De effecten van het “groene slotje”

Christiaan Brands (S1130920), Daniël Golovko (S1125197),
Thomas van den Nieuwenhoff (S1124775), Stefano Stokman (S1128417)
Hogeschool Windesheim
Opleiding HBO-ICT IDS
Zwolle, Nederland

Samenvatting

In het heden maakt men grootschalig gebruik van het wereldwijde web voor het opzoeken van informatie. Voor het jaar 2000 was men over het algemeen niet bewust van het “groene slotje”. Met dit slotje wordt het icoon in de adresbalk van je browser bedoeld (zie Figuur 1 [1]). Met het ‘’groene slotje’’ wordt aangegeven of er van een beveiligde verbinding met een website gebruik wordt gemaakt [2].

Figuur 1. Groen slotje in browsers.

Een website is een verzameling van webpagina's op het internet (World Wide web) die tekst, afbeeldingen, video’s of ander digitaal materiaal bevatten [3], [4].

Volgens de laatste scan van Qualys op 3 december 2019 zijn bijna 70% (93.160) van de 133.937 populairste websites beveiligd door middel van een ‘’groen slotje’’ [5]. De doelstelling van dit onderzoek is om te onderzoeken of het “groene slotje” invloed heeft op de perceptie van betrouwbaarheid van een internetbron. Ook willen we mensen stil laten staan bij de daadwerkelijke effecten van het “groene slotje”; wat die nou echt doet en hoe je ermee om kunt gaan.

Dit onderzoek vindt plaats op Hogeschool Windesheim in Zwolle. De informatie voor dit onderzoek werd vergaard in de periode van 12-11-2019 tot en met 19-01-2020.

Voor dit onderzoek is er gebruik gemaakt van onderzoeksmethodieken van de HBO-i stichting [6]. De gebruikte methodieken zijn:

- Literatuuronderzoek
- Enquête
- Interview
- Data-analyse

Uit het onderzoek is gebleken dat de aanwezigheid van het ‘’groene slotje” impact heeft op het gedrag van gebruikers. In dit onderzoek hebben we een enquête uitgerold naar gebruikers en deze laten valideren met behulp van interviews. Toen de enquête werd gesloten, waren er 55 respondenten op de enquête. Ter validatie zijn er 6 interviews uitgevoerd.

Bijna 80% (60) van de respondenten geeft aan dat de aanwezigheid van het ‘’groene slotje’’ opvalt. Meer dan de helft (42) van de respondenten op de enquête geeft aan niet weg te klikken bij de afwezigheid van het slotje. 76% van de respondenten weet daadwerkelijk wat het ‘’groene slotje’’ inhoudt.

Het EV-certificaat (ook wel bekend als extended validation of uitgebreide validatie) is de hoogste vorm van SSL-beveiliging. Een dergelijk certificaat koppelt de naam van een domein, server of host aan de identiteit en locatie van een bedrijf [7], [8]. EV-certificaten zijn bedoeld om vertrouwen te wekken bij gebruikers. De websites met EV-certificaten hebben immers een proces doorlopen om hun identiteit te verifiëren [9].

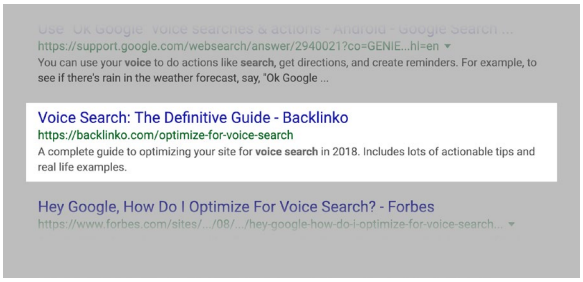
Uit de studies en daadwerkelijke functionaliteit van EV-certificaten (gedaan door onder andere Google en Mozilla) kan geconcludeerd worden dat de toegevoegde waarde van EV-certificaten steeds minder wordt. Ontwikkelaars verplaatsen het certificaat al meer naar de achtergrond. Hierdoor is er in het eerste opzicht visueel gezien geen verschil meer tussen de soorten certificaten. Door op het slotje te klikken is het EV-certificaat nog wel zichtbaar indien deze aanwezig is.

De aanwezigheid van het ‘’groene slotje’’ heeft ook economische impact. Met economische impact wordt het koopgedrag van bedrijven of consumenten bedoeld. Meerdere bronnen, waaronder het zakentijdschrift Emerce, geven de volgende redenen voor waarom het “groene slotje” belangrijk is [10], [11], [12]:

1. Het geeft meer vertrouwen en converteert beter;
2. Het kan de CTR (click-through rate; ofwel klikfrequentie) verhogen in Google resultaten;
3. Het is een ranking factor voor Google;
4. Voorkomt de ‘Niet beveiligd’ melding in Google Chrome;
5. Wet bescherming persoonsgegevens (Wbp);

Voor websitebezoekers geeft het “groene slotje” een professioneler en ‘’veiliger idee’’ tijdens het surfen op een website en stelt hen meer op hun gemak. Het converteert beter omdat des te meer bezoekers zich op hun gemak voelen op de website, des te groter de kans dat ze geneigd zijn om wat te kopen [13].

De aanwezigheid van het ‘’groene slotje’’ zorgt voor een verhoogde CTR in Google resultaten. Naast een goede opmaak van de “snippet” (zie Figuur 2 [14]) in de zoekresultaten, zijn het “groene slotje” en het zichtbare HTTPS in de URL een extra overtuiging waarom een gebruiker op jouw website moet doorklikken [13].



Figuur 2. Snippet in Google zoekresultaten.

Overigens wordt door de aanwezigheid van het ‘’groene slotje’’ de ‘’niet beveiligd’’ melding vanuit vele populaire browsers verholpen [15], [16].

De aanwezigheid van het ‘’groene slotje’’ is cruciaal vanuit het wettelijke oogpunt sinds 25 mei 2018. Het is namelijk verplicht voor bedrijven om de verzending of uitwisseling van persoonsgegevens via het internet te beveiligen.

Het aanwezig zijn van een geldig SSL-certificaat wordt dusdanig serieus genomen dat bij nalatigheid boetes kunnen oplopen tot wel 4.500 euro op persoonlijke titel [10].

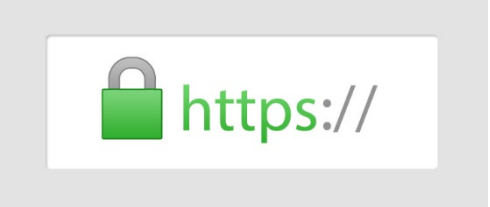
Het groene slotje heeft een grote impact op bedrijven, echter blijft het daar niet bij. Consumenten hebben net zoals bedrijven baat bij de aanwezigheid van een groen slotje op websites.

Het groene slotje voorkomt een zogenaamde man-in-the-middle (MitM) aanval. Het slotje voorkomt dat een gebruiker onbedoeld met een aanvaller verbindt. Eén van de gevolgen van deze aanval is dat de aanvaller data van het slachtoffer kan lezen [17].

Het groene slotje voorkomt niet alleen een mogelijke MitM aanval, door de aanwezigheid van het slotje is het mogelijk om typosquatting te voorkomen. Deze vorm van misbruik van het internet is gebaseerd op het feit dat mensen zich weleens vergissen bij het intypen van een websiteadres. De zogenaamde typesquatter zet een website op, waarvan het adres (domeinnaam) slechts een paar tekens verschilt van het adres van een populaire website. De bezoeker heeft niet door dat die op een malafide website zit en geeft mogelijk persoonsgegevens af aan de aanvaller [18], [19], [20], [21], [22].

Inleiding

In het heden maakt men grootschalig gebruik van het wereldwijde web voor het opzoeken van informatie. Voor het jaar 2000 was men over het algemeen niet bewust van het “groene slotje”. Met dit slotje wordt het icoon in de adresbalk van je browser bedoeld (zie Figuur 3 [1]). Met het ‘’groene slotje’’ wordt aangegeven of er van een beveiligde verbinding met een website gebruik wordt gemaakt [2].



Figuur 3. Groen slotje in browsers.

Tegenwoordig maakt men bewust (of onbewust) gebruik van het “groene slotje”. In de huidige situatie zijn ongeveer 70% (93.160) van de 133.000 populairste websites voorzien van het “groene slotje” [5]. Het “groene slotje” kan worden vertaald als de versleuteling tussen een website en cliënt. In dit onderzoekspaper wordt de impact van het “groene slotje” onderzocht. De verschillende hoeken waaruit deze impact kan worden bekeken, worden uitgewerkt in dit paper.

Context

Dit onderzoek vindt plaats op Hogeschool Windesheim in Zwolle. De informatie voor dit onderzoek wordt vergaard in de periode van 12-11-2019 tot en met 19-01-2020. De bronnen van dit onderzoek zullen voornamelijk voorzien worden door de huidige informatie op het internet en enquêtes & interviews op de campus in Zwolle.

Doelstelling

De doelstelling van dit onderzoek is om te onderzoeken of het “groene slotje” invloed heeft op de perceptie van betrouwbaarheid van een internetbron. Ook willen we personen stil laten staan bij de daadwerkelijke effecten van het “groene slotje”; wat die nou echt doet en hoe je ermee om kunt gaan.

Hoofd- en deelvragen

De hoofdvraag van dit onderzoek luidt:

> **Wat is de huidige impact van het aanwezig zijn van het “groene slotje” op websites?**

Deze hoofdvraag bestaat uit vijf deelvragen:

1. Wat is een website?
2. Wat is het “groene slotje”?
3. Wat zijn de psychologische effecten van het “groene slotje”?
4. Wat is/was de toegevoegde waarde van EV-certificaten achter het slotje?
5. Wat is de economische impact van het “groene slotje”?

In het hoofdstuk Resultaten zijn de bovenstaande deelvragen uitgewerkt volgens diverse onderzoeksmethoden. De toegepaste onderzoeksmethoden voor dit onderzoek zijn beschreven in het hoofdstuk Methodebeschrijving.

Methodebeschrijving

Tijdens dit onderzoek zijn er een aantal onderzoeksmethodieken toegepast. Deze onderzoeksmethodieken komen van de HBO-i stichting [6].

Literatuuronderzoek

Bij literatuuronderzoek worden er aan de hand van relevante sleutelwoorden gerelateerde bronnen geraadpleegd voor informatie. Binnen een bron wordt naar interessante referenties en nieuwe sleutelwoorden gezocht. Hiermee wordt het zoekproces herhaald. De sleutelwoorden worden toegepast op een aantal zoekmachines, namelijk [23]:

- Google - https://www.google.com/
- DuckDuckGo - https://duckduckgo.com/
- WindeSearch - https://mediacentrumwindesheim.nl/windesearch/
- NARCIS - https://www-narcis-nl.windesheim.idm.oclc.org/
- Nexis Uni - https://advance-lexis-com.windesheim.idm.oclc.org/

Ten slotte wordt geselecteerd welk materiaal in detail gelezen en gebruikt wordt in dit paper.

Enquête

Bij deze onderzoeksmethode wordt een gewenste doelgroep steekproefsgewijs geraadpleegd om kwantitatieve vragen te beantwoorden. Door een enquête uit te rollen naar een representatieve steekproef van deelnemers, met behulp van de juiste kanalen, wordt er op een snelle manier een beeld van een situatie of vraagstelling geschetst [24]. De verspreidingskanalen zijn in dit geval:

- #promote en #or in de Windesheim ICT Helpdesk Discord server.
- Mond-tot-mondreclame.
- Posters op de campus.

Bij een enquête hangt echter het risico erachter dat de verstrekte informatie vanuit de participant

niet betrouwbaar is. De validiteit en betrouwbaarheid van de enquête wordt gewaarborgd door onder andere een ontwerp van de vragenlijst te maken. Begrippen vanuit de literatuur worden in dit ontwerp geoperationaliseerd, er wordt gebruik gemaakt van al gevalideerde vragenlijsten, de populatie wordt bepaald, de mate van de dekking van de items wordt bepaald en er wordt een testronde (pre-test) uitgevoerd. Ook worden de omstandigheden van de afname van de vragenlijst bepaald, de lengte beperkt gehouden en anonimiteit gegarandeerd. Daarnaast is er een CAPTCHA geïmplementeerd om spam tegen te gaan. Tijdens de data-analyse wordt de gerealiseerde respons vastgesteld, de kenmerken van de respondenten in verband met representativiteit geanalyseerd en correlaties & samenhang berekend [24], [25].

De opgegeven antwoorden worden verzameld, en gebruikt om te analyseren en uiteindelijk te verwerken in dit paper.

Interview

Bij interviews wordt een gewenste doelgroep persoonlijk benaderd om meningen, gedrag, doelen, houdingen of ervaringen met een bepaald onderwerp vast te leggen. Hierbij vraagt een persoon van de onderzoeksgroep een aantal vragen aan een gekozen geïnterviewde om informatie te vergaren. Het interview wordt vastgelegd om later te analyseren en te verwerken in dit paper. Overigens zijn interviews een goede bevestigingsmethode van enquêtes.

Data-analyse

Bij de data-analyse wordt relevante data verzameld voor verdere analyse of onderzoek. Bij het onderzoeken van een vergaarde dataset (resultaten vanuit bijvoorbeeld een interview of enquête) kan er bruikbare kwantitatieve informatie over een gewenst onderwerp worden opgedaan. De verdere analyse over een vergaarde dataset wordt gedaan door een algoritme toe te passen. De dataset wordt opgesplitst in een trainingsset en een testdataset. Er wordt een werkend algoritme gezocht met de trainingsgegevens. Het Algoritme wordt gecontroleerd op betrouwbaarheid met de testgegevens [26].

Resultaten

Na de beschreven onderzoeksmethoden toegepast te hebben op de (deel)vragen van dit onderzoek, zijn er een aantal resultaten teruggekomen. Deze resultaten zijn verwerkt in dit onderdeel van de paper.

Wat is een website?

Een website is een verzameling van webpagina's op het internet die tekst, afbeeldingen, video's of ander digitaal materiaal bevatten [3], [4]. Het woord 'web' in website is afgeleid van wereldwijd web, wat verwijst naar het aanbieden van informatie over het internet [27]. Iedere website wordt beheerd door een persoon of organisatie [4].

Omdat webpagina en website verwijzen naar verwante functionaliteiten – of misschien omdat ze allebei met "web" beginnen – is het begrijpelijk dat de twee termen soms met elkaar worden verward [28]. Er zit echter wel een groot verschil in de betekenis van de twee termen. Een webpagina is een enkel document welke online kan worden bekeken. Dit kan een pagina vol tekst, afbeeldingen of video's zijn [28]. De plaats waar webpagina's samen komen tot een geheel, is een website (vergelijkbaar met de pagina's in een boek) [28].

Wat is het "groene slotje"?

HTTP staat voor Hypertext Transfer Protocol. Dit is een protocol dat gebruikt wordt voor de communicatie tussen de web client (ook wel bekend als browser) en de webserver. [29] Het nadeel van het HTTP-protocol is dat het verkeer tussen de web client en webserver niet versleuteld is. Dit betekent dat, in theorie, iedereen kan zien wat je opvraagt en verstuurd wanneer je een website bezoekt [29], [30].

HTTPS is een andere, beveiligde, manier om data te versturen. De extra 'S' staat voor Secured. Informatie wordt namelijk versleuteld zodat alleen de verstuurder en ontvanger de informatie kunnen lezen (en geen derde partijen die kwaad willen) [30].

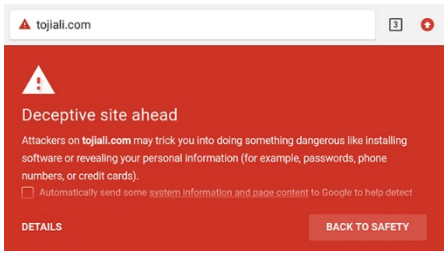
Volgens de laatste scan van Qualys op 3 december 2019 zijn bijna 70% van de 133.937

populairste websites beveiligd door middel van HTTPS [5]. Naast de versleuteling kan de echtheid van een website worden geverifieerd zodat een gebruiker er zeker van kan zijn dat de website geen kopie van criminelen of oplichters is [31]. Een HTTPS-verbinding met een website kan worden gekenmerkt door een slotje of een URL die begint met 'https://' in de adresbalk van je browser (zie Figuur 4 [32]) [31].

Figuur 4. HTTP v.s. HTTPS in browsers.

Als een website met HTTPS bereikbaar is, zegt dat niets over de inhoud van de website. Ook criminelen kunnen websites bouwen die gebruik maken van HTTPS. De beveiliging van HTTPS zegt alleen iets over de betrouwbaarheid van de verbinding met de website, niet de inhoud van de website [31]. Sommige browsers waarschuwen voor bekende valse websites middels een zwarte lijst (zie

Figuur 5 [33]) [34]. Als je een van de eerste bezoekers van een valse website bent, loop je het risico dat de website nog niet op een zwarte lijst staat. Het is dus geen watervaste methode, maar voor de meeste mensen is het erg behulpzaam [34].



Figuur 5. Misleidende site gedetecteerd.

Wat zijn de psychologische effecten van het "groene slotje"?

Bezoekers denken door de aanwezigheid van het groene slotje dat de website volledig veilig is, echter is alleen de verbinding met de website beveiligd [35] [36]. Mensen vertrouwen het slotje zodanig, dat ze niet eens meer nadenken of ze de achterliggende instantie wel vertrouwen [37].

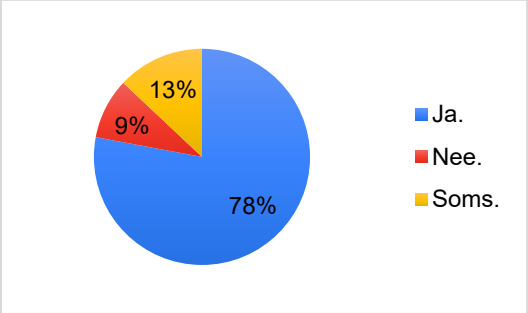
Om tot een objectief antwoord te komen voor de psychologische impact van HTTPS, moeten de vragen gesteld worden aan diverse doelgroepen. De volgende doelgroepen zijn bevraagd ten behoeve van dit onderzoek:

- Studenten
- Docenten
- Facilitaire Medewerkers
- Horeca Medewerkers

In Bijlage A zijn de enquêtevragen opgenomen.

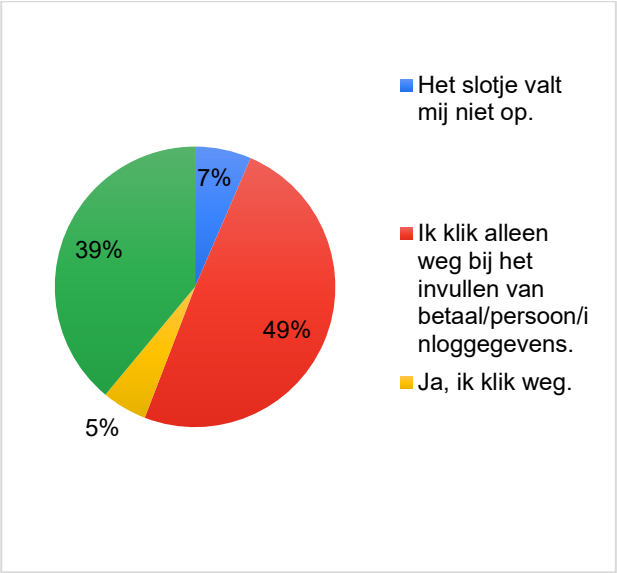
Op 16 december 2019 is de enquête gedistribueerd over de genoemde doelgroepen. Twee weken na de uitroldatum zijn er zijn 55 respondenten geweest welke antwoord hebben gegeven op de vragen. De 55 respondenten hebben de volgende antwoorden opgegeven.

In Figuur 6 wordt weergegeven wat het percentage van respondenten is welke de aanwezigheid van het slotje op websites opvalt.



Figuur 6. Valt het jou op als er een "slotje" aanwezig is op websites?

In Figuur 7 wordt weergegeven wat het percentage van respondenten is welke een website wegklikken wanneer er geen slotje aanwezig is.



Figuur 7. Wanneer er geen "groen slotje" aanwezig is, klik je dan weg?

In Figuur 8 wordt weergegeven wat het percentage van respondenten is welke wel eens inloggen op een website zonder slotje.

Figuur 8. Log je wel eens in op websites zonder "slotje"?

In Figuur 9 wordt weergegeven wat het percentage van respondenten is welke het certificaat achter het slotje analyseert.

Figuur 9. Analyseer je het certificaat achter het "groene slotje"?

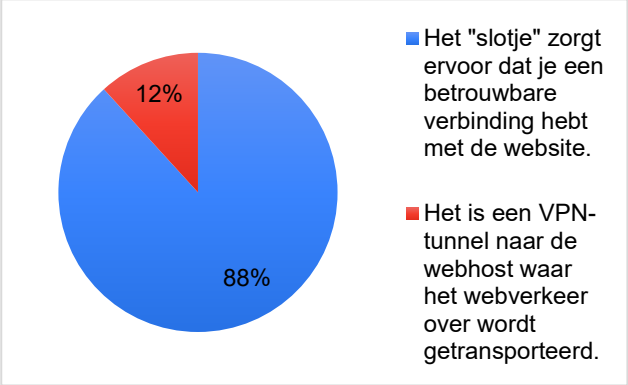
De respondenten hebben drie primaire antwoorden gegeven op de enquête vraag. 36,4% geeft als antwoord dat zij de website controleren om hun veiligheid te waarborgen. 23,6% geeft als antwoord dat zij de websites niet controleren omdat ze de websites die zij bezoeken vertrouwen. 21,8% geeft aan dat zij controleren of zij op de goede website zitten. De overige antwoorden op deze enquêtevraag waren:

- Te veel moeite om te checken.
- Ik controleer het niet om dat mijn browser dit automatisch voor mij doet.
- Weet niet waar het voor bedoeld is.
- Ik vertrouw geen enkele website, slot of niet.
- Ik besteed hier meestal weinig aandacht aan, alleen op sites waar persoonsgegevens moeten ingevuld worden let ik erop.
- Doet me niks.
- Ik controleer het om mijn gegevens te waarborgen.
- Omdat dit tegenwoordig eigenlijk niks meer uit maakt controleer ik dit alleen wanneer ik op een website van bijvoorbeeld een bank of overheidsinstantie zit.
- Het slotje zegt alleen iets over de verbinding met de server. Je kan ook zonder een groen slotje een beveiligde communicatie hebben met de server. Als

het niet zo is heb ik altijd een VPN aan staan (via professionele provider) zodat lokaal nog steeds weinig gedaan kan worden met packets die worden afgevangen.

Van de 47 respondenten die hebben aangegeven te weten wat het ''groene slotje'' inhoudt, worden de onderstaande validatieantwoorden ingestuurd.

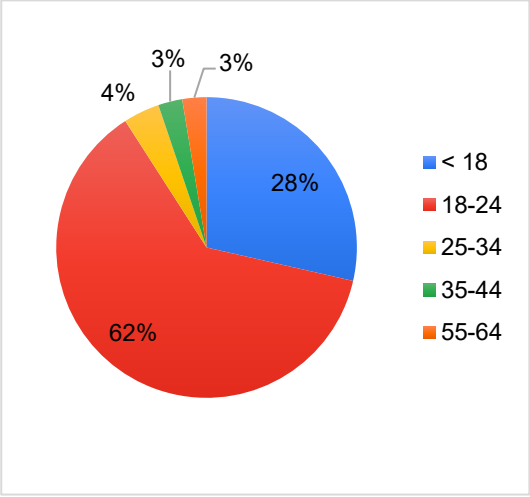
Van de totaal 55 respondenten weet 76% wat het groene slotje inhoudt.



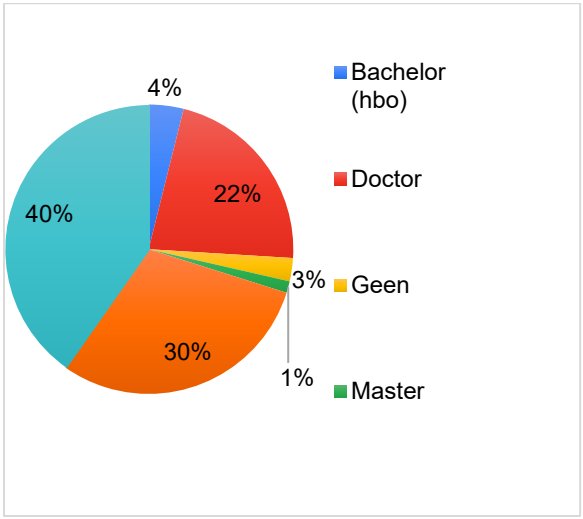
Figuur 10. Welke van de volgende opties beschrijven het "groene slotje" het beste?

Demografische gegevens respondenten

In Figuur 11 wordt weergegeven wat de leeftijdscatergoriën van de respondenten zijn.



Figuur 11. Leeftijd.



Figuur 12 Wat is jouw hoogst behaalde diploma?

Van de 55 respondenten zijn 76,4% van het mannelijke geslacht. 18,2% zijn van het vrouwelijke geslacht. 5,4% is van een overig geslacht.

Interviews

Ter validatie van de antwoorden op de enquête zijn er zes interviews uitgevoerd. De respondenten die geïnterviewd zijn geven verscheidene antwoorden op onze enquêtes. Op enkele vragen zijn soortgelijke antwoorden gegeven, sommige enquêtevragen hebben uiteenlopende antwoorden ontvangen.

De eerste enquêtevraag betrof het opvallen van het groene slotje. De respondenten gaven op deze vraag uiteenlopende antwoorden.

83% van de respondenten geeft aan dat hen opvalt wanneer er een slotje aanwezig is op de website.

De reactie van de respondenten op het ontbreken van een groen slotje verschilt.

De respondenten geven aan dat zij wegklikken afhankelijk van de soort website waar zij zich op bevinden. Er wordt voornamelijk weg geklikt wanneer er persoonsgegevens moeten worden ingevuld op de website, verder klikken alle respondenten weg wanneer zij betaalgegevens in moeten vullen op een website die niet is voorzien van een groen slotje.

33% geeft aan dat zij niet bewust zijn als zij inloggen op een website die niet is voorzien van een groen slotje. Niet elke respondent is bekend met de achterliggende certificaten van de groene slotjes, 50% geeft aan dat zij bewust zijn van de certificaten van websites.

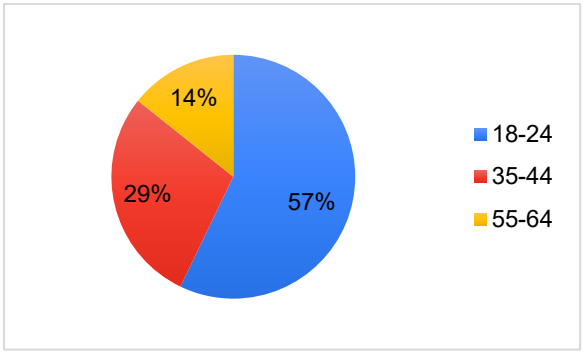
Het grootste gedeelte van de respondenten, 83%, geeft aan dat zij weten wat het slotje inhoudt. De term veiligheid wordt vaak genoemd. De respondenten geven uiteenlopende antwoorden waarom zij wel of niet controleren als de website voorzien is van een groen slotje. De antwoorden die zij gaven betroffen de volgende:

- Ik controleer niet omdat ik de website die ik bezoek vertrouw.
- Ik controleer de website om mijn veiligheid te waarborgen.
- Ik controleer het om te checken als ik op de juiste website zit.
- Ik controleer de website omdat ik nog nooit eerder de website heb bezocht.
- Ik controleer de website afhankelijk van op welk soort apparaat ik zit, (Laptop of mobiele telefoon)
- Ik controleer het eigenlijk niet.
- Ik controleer altijd de website wanneer ik moet inloggen.

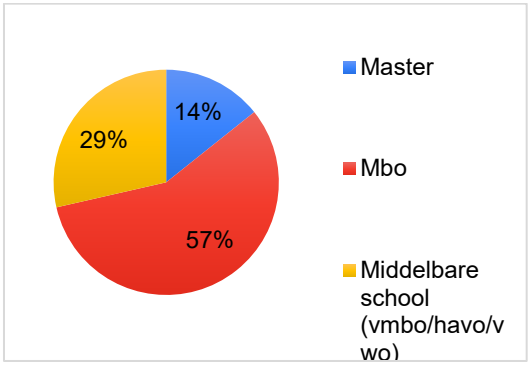
Van het viertal opties die het slotje beschrijven, kiest 83% van de respondenten voor optie C, “Het slotje” zorgt ervoor dat je een betrouwbare verbinding hebt met de website”.

Een enkele respondent kies voor optie A, “Het is een VPN-tunnel naar de webhost waar het webverkeer over wordt getransporteerd.”

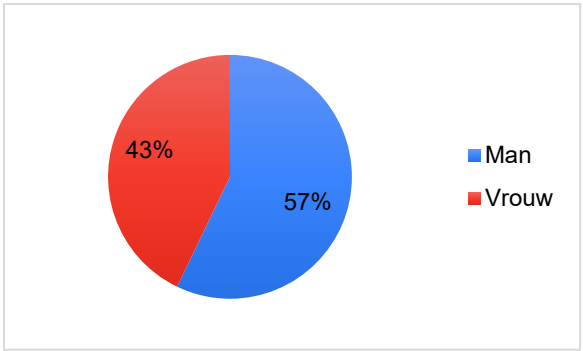
Demografische gegevens geïnterviewden



Figuur 13 Leeftijd.



Figuur 14 Wat is jouw hoogst behaalde diploma?



Figuur 15 Geslacht.

Overlap tussen de enquêtes en interviews

Tussen de enquêtes interviews zit enkele overlap, zowel de geïnterviewden en respondenten die de enquête hebben ingevuld, geven aan dat de aanwezigheid van het slotje op websites hen opvalt. Respectievelijk geven zij hier beiden “ja” op als antwoord. 78% van de respondenten antwoord met “ja”, 83% van de geïnterviewden doet dit ook.

Op de vraag: “weet jij wat het slotje inhoudt” geeft 84,5% van de respondenten als antwoord “ja”, 83% van de geïnterviewden geeft eveneens “ja” als antwoord op deze vraag.

Op de vraag “Welke van de volgende opties beschrijven het “groene slotje” het beste?” geeft 89% van de respondenten antwoord optie C. 83% van de geïnterviewden geeft als antwoord optie C.

Wat is/was de toegevoegde waarde van EV-certificaten achter het slotje?

Om deze vraag te beantwoorden wordt eerst onderzocht wat een EV-certificaat nou eigenlijk is en waarvoor dit wordt gebruikt.

Het EV-certificaat (ook wel bekend als Extended Validation of uitgebreide validatie) is de hoogste vorm van SSL-beveiliging. Een dergelijk certificaat koppelt de naam van een domein, server of host aan de identiteit en locatie van een bedrijf [38] [8].

Tot voor kort was een EV-certificaat visueel te herkennen; het stond altijd naast het slotje in de vorm van de bedrijfsnaam van de website, zoals onderstaand voorbeeld met Savvii B.V (zie figuur 16 [8]).

Figuur 16. EV-certificaat.

Dat verschilt visueel behoorlijk met een website met een “normaal” certificaat dat alleen HTTPS bevat zoals hieronder is weergegeven, hiernaast verschilt dit ook nog per browser. Zo verviel tot en met Safari 12 de hele adresbalk en was alleen de naam van het EV-certificaat zichtbaar (zie figuur 17 [8]).

Figuur 17. DV-certificaat.

Een EV-certificaat kan verstrekt worden door certificaat autoriteiten. Als bedrijven in aanmerking willen komen voor een EV-certificaat moeten ze een aanvraagprocedure doorlopen, waaronder een identiteitscontrole die bestaat uit meerdere stappen om de betrouwbaarheid te verifiëren [8].

EV-certificaten zijn bedoeld om vertrouwen te wekken bij gebruikers. De websites met EV-certificaten hebben immers een proces doorlopen om hun identiteit te verifiëren [9].

Google heeft een aantal onderzoeken uitgevoerd op grote schaal d.m.v. field onderzoek; waaronder survey’s en test personen. Hieruit bleek dat de visuele indicatoren van EV-certificaten gebruikers niet beschermen tegen phishing zoals bedoeld, maar uit geen enkele studie bleek dat de aanwezigheid van deze indicatoren compleet ineffectief waren. Er werd ook niet ontkend dat dit effectief gemaakt kon worden [39]. Echter vond Google dit wel genoeg aanleiding om de EV-indicatoren uit het zicht te laten, en is dit sinds Chrome 77 verplaatst naar info binnen het slotje [40].

Firefox heeft soortgelijke wijzigingen doorgevoerd in Firefox 70 vanwege een studie die aangaf dat de weergave van de bedrijfsnaam en het land van een website met een EV-certificaat geen extra veiligheid biedt. Als toevoeging hierop werd verwezen naar een voorbeeld: een namaakwebsite met EV-certificaat met dezelfde naam als de echte website, maar aangevraagd bij een andere certificaat autoriteit [41].

Uit de studies en daadwerkelijke functionaliteit van EV-certificaten kan geconcludeerd worden dat de toegevoegde waarde van EV-certificaten steeds minder wordt. Ontwikkelaars verplaatsen het certificaat al meer naar de achtergrond. Hierdoor is er in het eerste opzicht visueel gezien geen verschil meer tussen de soorten certificaten. Door op het slotje te klikken is het EV-certificaat nog wel zichtbaar indien deze aanwezig is.

Wat is de economische impact van het “groene slotje”?

Om deze vraag te kunnen beantwoorden wordt er gekeken naar de impact voor bedrijven en de impact voor consumenten.

Impact bedrijven

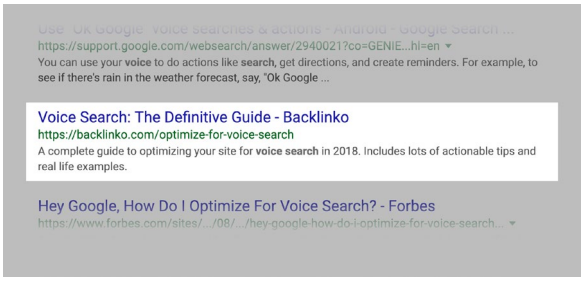
Om deze impact te weten is het handig om te kijken naar hoe het “groene slotje” kan voorkomen dat klanten verloren raken.

Meerdere bronnen, waaronder het zakentijdschrift Emerce, geven de volgende redenen voor waarom het “groene slotje” belangrijk is [10], [11], [12]:

1. Het geeft meer vertrouwen en converteert beter;
2. Het kan de CTR (click-through rate; ofwel klikfrequentie) verhogen in Google resultaten;
3. Het is een ranking factor voor Google;
4. Voorkomt de ‘Niet beveiligd’ melding in Google Chrome;
5. Wet bescherming persoonsgegevens (Wbp);

In het eerste punt wordt benoemd dat het meer vertrouwen geeft. Dit is het resultaat van betere beveiliging en helpt dus mee om het vertrouwen van websitebezoekers te winnen. Voor websitebezoekers geeft het “groene slotje” een professioneler en veiliger idee tijdens het surfen op een website en stelt hen meer op hun gemak. Het converteert beter omdat des te meer bezoekers zich op hun gemak voelen op de website, des te groter de kans dat ze geneigd zijn om wat te kopen [13].

Het tweede punt benoemd de verhoogde CTR in Google resultaten. Naast een goede opmaak van de “snippet” (zie Figuur 8 [14]) in de zoekresultaten, zijn het “groene slotje” en het zichtbare HTTPS in de URL een extra overtuiging waarom een gebruiker op jouw website moet doorklikken [13].



Figuur 18. Snippet in Google zoekresultaten.

Het derde punt benoemd dat een beveiligde website een ranking factor is voor Google [13]. John Mueller [42] (webmaster trends analist van Google) tweet op 29 januari 2019 het volgende: “We gebruiken HTTPS als een lichtgewicht rangschikkingsfactor en het hebben van HTTPS is geweldig voor gebruikers.” De impact lijkt dus beperkt te zijn: het draagt bij aan betere vindbaarheid, maar het zal geen groot verschil zijn na het overstappen naar HTTPS [10].

Het vierde punt benoemd de ‘Niet beveiligd’ melding die sinds oktober 2017 in Google Chrome wordt weergegeven. Deze melding kan websitebezoekers weerhouden om persoonlijke gegevens te delen wanneer ze worden geconfronteerd met deze melding. Wanneer dat het geval is, worden de bestedingen en aankopen van bezoekers via de website negatief beïnvloed. In november 2014 heeft GlobalSign [43] (een Certificate Authority) in Europa onderzoek gedaan naar hoe het vertrouwen van klanten en conversies verhoogt kan worden met SSL. Hieruit bleek dat 84% (5.143) van de 6.122 bezoekers afstand zou doen van een transactie als de website onveilig zou blijken te zijn. Samengevat verhoogt HTTPS niet per se de online verkoop, maar zonder wordt het verliezen van klanten door een gebrek aan vertrouwen geriskeerd [15], [16].

Het vijfde punt benoemd de wet bescherming persoonsgegevens welke sinds 25 mei 2018 niet meer geldt. Op die datum is namelijk de nieuwe algemene verordening gegevensbescherming (AVG of GDPR) van kracht gegaan [44]. Echter is de reden waarom deze wet belangrijk is nog steeds geldig. Het is namelijk verplicht voor bedrijven om de verzending of uitwisseling van persoonsgegevens via het internet te beveiligen. Dit wordt dusdanig serieus genomen dat bij nalatigheid boetes kunnen oplopen tot wel 4.500 euro op persoonlijke titel [10].

Dat klanten wantrouwig zijn bij websites zonder SSL-certificaat, blijkt ook uit het onderzoek van GlobalSign [43] uit 2014. Het blijkt namelijk dat 50% (3061) van de 6122 online shoppers bang is dat hun betalingsgegevens worden gestolen [45].

Impact consumenten

Wat de impact is voor bedrijven is nu duidelijk. Maar waarom is een beveiligde SSL-link zo belangrijk voor consumenten?

Wanneer een gebruiker naar een met HTTPS beveiligde website navigeert, is het eerste wat de browser doet verifiëren of de website waar verbinding mee wordt gemaakt de site is die het zegt dat het is. Als deze verificatie niet plaats zou vinden, zou er een man-in-the-middle (MitM) aanval plaats kunnen vinden. Zonder deze verificatie middels een certificaat, kan het zijn dat een gebruiker onbedoeld met een aanvaller verbindt. De aanvaller zou dan een beveiligde verbinding opzetten naar de echte site en zich voordoen als de gebruiker. Desondanks de beveiligde verbinding tussen gebruiker (in dit geval de aanvaller) en de website, wat zou moeten voorkomen dat een derde de data uit kan lezen, kan de aanvaller de data decrypten en vervolgens weer doorsturen naar de echte gebruiker [17].

Naast deze aanval, welke voorkomen zou kunnen worden door een up-to-date browser te gebruiken en naar het certificaat te kijken, is er ook nog een andere veel gebruikte aanval techniek. Deze techniek heet typosquatting. Deze vorm van misbruik van het internet is gebaseerd op het feit dat mensen zich weleens vergissen bij het intypen van een websiteadres. De zogenaamde typosquatter zet een website op, waarvan het adres (domeinnaam) slechts een paar tekens verschilt van het adres van een populaire website. Deze techniek wordt vaak gebruikt om bezoekers te trekken naar een pornosite of online casino om daar geld mee te verdienen. Soms wordt typosquatting gebruikt om bezoekers van een concurrent te lokken, bijvoorbeeld naar een zoekmachine, veilingsite of een onlinewinkel. Som wordt typosquatting gebruikt om mensen toegangscode of credit-cardgegevens te ontfutselen. Dan wordt de website van een populaire bank of webwinkel nagebootst. Bezoekers die een typefout maken en op de verkeerde website terechtkomen, worden verleid om hun wachtwoord of credit-cardgegevens achter te laten. Deze manier van het ontfutselen van gegevens wordt ook wel phishing genoemd. Soms worden de valse domeinnamen gebruikt om virussen, adware, spyware en dergelijke te verspreiden. Soms gaat het om een satirische site, waar de organisatie van de originele website of een persoon bespot worden [18], [19], [20], [21], [22], [46]. Tweakers rapporteerde in 2018 het volgende: “SIDN, de organisatie die zich bezighoudt met het beheer van het .nl-domein, heeft met een eigen onderzoek 451 phishingsites geïdentificeerd die zich richten op de domeinen van zorgverzekeraars. Dat doen de kwaadaardige sites met sterk gelijkende domeinnamen.” [47] SIDN zegt zelf dat hun analyse geen 100% garantie geeft dat deze sites ook echt phishing zijn, maar het is wel een goede indicatie [48].

De methoden die gebruikt worden voor deze typosquatting aanval zijn vrij simpel. Gebruik typische spelfouten: het overslaan of verwisselen van letters. Gebruik vergissingen in de naamgeving van de website: bijvoorbeeld een streepje of een punt te veel of te weinig; of maak gebruik van een afkorting in plaats van de volledige naam. Gebruik een ander toplevel domain (.com, .org, .net, .nl, etc.). Gebruik een alternatieve naam die duidelijk verschilt van de juiste site, maar toch sterk refereert naar het juiste adres [18].

Een aantal voorbeelden van typosquatting [18]:

- zeehondencentrum.nl > zeehondencreche.nl;
- whitehouse.gov > whitehouse.com; whitehouse.org;
- wikipedia.org > wikiepedia.org; wiipedia.org; ekipedia.org; wilipedia.org;
- bundesregierung.de > republicofgermany.com;
- inholland.nl > injeholland.nl;
- nintendo.nl > nentindo.nl;

Discussie

Dit onderzoek heeft de effecten van het ‘’groene slotje’’ aan de hand van de geschetste context in kaart gebracht. De functionele werking is ook in kaart gebracht. Uit de beschreven functionaliteiten van het ‘’groene slotje’’ kan een gebruiker opmaken wat het belang is.

Een website zorgt ervoor dat een eindgebruiker tekst, afbeeldingen, video’s of ander digitaal materiaal kan opvragen vanaf een browser op hun eigen systeem [3], [4].

Het ‘’groene slotje’’ zorgt ervoor dat het verkeer tussen een website/webserver en een webbrowser versleuteld is, het ‘’groene slotje’’ zegt echter niets over de inhoud van de website [30], [31]. Hieruit is te concluderen dat je in de huidige situatie in principe nooit een website volledig kunt vertrouwen. Mogelijk zou een menselijke factor alsnog kwade invloed kunnen hebben op de inhoud van de website (en de website kwaadaardig opstellen). Over het algemeen heeft iedereen met administratieve toegang tot de content van een website ongecontroleerd de macht om een website aan te passen naar wens. Als je een website benadert waarvan je compleet zeker bent dat je de enige bent met toegang (zoals in een geïsoleerd privé- of testnetwerk), is uiteraard de website hoogstwaarschijnlijk wel betrouwbaar. In een vervolgonderzoek zou het een interessante vraag kunnen zijn of er iets te implementeren is waardoor je de inhoud van een website echt kunt vertrouwen.

In dit paper is een onderzoek uitgevoerd naar de psychologische effecten van het groene slotje. Hierbij is een enquête uitgerold naar respondenten. Daarnaast zijn er 6 personen geïnterviewd. Respondenten van de interviews en enquête geven aan dat zij een veilig gevoel hebben wanneer zij zich bevinden op een website die is voorzien van een slotje. 26% van de respondenten geeft aan dat zij bewust niet wegklikken op een website die een potentieel risico vormt voor hun veiligheid.

Het niet wegklikken kan komen doordat de website voorzien is van een slotje. Dit slotje stelt de gebruikers gerust, door deze geruststelling zijn gebruikers eerder geneigd om verder te browsen op een potentieel onveilige website. Het niet wegklikken kan ook afhankelijk zijn van de soort website die de gebruiker bezoekt. Sommige geïnterviewden geven aan dat zij de website niet controleren omdat zij de website vertrouwen.

De effectiviteit van EV-certificaten is aangetast; browserontwikkelaars hebben het EV-certificaat naar de achtergrond verplaatst [40], [41]. Hierdoor is er voor gebruikers geen merkbaar verschil tussen de soorten certificaten als zij het achterliggende certificaat niet analyseren. Deze verplaatsing heeft ook geleid naar een visuele wijziging aan het slotje; het “groene” slotje is nu grijs geworden. Dit kan gezien worden als het gelijk trekken van de certificaten.

De economische impact op bedrijven uit zich waarschijnlijk in het toenemen van de omzet door een groter aantal klanten. Het “groene slotje” die bezoekers in hun browsers zien, zorgt waarschijnlijk voor meer vertrouwen tijdens het maken van betalingen of versturen van persoonsgegevens [10], [11], [12]. Het zou namelijk een professioneler en veiliger gevoel moeten geven door te weten dat de data over een beveiligde verbinding wordt gestuurd. Dit geldt onder het voorbehoud dat bezoekers het “groene slotje” kunnen vertrouwen op het aantonen van een veilige omgeving. Als dit het geval is, zouden bezoekers zich ook meer op hun gemak moeten voelen. Dit zal vervolgens voor een hogere conversie moeten zorgen. Des te meer bezoekers zich op hun gemak voelen, des te groter de kans is dat ze geneigd zijn om wat te kopen [13]. Onder het voorbehoud dat bezoekers zich laten beïnvloeden door dit veilige gevoel. Dit zijn niet de enige redenen dat bedrijven meer klanten zullen krijgen. Potentiële klanten zouden de website namelijk ook beter moeten kunnen vinden via Google. John Mueller [42], webmaster trends analist van Google, tweette op 29 januari 2019 namelijk dat HTTPS als lichtgewicht rangschikkingsfactor gebruikt wordt. Dit is onder het voorbehoud dat Google HTTPS nog steeds op dezelfde manier als rangschikkingsfactor gebruikt en dat het überhaupt als factor wordt gebruikt. Een andere economische impact voor bedrijven zal hoogst waarschijnlijk een vermindering van klanten en dus omzet zijn, wanneer er geen “groen slotje” te zien is op de website [15], [16]. Dit zou klanten af moeten schrikken, omdat bezoekers ervan weerhouden worden om persoonlijke gegevens te delen. Dit komt door de ‘Niet-beveiligd’ melding die in browsers als

Google Chrome te zien is. Uit onderzoek van GlobalSign [43] uit november 2014 bleek dat 84% van de 6.122 ondervraagde Europese bezoekers afstand zou doen van een transactie als de website onveilig zou blijken te zijn. Dit is onder het voorbehoud dat dit heden ten dage nog steeds het geval is en de melding in Chrome hetzelfde blijft. De laatste economische impact voor bedrijven zal zijn dat het verzenden of uitwisselen van persoonsgegevens zonder beveiliging veel geld gaat kosten. Dit is namelijk verboden en wordt beboet tot wel 4.500 euro [10]. Deze wet valt onder de algemene verordening gegevensbescherming (AVG) [44], welke sinds 25 mei 2018 van kracht is. Dit is onder het voorbehoud dat deze wet niet aangepast wordt [17].

Dan rest de economische impact voor consumenten nog. Zonder HTTPS-beveiliging zou het goed mogelijk zijn dat persoonsgegevens in verkeerde handen komen en gebruikt worden om geld te stelen. Zonder verificatie van een certificaat, kan het zo maar zijn dat er verbinding gemaakt wordt met een malafide server. Dit staat bekend als een man-in-the-middle (MitM) aanval. De aanvaller doet zich dan voor als de website waarmee je probeert te verbinden en ziet ondertussen al het verkeer tussen jou en de website. Dit is onder het voorbehoud dat er een aanval plaats vindt. Een tweede waarmee geld gestolen kan worden, is door een techniek genaamd typosquatting. Hierbij zet een aanvaller een website op met een domeinnaam die heel veel lijkt op de website die je probeert te bereiken. Hierbij zou het duidelijk aan het certificaat, of het ontbreken ervan, te zien moeten zijn dat het een malafide website is. Het voorbehoud is dat er naar een fout domein genavigeerd wordt [17].

Het zou interessant zijn om te weten of dit allemaal op grotere schaal ook het geval is. Er zijn bij dit onderzoek namelijk slechts 55 respondenten geweest. Wanneer het onderzoek buiten Windesheim zal worden uitgevoerd, bijvoorbeeld op landelijke schaal is het mogelijk dat de resultaten zullen verschillen. Als er uit een landelijk onderzoek blijkt dat ongeveer hetzelfde percentage personen niet wegklikken (terwijl ze wel weten wat het ‘’groene slotje’’ inhoudt), zou het mogelijk een goede optie zijn om een bewustwordingscursus aan te bieden.

Omdat gedrag van personen soms ook onbewust is, zou het voor een vervolgonderzoek ideaal zijn om observaties uit te voeren [49]. Bij een observatie wordt gedrag namelijk geanalyseerd zonder het creëren van een mogelijke bias.

Een ander interessant inzicht is dat een SSL-certificaat een website niet per definitie veilig maakt [31]. Voor een vervolgonderzoek zou het een idee kunnen zijn om uit te zoeken hoe je er het meest zeker van kunt zijn of de inhoud van een website integer is.

Literatuurlijst

[1] Unique Design, „Browser wijzigingen voor HTTP en EV SSL certificaten,” Unique Design, [Online]. Available: https://unique-design.nl/browser-wijzigingen-voor-http-en-ev-ssl-certificaten/. [Geopend 18 december 2019].

[2] Wikipedia contributors, „HTTPS,” Wikipedia, The Free Encyclopedia, 17 december 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=HTTPS&oldid=931228055. [Geopend 18 december 2019].

[3] Webbits, „Wat is een website?,” Webbits, [Online]. Available: http://www.webbits.be/website-tips-succes/articles/wat-is-een-website.cfm. [Geopend 18 december 2019].

[4] SeniorWeb, „Wat is website?,” SeniorWeb, [Online]. Available: https://www.seniorweb.nl/computerwoordenboek/w/website. [Geopend 18 december 2019].

[5] Qualys, „Qualys SSL Labs,” Qualys, 3 december 2019. [Online]. Available: https://www.ssllabs.com/ssl-pulse/. [Geopend 18 december 2019].

[6] HBO-i stichting, „Methods - ICT research methods,” HBO-i stichting, 9 februari 2018. [Online]. Available: http://ictresearchmethods.nl/index.php?title=Methods&oldid=100. [Geopend 18 december 2019].

[7] LeaderSSL, „Het verschil tussen OV en EV SSL-certificaten," LeaderSSL, [Online]. Available: https://www.leaderssl.nl/articles/233-het-verschil-tussen-ov-en-ev-ssl-certificaten. [Geopend 18 december 2019].

[8] G. Hovens, „Wat is een EV SSL-certificaat en wat zijn de voordelen?," Savvii, 21 september 2018. [Online]. Available: https://www.savvii.com/nl/blog/wat-is-een-ev-ssl-certificaat/. [Geopend 18 december 2019].

[9] DigiCert, „Extended Validation Certificate FAQ," DigiCert, [Online]. Available: https://www.digicert.com/extended-validation-ssl.htm. [Geopend 18 december 2019].

[10] P. Meijer, „Zes redenen waarom je je website van HTTP naar HTTPS moet overzetten," Emerce, 16 oktober 2017. [Online]. Available: https://www.emerce.nl/achtergrond/6-redenen-waarom-website-http-https-moet-overzetten. [Geopend 15 januari 2020].

[11] E-commerce Nation, „SSL in e-commerce: everything you always wanted to know," E-commerce Nation, 16 april 2019. [Online]. Available: https://www.ecommerce-nation.com/ssl-in-ecommerce/. [Geopend 15 januari 2020].

[12] J. Bruce, „What is an SSL certificate, and why you need an SSL Certificate for eCommerce Website?," Mageplaza, [Online]. Available: https://www.mageplaza.com/blog/ssl-certificate-for-ecommerce-website.html. [Geopend 15 januari 2020].

[13] J. Santora, „The 10 Essential SEO Ranking Factors You Need to Rank #1 in 2019," OptinMonster, 19 december 2019. [Online]. Available: https://optinmonster.com/seo-ranking-factors/. [Geopend 15 januari 2020].

[14] Backlinko, „Rich Snippets: The Complete Guide for 2019," Backlinko, [Online]. Available: https://backlinko.com/hub/seo/snippets. [Geopend 15 januari 2020].

[15] BigCommerce, „HTTPS: Why Is It Important For Ecommerce Website?," BigCommerce, [Online]. Available: https://www.bigcommerce.com/ecommerce-answers/https-what-is-it-and-what-ecommerce-merchants-need-to-know/. [Geopend 15 januari 2020].

[16] K. Bali, „EV SSL for Ecommerce Website: Why It's the Right Time to Have It?," ServerGuy, 4 november 2019. [Online]. Available: https://serverguy.com/security/ssl-for-ecommerce/. [Geopend 15 januari 2020].

[17] J. Boote, „Why should every eCommerce website have an SSL certificate?," Synopsys, 31 mei 2017. [Online]. Available: https://www.synopsys.com/blogs/software-security/ecommerce-ssl-certificate/. [Geopend 15 januari 2020].

[18] Wikipedia-bijdragers, „Typosquatting," Wikipedia, de vrije encyclopedie, 1 september 2018. [Online]. Available: https://nl.wikipedia.org/w/index.php?title=Typosquatting&oldid=52177075. [Geopend 17 januari 2020].

[19] C. Bell, „'Typosquatting': How 1 mistyped letter could lead to ID theft," Bankrate, 17 augustus 2015. [Online]. Available: https://www.bankrate.com/finance/credit/typosquatting-identity-theft.aspx. [Geopend 17 januari 2020].

[20] McAfee, „What is Typosquatting?," McAfee, 3 juli 2013. [Online]. Available: https://www.mcafee.com/blogs/consumer/what-is-typosquatting/. [Geopend 17 januari 2020].

[21] Infradata, „Onderzoek: Typosquatting nog steeds een groot risico," Infradata, 15 maart 2019. [Online]. Available: https://www.infradata.nl/nieuws-blog/typosquatting-nog-steeds-zeer-groot-risico/. [Geopend 17 januari 2020].

[22] Sophos, „Typosquatting – what happens when you mistype a website name?," Sophos, [Online]. Available: https://nakedsecurity.sophos.com/typosquatting/. [Geopend 17 januari 2020].

[23] HBO-i stichting, „Literature study,” HBO-i stichting, 9 februari 2018. [Online]. Available: http://ictresearchmethods.nl/index.php?title=Literature_study&oldid=57. [Geopend 18 december 2019].

[24] HBO-i stichting, „Survey,” HBO-i stichting, 9 februari 2018. [Online]. Available: http://ictresearchmethods.nl/index.php?title=Survey&oldid=73. [Geopend 18 december 2019].

[25] B. Swaen, "Validiteit en betrouwbaarheid in een enquête," Scribbr, 21 03 2017. [Online]. Available: https://www.scribbr.nl/onderzoeksmethoden/validiteit-en-betrouwbaarheid-een-enquete/. [Accessed 24 11 2019].

[26] HBO-i stichting, "Data analytics," HBO-i, 09 02 2018. [Online]. Available: http://ictresearchmethods.nl/Data_analytics. [Accessed 18 11 2019].

[27] webkrunch.be, "Een website, wat is dat?," webkrunch.be, [Online]. Available: https://www.webkrunch.be/wiki/website/. [Accessed 18 12 2019].

[28] WebsitePlanet.com, "Website versus webpagina – Is er een verschil?," WebsitePlanet.com, 19 01 2020. [Online]. Available: https://www.websiteplanet.com/nl/blog/website-versus-webpagina-er-een-verschil/. [Accessed 19 01 2020].

[29] VPNGids, "HTTP en HTTPS uitgelegd: een goede stap richting een veiliger internet?," VPNGids, 6 augustus 2019. [Online]. Available: https://www.vpngids.nl/veilig-internet/surfen/http-en-https-uitgelegd/. [Accessed 18 december 2019].

[30] M. Oud, „Wat is HTTPS?,” Webvalue, 23 juli 2019. [Online]. Available: https://webvalue.nl/blog/wat-is-https. [Geopend 18 december 2019].

[31] SeniorWeb, „Herken een veilige website,” SeniorWeb, 14 febrari 2019. [Online]. Available: https://www.seniorweb.nl/tip/tip-herken-een-veilige-website. [Geopend 18 december 2019].

[32] Sanskruti, „HTTPS,” Sanskruti, [Online]. Available: https://sanskruti.net/tag/https/. [Geopend 17 december 2019].

[33] T. Ali, „Deceptive site ahead,” Toji Ali. [Online]. [Geopend 17 december 2019].

[34] P. Arntz, „HTTPS: why the green padlock is not enough,” Malwarebytes, 9 may 2018. [Online]. Available: https://blog.malwarebytes.com/101/2018/05/https-why-the-green-padlock-is-not-enough/. [Geopend 18 december 2019].

[35] A. v. d. S. J. Schellevis, "Duizenden sites met groen slotje onveilig," NOS, 02 06 2018. [Online]. Available: https://nos.nl/artikel/2234720-duizenden-sites-met-groen-slotje-onveilig.html. [Accessed 24 11 2019].

[36] TNO, "IS GROEN SLOTJE IN BROWSER GARANTIE VEILIG INTERNET?," TNO, 04 06 2018. [Online]. Available: https://www.tno.nl/nl/over-tno/nieuws/2018/6/is-groen-slotje-in-browser-garantie-veilig-internet/. [Accessed 30 12 2019].

[37] C. Cimpanu, "Extended Validation (EV) Certificates Abused to Create Insanely Believable Phishing Sites," BleepingComputer, 12 12 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/extended-validation-ev-certificates-abused-to-create-insanely-believable-phishing-sites/. [Accessed 03 01 2020].

[38] LeaderSSL, "leaderssl," [Online]. Available: https://www.leaderssl.nl/articles/233-het-verschil-tussen-ov-en-ev-ssl-certificaten. [Accessed 5 1 2020].

[39] Google, "The Web's Identity Crisis Understanding: The Effectiveness of Website Idendtity Indicators," Google, 2018.

[40] Google, "EV UI Moving to Page Info," 2018. [Online]. Available:

https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/ev-to-page-info.md#ev-ui-moving-to-page-info. [Accessed 5 1 2020].

[41] J. Hofmann, "Improved Security and Privacy Indicators in Firefox 70," Mozilla, 15 10 2019. [Online]. Available: https://blog.mozilla.org/security/2019/10/15/improved-security-and-privacy-indicators-in-firefox-70/. [Accessed 2020 1 5].

[42] J. Mueller, „John on Twitter: "@krinal @Uniregistry @rustybrick ...," Twitter, 19 januari 2019. [Online]. Available: https://twitter.com/JohnMu/status/1090196646200307712. [Geopend 15 januari 2020].

[43] GlobalSign, „Increase conversions with SSL," GlobalSign, 2014.

[44] Autoriteit Persoonsgegevens, „Introductie AVG," Autoriteit Persoonsgegevens, [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/algemene-informatie-avg. [Geopend 15 januari 2020].

[45] S. Weber, „Waarom e-commerce niet om SSL heen kan," Networking4all, 31 juli 2016. [Online]. Available: https://blog.networking4all.com/2016/07/waarom-e-commerce-niet-om-ssl-heen-kan/. [Geopend 15 januari 2020].

[46] Wikipedia contributors, „Typosquatting," Wikipedia, The Free Encyclopedia, 27 september 2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Typosquatting&oldid=918285826. [Geopend 17 januari 2020].

[47] S. van Voortst, „SIDN vindt phishingsites die zich via typosquatting op zorgverzekeraars richten," Tweakers, 11 september 2018. [Online]. Available: https://tweakers.net/nieuws/143237/sidn-vindt-phishingsites-die-zich-via-typosquatting-op-zorgverzekeraars-richten.html. [Geopend 19 januari 2020].

[48] SIDN, „Cybercriminelen zetten valse websites in om zorggegevens te achterhalen," SIDN, 11 september 2018. [Online]. Available: https://www.sidn.nl/nieuws-en-blogs/cybercriminelen-zetten-valse-websites-in-om-zorggegevens-te-achterhalen. [Geopend 19 januari 2020].

[49] HBO-i instituut, "Observation," HBO-i, 09 02 2018. [Online]. Available: http://ictresearchmethods.nl/Observation. [Accessed 19 01 2020].

[50] P. Arntz, „HTTPS: why the green padlock is not enough," Malwarebytes, 9 may 2018. [Online]. Available: https://blog.malwarebytes.com/101/2018/05/https-why-the-green-padlock-is-not-enough/. [Geopend 18 december 2019].

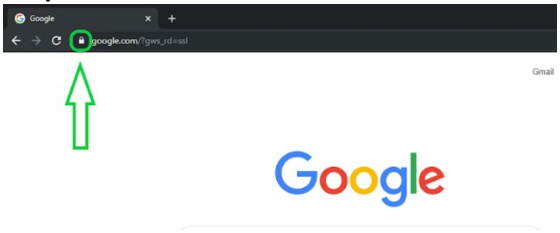
Sleutelwoorden

website betekenis; website vs webpagina; what is the browser padlock; browser; https; padlock; psychologische effecten van het groene slotje; let's encrypt trustworthyness; lock icon browser consumer; encrypted website connection why; https false security; browser green lock effects on people; https padlock society; Typosquatting; EV Certificate; What is an EV Certificate?; EV Certificate announcement chrome; EV Certificate announcement firefox; EV Certificate announcement; economisch impact groen slotje; https ecommerce; ssl ecommerce; ssl certificate compare

Bijlagen

Bijlage A

1. **Valt het jou op als er een "slotje" aanwezig is op websites?**



   a. Ja.

b. Nee.

2. **Wanneer er geen "groen slotje" aanwezig is, klik je dan weg?**
    a. Ja, ik klik weg.
    b. Ik klik alleen weg bij het invullen van betaal/persoon/inloggegevens.
    c. Nee, ik klik niet weg.
    d. Het slotje valt mij niet op.
3. **Log je wel eens in op websites zonder "slotje"?**
    a. Ja.
    b. Nee.
    c. Ik ben mij hier niet van bewust.
4. **Analyseer je het certificaat achter het "groene slotje"?**
    a. Ja, altijd.
    b. Alleen bij het invullen van betaal/persoon/inloggegevens.
    c. Incidenteel.
    d. Nee.
    e. Ik ben mij niet bewust van de certificaten van websites.
5. **Weet je wat het "slotje" inhoudt?**
    a. Ja.
    b. Nee.
6. **Waarom controleer je wel/niet of websites een "groen slotje" hebben?**
    a. Ik controleer het om zeker te weten dat ik op de goede website zit.
    b. Ik controleer het om mijn veiligheid te waarborgen.
    c. Ik controleer niet omdat ik niets te verbergen heb.
    d. Ik controleer niet omdat ik de websites die ik bezoek vertrouw.
7. **(Indien "Ja" is geantwoord op vraag 5) Welke van de volgende opties beschrijven het "groene slotje" het beste?**
    a. Het is een VPN-tunnel naar de webhost waar het webverkeer over wordt getransporteerd.
    b. Het betekent dat je een snelle verbinding hebt.
    c. Het "slotje" zorgt ervoor dat je een betrouwbare verbinding hebt met de website.
    d. Het "slotje" zorgt voor een betere weergave van de website.