Сигурност на браузъра Google Chrome

Google Chrome включва функции, които помагат на потребителите да защитят себе си и компютъра си от злонамерени уебсайтове, докато сърфират в мрежата. Chrome използва технологии като **Безопасно сърфиране, безопасна виртуална среда („sandboxing“)** и **автоматични актуализации**, за да способства за защитата срещу злонамерен софтуер и фишинг атаки.

Безопасно сърфиране

Chrome показва предупредително съобщение, преди потребителят да посети сайт, за който се подозира, че съдържа злонамерен софтуер или фишинг.
Фишинг атака се изразява в представяне под чужда самоличност с цел да бъде подведен потребителя да споделите лична или друга поверителна информация, обикновено през фалшив уебсайт.
Злонамереният софтуер от друга страна представлява софтуер, инсталиран на компютъра на потребител без неговото знание, и има за цел да му навреди или евентуално да открадне информация от него.
Благодарение на активираната в Chrome технология за безопасно сърфиране, ако в мрежата потребителят попадне на уебсайт, за който се подозира, че съдържа злонамерен софтуер или фишинг, ще види предупредителна страница. Функцията за откриване на фишинг и злонамерен софтуер е активирана по подразбиране.

Как работи безопасното сърфиране?

Функцията за безопасно сърфиране в Google Chrome, която установява наличието на фишинг и злонамерен софтуер, е разработена, за да защитава компютъра и поверителността на потребителя, като същевременно спестява трафик, изпращайки много малки количества данни към и от компютъра. Когато е активирана, Google зарежда в браузъра списък с информация за сайтове, които може да съдържат злонамерен софтуер или да извършват фишинг. Списъкът обаче не включва пълния URL адрес на отделните подозрителни сайтове. Вместо това всеки URL адрес е хеширан (замаскиран, така че да не може да бъде прочетен) и след това разделен на части. В списъка в браузъра е включена само част от съответния хеширан URL адрес. Когато потребителя сърфира в мрежата, браузърът създава хеширани версии на посещаваните от него URL адреси и ги сравнява с тези в списъка. Ако изглежда, че посещаван от него сайт съответства на фрагмент от хеширан URL адрес от списъка, браузърът се свързва със сървърите на Google, за да изиска списъка с пълните (не само частичните) хеширани URL адреси, за които се счита, че са опасни. След това компютърът на потребителя може да определи дали посещаваният сайт представлява риск и да го предупреди за това. Когато компютърът се свърже с Google, за да получи още информация за фрагмент от конкретен хеширан URL адрес или за да актуализира списъка, Google получават стандартна информация от регистрационните файлове,

включително потребителския IP адрес и, евентуално, „бисквитка“. Тези данни не го идентифицират лично и се запазват само за период от няколко седмици. Всяка информация, която получава Google чрез този процес, е защитена в съответствие със стандартните условия на Декларацията за поверителност на Google.

Безопасна виртуална среда („sandboxing“)

Използването на безопасна виртуална среда (англ. „sandboxing“) не позволява на злонамерения софтуер да се инсталира на компютъра на потребителя и да използва това, което се случва в един раздел на браузъра, за да повлияе на това в друг. Виртуалната среда добавя допълнителен защитен слой към браузъра, осигурявайки защита срещу злонамерени уеб страници, които се опитват да оставят програми на компютъра на потребителя, да следят дейностите му в мрежата или да откраднат поверителна информация от твърдия му диск.

Chrome разпределш всеки таб в отделен процес, за да предотврати злонамерен софтуер да се инсталира в компютъра на потребителя и да попречи това, което се случва в един таб да повлияе на случващото се в друг, обаче, същинският модел на разпределение на процесите е по-сложен. Следва се принципът на най-малко привилегии, всеки процес е ограничен от правата, които има и може да извършва изчисления, но не може да записва файлове или чете от определени области като документи, десктоп, това е подобно на „Protected Mode” използван в Internet Explorer на Windows Vista и Windows 7. Ако злонамерен софтуер е стартиран в един таб, той не може да подслушва въведени номера на кредитни карти въведени в друг таб, не може да взаимодейства с мишката или да каже на Windows да стартира изпълним файл при следващо стартиране на системата, когато този таб бъде затворен изпълнението на злонамерения софтуер ще бъде прекъснато.

Плъгините (Plugins) като Adobe Flash Player не са стандартизирани и като такива не могат да бъдат „sandboxed” както табовете. Те често трябва да бъдат изпълнени на или над нивото на сигурност на самия браузър. За да се намали възможността за атака, плъгините се изпълняват в отделни процеси, които комуникират с renderer, оперират с много ниски привилегии в определени за-таб процеси. Плъгините трябва да бъдат модифицирани, за да работят в тази софтуерна архитектура, докато следват принципа на най-малка привилегия. Chrome поддържа Netscape Plugin Application Programming Interface (NPAPI), но не поддържа вграждане на контролите ActiveX. На 30 март 2010 Google обяви, че новата версия на Chrome ще включва Adobe Flash като част от браузъра, елиминирайки нуждата да се сваля и инсталира отделно. Flash ще бъде обновяван като част от обновяванията на самия Chrome. Поддръжка на Java applet е налична с Chrome от Java 6 update 12 и нагоре. д

Автоматични актуализации

За да гарантира, че потребителят е защитен с най-новите актуализации за сигурност, Chrome редовно проверява за актуализации, за да бъде винаги в крак с тях. Проверките гарантират, че версията на потребителя на Chrome се актуализира

автоматично с най-новите, свързани със сигурността функции и корекции, без да са необходими никакви действия от негова страна.

Индикатори за сигурност на уебсайтовете

Когато потребителят се свърже с даден уебсайт, Google Chrome може да му покаже подробности за връзката и да му сигнализира, ако не успее да установи изцяло защитена връзка със сайта. Ако в дадена страница въвежда поверителна лична информация, тоя трябва да потърси икона на катинар отляво на URL адреса на сайта в адресната лента, за да види дали сайтът използва SSL.

SSL е протокол, предоставящ шифрована тунелна връзка между компютъра на потребителя и сайта, който разглежда. Сайтовете могат да използват SSL, за да предотвратяват достъпа на трети страни до информацията, която се прехвърля през тунелната връзка.

Икона	Какво означава това
	Сайтът не използва SSL. За повечето сайтове не е необходимо да се използва SSL, тъй като те не боравят с поверителна информация. Избягвайте да въвеждате поверителна информация, като потребителски имена и пароли, на страницата.
https://	**Google Chrome е установил успешно защитена връзка със сайта.** Потърсете тази икона и проверете URL адреса, ако от вас се изисква да влезете в сайта или да въведете поверителна информация на страницата. Ако даден сайт използва сертификат Extended Validation SSL (EV-SSL), името на организацията също се показва до иконата, изписано със зелени букви. Уверете се, че браузърът е настроен да проверява за анулиране на сертификата на сървъра, за да идентифицира сайтове с EV-SSL сертификати.
https://	**Сайтът използва SSL, но Google Chrome е открил несигурно съдържание на тази страница.** Бъдете внимателни, ако въвеждате поверителна информация на тази страница. Несигурното съдържание може да даде на някого вратичка, през която да манипулира страницата.
~~https~~://	**Сайтът използва SSL, но Google Chrome е открил или високорисково несигурно съдържание на страницата, или проблеми със сертификата на сайта.** Не въвеждайте поверителна информация на тази страница. Невалиден сертификат или друг сериозен проблем с https може да означава, че някой се опитва да фалшифицира връзката ви със сайта.

Преглед на допълнителни подробности за сайта

Потребителят трябва да кликне върху иконата или иконата на катинар, за да види още повече подробности за самоличността на сайта, връзката и историята на неговите посещенията на този сайт.

Самоличност на сайта

Използващите SSL сайтове представят на браузъра сертификати за сигурност, за да бъде проверена самоличността им. Всеки може да създаде уебсайт, който се представя за друг, но само истинският сайт притежава валиден сертификат за сигурност за URL адреса, до който се опитвате да стигнете. Невалидните сертификати могат да означават, че някой се опитва да фалшифицира връзката ви със сайта.

Икона	Какво означава това
	**Сертификатът на сайта е валиден** и идентичността му е потвърдена от надежден орган трета страна.
	**Сайтът не е представил на браузъра сертификат.** Това е нормално за обикновени HTTP сайтове (потърсете иконата в адресната лента), тъй като сертификати се предоставят обикновено само когато сайтът използва SSL.
	**Google Chrome е открил проблеми със сертификата на сайта.** Трябва да действате внимателно, тъй като е възможно сайтът да се представя за друг с цел да ви подмами да разкриете лична или друга поверителна информация.

Връзката между потребителя и сайта

Google Chrome дава информация дали връзката е изцяло шифрована. Ако връзката е незащитена, съществува възможност за трети страни да видят или фалшифицират информацията, която потребителяте предоставя на сайта.

Икона	Какво означава това
	**Google Chrome е установил успешно защитена връзка със сайта, който разглеждате.**
	**Връзката ви със сайта не е шифрована.** Това е нормално за обикновени HTTP сайтове (потърсете иконата  в адресната лента).
	**Връзката ви със сайта е шифрована, но Google Chrome е открил смесено съдържание на страницата.** Бъдете внимателни, ако въвеждате информация на тази страница. Смесеното съдържание може да даде на някого вратичка, през която да манипулира разглежданата от вас страница. Това съдържание може да включва вградени в страницата изображения, видеоклипове или реклами на трети страни. Смесеното съдържание е особено опасно, ако се свързвате с интернет посредством обществена безжична мрежа, защото безжичните мрежи могат да бъдат компрометирани по-лесно от кабелните.

История на посещенията

Ще се покаже, ако преди това потребителят е посещавал сайта. Ако обаче е изчистил кеш паметта и „бисквитките“, историята на посещенията също се изчиства.

Икона	Какво означава това
	**Посещавали сте сайта и преди**, така че вероятно му имате доверие.
	**Никога преди това не сте посещавали този сайт.** Нормално е да видите това съобщение, ако знаете, че това е вярно. Но ако сайтът ви се струва познат и не сте изчиствали наскоро историята си на сърфиране, възможно е той да се представя за друг сайт. Моля, действайте внимателно.

Използвани източници

1. http://en.wikipedia.org/wiki/Google_Chrome
2. http://www.google.com/chrome/intl/bg/more/security.html