty yleisimpiä.

Takaovi on ohjelma, joka sallii vieraan pääsyn tietokoneelle ohittaen normaalit tietoturvamekanismit. Takaovi on yleensä sisäänrakennettuna hyödylliseltä vaikuttavaan ohjelmaan, vaikka vain kiinteiden salasanojen muodossa. Tunkeutuja pääsee näin käyttäjän koneelle ja käsiksi esimerkiksi tiedostoihin ja selaimen muistiin tallennettuihin tietoihin, kuten salasanoihin. Myös käyttäjän kamera on mahdollista ottaa haltuun ja käyttää sitä vakoiluun.

Rootkit on haittaohjelma, jonka asentaminen antaa pääsyn, eli avaa takaoven tunkeutujalle. Rootkit eroaa edellisestä siinä, että takaovi on siis yleensä asennettuna valmiiksi johonkin muuhun ohjelmaan, kun taas rootkit on oma ohjelmansa, joka avaa pääsyn koneelle.

Vakoiluohjelma on ohjelma, joka kerää tietoa, kuten vierailtujen sivustojen osoitteita tai luottokorttinumeroita, ja lähettää ne isännälleen.

Mainosohjelma on ohjelma, joka näyttää mainoksia tietokoneen näytöllä. Tällaiset ohjelmat asentuvat yleensä muiden ohjelmien mukana, tai tietoturva-aukkojen kautta esimerkiksi websivulta. Ohjelman tarkoitus on kerätä rahaa isännälleen, joka saa tietyn summan näytettyjen mainosten määrän mukaan. Nämä ohjelmat ottavat myös yhteyden isäntäkoneeseensa, joten ne voidaan luokitella vakoiluohjelmiksi.

Kiristysohjelma on ohjelma, joka estää tietokoneen käytön esimerkiksi poliisin nimissä väittäen tietokoneen sisältävän esimerkiksi lapsipornografiaa. Lukituksen avatakseen tulisi maksaa sakko kiristäjän tilille (Poliisi, CERT-FI, F-Secure 2013).

5.6 Uudet ympäristöt ja tekniikat luovat uusia mahdollisuuksia myös huijareille

Internet ja sen käyttö muuttuu niin nopeasti, että käyttäjille tulee usein eteen uusia asioita ja ympäristöjä. Käyttäjä ei osaa käyttää aina heti uutta ympäristöä, eikä tämän vuoksi tiedä, mikä on turvallista ja mikä ei. Esimerkiksi Facebook levisi Suomeen nopeasti vuoden 2006 jälkeen ja vuonna 2011 suomalaisia Facebook-käyttäjiä arvioitiin olevan jo 1,7 miljoonaa. (Pönkä 2011) Kaikki käyttäjät tuskin ymmärtävät ainakaan aluksi, ettei Facebook vastaa kaikista sen sovelluksista, vaan kuka tahansa voi tuottaa palveluun sovelluksen, jolle ei kannata antaa tietojaan.

Trend Micro (2013) ja F-Secure (2013) ovat tehneet tutkimuksia, joiden mukaan mobiilihaittaohjelmien määrä on tällä hetkellä rajussa kasvussa. Marketvision vuonna 2012 tekemän tutkimuksen mukaan (Tietokone 2012) joka toinen Suomessa myyty puhelin oli älypuhelin. Kaikki käyttäjät eivät varmasti ole vielä ajantasalla sen suhteen, mikä puhelimen käytössä on turvallista ja mikä ei. Veracoden tutkimusten mukaan peräti 91 prosenttia sovelluksista kerää sovelluksen toimimisen kannalta tarpeettomia tietoa käyttäjistään (Veracode 2013). Vakoilusovelluksen saastuttaman mobiililaitteen käyttäminen yrityksen verkossa vaarantaa puolestaan yrityksen tietoturvaa.

Myös kielenkäännösohjelmat kehittyvät jatkuvasti, jolloin uskottavia Suomen kielisiä huijausyrityksiäkin tullee tulevaisuudessa enemmän (Tambouratzis ym. 2013).

Uudet mahdollisuudet ja tekniikat luovat siis koko ajan uusia mahdollisuuksia, joten vanhoista menetelmistä valistaminen ei yksin riitä vähentämään huijattuksi tulevien määrää.

6 Johtopäätökset

Ihmiset eivät lue läpi tarkasti kaikkea internetsivuston sisältöjä vaan selailevat ja silmäilevät niitä. Ihminen arvioi aikaisemmin opittujen tietojensa ja kokemustensa perusteella, mistä ja miten olennaisia asioita tulisi etsiä ja valikoi tarjolla olevista havainnoista mielestään olennaisen tiedon. Tämän vuoksi sivustoilla ei kannata poiketa liian radikaalisti vakiintuneista käytänteistä. Ihmiset ovat tottuneet käyttämään internetiä kiireessä. Virhevalinnoista ei ole tavallisesti paljoa haittaa ja ihminen valitsee usein ensimmäisen kelvolliselta vaikuttavan vaihtoehdon. Käyttäjiä ei myöskään kiinnosta, miten asioiden, kuten suojatun internetyhteyden, tulisi todellisuudessa toimia. Jokin kerran toimivaksi todettu tapa, jolla käyttämisestä suoriudutaan, riittää. Olennainen osa havaitsemisprosessia on myös tarkkaavaisuus, jonka suuntautumiseen on mahdollista vaikuttaa ärsykekynnyksen ylittävällä virikkeellä.

Ihmisten internetkäyttötottumusten, kiireen ja huolimattomuuden vuoksi voi olla hyvin mahdollista, että kokeneempikin käyttäjä joutuu huijauksen uhriksi. Tarkkaavaisuuden ja huomion ohjaamseen voidaan käyttää hahmolakeja, tiedon hierarkisoimista ja sisällön jäsentelyä, tilaan ja aikaan liittyviä vihjeitä, tuttuja metaforia, ikkunointia, värejä, liikettä ja erilaisia varoitustekniikoita. Tämän perusteella vaikuttaisi, että käyttäjän tarkkaavaisuus on mahdollista saada ohjattua pois esimerkiksi osoiteriviltä, joka paljastaisi sivuston epäaidoksi.

Stanfordin tutkimuksessa vain 8,8 prosenttia kommenteista, joissa arvioitiin sivustojen luotettavuutta, mainittiin verkkosivuston ylläpitäjän todellisen identiteetin vaikuttavan arvioon. Harvardin tutkimuksen mukaan käyttäjien tietämys sivustojen turvallisuuden ilmaisimista jakautuu viiteen eri ryhmään.

- Ensimmäinen ryhmä arvioi sivuston luotettavuutta ainoastaan sisällön perusteella
- Toinen ryhmä arvioi sivuston luotettavuutta sisällön ja osoitteen perusteella
- Kolmas ryhmä toimii kuten edellinen, mutta luottaa sivustoon vain, jos osoitteessa on “https://”-alku
- Neljäs ryhmä toimii kuten edellinen, mutta arvioi luotettavuutta myös riippulukkoikonin perusteella
- Viides ryhmä toimii kuten edellinen, mutta arvioi luotettavuutta myös varmenteiden perusteella

Tutkimuksen perusteella vaikuttaisi, että ensimmäisen käyttäjäryhmän huijaamiseen riittää

suurella todennäköisyydellä kopio aidosta sivustosta tai taitavasti rakennettu uusi huijaussivusto. Sivuston ulkoasusta, värimaailmasta, tekstisisällöstä sekä visuaalisesta rakenteesta ja hierarkista voidaan luoda käyttäjiä miellyttävä ja vakuuttava kokonaisuus. Lisäksi houkuttelevuutta valita kyseinen sivusto voi lisätä esimerkiksi huima avajaistarjous, joka selittää myös sen miksi käyttäjä ei ole kuullut aikaisemmin yrityksestä. Illuusiota sivuston ja yrityksen hyvästä luotettavuudesta voidaan luoda myös tekaistuilla ulkopuolisilla suosituksilla, työntekijäesittelyillä sekä yhteystiedoilla, jotka voivat antaa hyvän kuvan myös asiakaspalvelun saatavuudesta. Myös sivustotyypillä on väliä.

Toisen ryhmän huijaamista voidaan yrittää valitsemalla sivuston URL-osoite niin, että sen huomaa vain tarkkaavainen käyttäjä. Kolmannen ryhmän käyttäjien huijaaminen on jo vaikeampaa, sillä selaimet varoittavat käyttäjää, mikäli varmenteen myöntäjä ei löydy niiden rekisteristä. Lienee mahdollista, että huijaus saattaa varoituksesta huolimatta toimia, mikäli käyttäjä ei tunne varmenteiden merkitystä ja on törmännyt aikaisemmin turhiin varoituksiin. Ryhmän neljä käyttäjiä voidaan pyrkiä huijaamaan samoin ja lisäämällä vielä riippulukkoikoneita osaksi sivuston sisältöä. Mikäli rikolliset onnistuvat saamaan takauksen identiteetistään joltakin varmenteita myöntävältä yritykseltä, voi huijaussivuston erottaminen oikeasta olla mahdoton tehtävä kenelle tahansa. Lisäksi käyttäjiä voidaan tekosyyhyn vedoten houkutella sivustolle tai pyytää luovuttamaan rahaa ja tietojaan tai pyytää asentamaan, jokin haittaohjelma koneelle.

Tutkimukset ovat siis osoittaneet, että käyttäjien tiedot turvallisuuden ilmaisimista ovat puutteelliset ja arvio sivuston luotettavuudesta tehdään monesti turvallisuuden kannalta merkityksettömien tekijöiden perusteella. Kun yhtälöön lisätään ihmisten tyypilliset internetin käyttötavat, kiire ja huolimattomuus, on pitkälti vastattu johdannossa esitettyyn tutkimuskysymykseen “Miten joku voi olla niin tyhmä, että joutuu huijauksen kohteeksi?” Tutkimukset osoittavat mielestäni myös sen, että kysymyksen sävy on huijauksen uhreja kohtaan turhan ylimielinen, sillä parhaiten toteutettu huijaussivusto onnistui huijaamaan jopa 90 prosenttia koehenkilöistä. Meidän suomalaisten asennetta ja kysymyksen ylimielistä sävyä selittänee kuitenkin huijaussähköpostien käännösten heikko laatu. Olisi mielenkiintoista tietää, arvioivatko suomalaiset suomenkielisten verkkosivujen uskottavuutta ja turvallisuuden ilmaisimia samoin kuin englantia äidinkielenään käyttävät Stanfordin ja Harvardin tutkimuksissa. Jatkuvasti kehittyvät käännöstekniikat ovat myös huijareiden käytössä, jonka vuoksi aihe saattaa olla tulevaisuudessa erittäin relevantti suomalaisten kannalta. Entä pystytäänkö esimerkiksi kuvalla ihmisen kasvoista tai punaista huomioväriä käyttämällä todella kaappaamaan käyt-

täjän huomio siinä määrin, että tarkkaavaisuus ohjautuu pois turvallisuuden ilmaisimista.

Kysymykset siitä, miten selainten tulisi ilmoittaa käyttäjälle epäluotettavasta varmenteesta, läpinäkyvästä elementistä tai kehyksestä, käyttäjää turhauttamatta, ovat jatkuvasti ajankohtaisia, koska uusia ympäristöjä ja huijauksia helpottavia tekniikoita tulee jatkuvasti lisää. Erittäin mielenkiintoisia tutkimuskysymyksiä olisivat mm. se, että millä perusteella käyttäjät arviovat kolmansien osapuolten internet- ja mobiilisovellusten luotettavuutta, tulisiko alustasivustojen ja mobiilialustojen ottaa enemmän kantaa ja vastuuta sovelluksille myönnettäviin pääsyoikeuksista, ja millä tekniikoilla tietoa voitaisiin esittää käyttäjille haitallisista sovelluksista.

Lähteet

Assemblix, Sani I., 2008 *Clickjacking varastaa hiiresi*. Saatavilla WWW-muodossa <URL: http://assemblix.net/2008/10/14/clickjacking-varastaa-hiiresi>. Viitattu 20.11.2013.

Beaird J., 2007 *The Principles of Beautiful Web Design*. Australia: Sitepoint Pty. Ltd.

Dhamija R., Tygar J.D., Hearst M., 2006 *Why Phishing Works*. Harvard University.

Dunn Cavelty M., 2010 *The Reality and Future of Cyberwar*. Parliamentary Brief, 30th March 2010.

Gervasio A., 2009 *Fundamental Design Princibles for Web Page Layout - The Golden Ratio law of propotion*. Saatavilla WWW-muodossa <URL: http://www.devarticles.com/c/a/Web-Style-Sheets/Fundamental-Design-P Viitattu 4.12.2013.

F-Secure 2013 *Mobile Threat Report - July-September 2013*. Saatavilla WWW-muodossa <URL: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_ Viitattu 20.11.2013.

Fogg B.J., Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, John Shon, Preeti Swani, Marissa Treinen, 2002 *What Makes A Web Site Credible? A Report on a Large Quantitative Study*. Stanford University.

Fogg B.J. ym., 2002 *Stanford Guidelines for Web Credibility - How can you boost your web site's credibility?*. Saatavilla WWW-muodossa <URL: http://credibility.stanford.edu/guidelines/ >. Viitattu 20.11.2013. Stanford University.

Hadnagy C., 2011 *Social Engineering: The Art of Human Hacking* . Indianapolis: Wiley

Publishing.

Helpa, 2007 *Värien merkitys*. Saatavilla WWW-muodossa <URL: http://verkkohelpa.edu.hel.fi/varien_merkitys.pdf>. Viitattu 20.11.2013. Helsingin palvelualojen oppilaitos.

Kettula A., 2003 *Käyttäjän tarkkaavaisuuden ohjaaminen*. Saatavilla WWW-muodossa <URL: http://www.soberit.hut.fi/T-121/T-121.200/suomi/syksy2003/essee
Viitattu 20.11.2013. Teknillinen korkeakoulu, Ohjelmistoliiketoiminnan ja -tuotannon laboratorio.

Kokkonen A., 2005 *Visuaalisen havainnoinnin huomioiminen käyttöliittymäsuunnittelussa*. Saatavilla WWW-muodossa <URL: http://www.soberit.hut.fi/T-121/T-121.200/suomi/syksy2004/essee2004/
Viitattu 20.11.2013. Teknillinen korkeakoulu, Ohjelmistoliiketoiminnan ja -tuotannon laboratorio.

Krug S., 2006 *Älä pakota minua ajattelemaan*. Helsinki: Readme.fi.

Laine A., 2004 *Hahmolait käytettävyyden parantajina*. Saatavilla WWW-muodossa <URL: http://www.mit.jyu.fi/opetus/opinnayte/LuK/Hahmolait/>. Viitattu 20.11.2013. Jyväskylän yliopisto, Tietotekniikan laitos.

Lee Y, Kozar K.A., 2005 *Investigating the effect of website quality on e-business success: an analytic hierarchy process (AHP) approach*. University of Kansas and University of Colorado.

Litan, A., 2004 *Phishing Attack Victims Likely Targets for Identity Theft*. Gartner Research. Saatavilla WWW-muodossa <URL: https://www.gartner.com/doc/431660>. Viitattu 4.12.2013.

Lehto M., 2013 *Kybermaailman ilmiöitä ja määrittelyitä V. 3.0*. Jyväskylän yliopisto, Tietotekniikan laitos.

Neisser U., 1976 *Cognition and Reality: Principles and Implications of Cognitive Psychology*. WH Freeman.

Nielsen J., 2000 *WWW-suunnittelu 2000*. Helsinki: Edita.

Pandove K., Jindal A., Kumar R., 2010 *Email Spoofing*. International Journal of Computer Applications (0975 – 8887) Volume 5– No.1, August 2010.

Piaget J., 1929 *The Child's Conception of the World*. New York: Harcourt, Brace Jovanovich.

Poliisi, CERT-FI, F-Secure 2013 *Look out for ransomware*. Saatavilla WWW-muodossa <URL: http://www.ransomware.fi/>. Viitattu 20.11.2013.

Pönkä H, 2011 *Facebookissa ei ole 2 miljoonaa suomalaista. Paljonko sitten?*. Saatavilla WWW-muodossa <URL: http://harto.wordpress.com/2011/07/22/facebookissa-ei-ole-2-miljoona Viitattu 20.11.2013.

Symantec Corporation, 2012 *Norton Cybercrime Report 2012*. Saatavilla WWW-muodossa <URL: http://us.norton.com/cybercrimereporti/>. Viitattu 20.11.2013.

Shinder D., 2002 *Scene of the Cybercrime* . Rockland MA: Syngress Publishing.

Sinkkonen I., Kuoppala H., Parkkinen J., Vastamäki R., 2002 *Käytettävyyden psykologia*. Helsinki: Edita.

Stalling W., 2011 *Cryptography and Network Security - Principles and Practise - Fifth edition*. Prentice Hall: Pearson Education .

Stavroulakis P, Stamp M. 2010 *Handbook of Information and Communication Security*. Berlin Heidelberg: Spirnger.

Sullivan S. 2011 *F-Secure webblog: Trends: From Phishing to "Man-in-the-Middle" Phishing*. Saatavilla WWW-muodossa <URL:

http://www.f-secure.com/weblog/archives/archive-092011.html>. Viitattu 20.11.2013.

Tambouratzis G., Sofianopoulos S. ,Vassiliou M. 2013 *Language-independent hybrid MT with PRESEMT*. Sofia, Bulgaria: Association for Computational Linguistics.

Tietokone-lehti 8.12.2009 *Huijaussivustot vakuuttavat joka toisen*. Saatavilla WWW-muodossa <URL: http://www.tietokone.fi/artikkeli/uutiset/huijaussivusto Viitattu 20.11.2013. Helsinki: Sanoma Magazines Finland Oy.

Tietokone-lehti 5.9.2012 *Älypuhelimet ohittivat peruskännykät Suomessa*. Saatavilla WWW-muodossa <URL: http://www.tietokone.fi/artikkeli/uutiset/alypuhelimet_ohittivat_per Viitattu 20.11.2013. Helsinki: Sanoma Magazines Finland Oy.

Trend Micro 2013 *Malicious and High-Risk Android Apps Hit 1 Million: Where Do We Go from Here?*. Saatavilla WWW-muodossa <URL: http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/ Viitattu 20.11.2013.

Veracode 2013 *Veracode Introduces Mobile Application Reputation Service*. Saatavilla WWW-muodossa <URL: http://www.veracode.com/content/view/2169/38>. Viitattu 20.11.2013.

ZDNet, Naraine R., 2010 *Researcher demos clickjacking attack on Facebook*. Saatavilla WWW-muodossa <URL: http://www.zdnet.com/blog/security/researcher-demos-clickjacking-att Viitattu 20.11.2013.

w3school.com *HTML <iframe> Tag*. Saatavilla WWW-muodossa <URL: http://www.w3schools.com/tags/tag_iframe.asp>. Viitattu 20.11.2013.