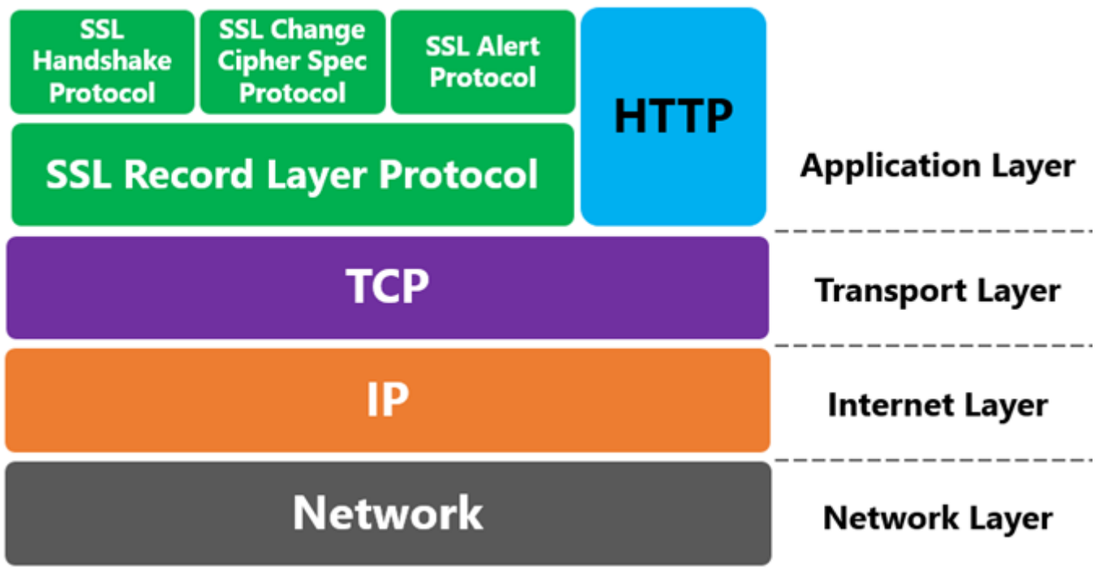
Serve migrare da HTTP a HTTPS?

30/09/2015 SCRITTO DA GIOVANNI SACHELI

10 COMMENTI



Full SSL Handshake

HTTP (HyperText Transfer Protocol) + **TSL** (Transport Layer Security) = **HTTPS**
**TCP e IP non fanno parte del protocollo HTTPS*

Dal 6 Agosto 2014, quando Google dichiarò esplicitamente che il protocollo HTTPS era diventato un fattore di ranking, ogni giorno nuovi siti migrano da HTTP a HTTPS per aumentare la sicurezza del proprio sito. Ma è davvero necessario?

A chi serve HTTPS e a chi invece non serve? **Cosa bisogna domandarsi** prima di migrare? **Quali sono le best practice** da seguire? Oggi cercherò di rispondere a queste domande.

Alla fine dell'articolo trovi importanti considerazioni di Maurizio Ceravolo sull'argomento HTTP vs HTTPS (PS: grazie Maurizio!).

Quando HTTPS è meglio di HTTP

Non tutti i siti hanno la necessità di criptare le connessioni client-server, tuttavia ci sono alcuni casi dove il protocollo HTTPS aggiunge fattori di sicurezza assolutamente necessari.

Il tuo sito tratta informazioni sensibili? E' possibile autenticarsi? E' possibile eseguire pagamenti attraverso il portale? I dati trasmessi sono critici? Se fattori come privacy, sicurezza di autenticazione, integrità dei dati e crittografia sono elementi di cui non puoi fare a meno allora la scelta di migrare ad HTTPS è obbligata.

- **Privacy:** l'HTTPS **protegge la privacy** di navigazione. Se navighi in HTTP uno sconosciuto può vedere i siti che stai navigando e capire i tuoi interessi e non solo. Se navighi in HTTPS la connessione è cifrata e nessuno può spiare le tue attività online.
- **Autenticazione:** l'HTTPS **certifica le parti**, assicura che tu sia connesso con la persona/azienda/server giusta e non con qualcuno che sta cercando di intromettersi nella comunicazione.
- **Integrità dei dati:** l'HTTPS certifica i dati che si inviano/ricevono. Non è possibile per terze parti intromettersi nella comunicazione e modificare i dati trasmessi in HTTPS. L'HTTPS offre sicurezza durante transazioni online e l'invio di informazioni sensibili.
- **Crittografia:** l'HTTPS maschera i dati trasmessi rendendoli illeggibili agli estranei. Navigando in HTTPS nessuno può intercettare i dati.

Il protocollo HTTPS interessa tutti

Diverse persone sono coinvolte con il sito aziendale: i visitatori, l'amministratore di sistema ed il webmaster/sviluppatore, ognuno con interessi e dubbi differenti:

- **Il visitatore:** perchè usare un sito non sicuro? Come posso proteggere la mia privacy? Come posso proteggere i miei dati?
- **L'amministratore del web server:** come si configura il TSL sul web server? Come posso migliorare le performance?
- **Lo sviluppatore del sito e proprietari:** come posso rendere i miei contenuti HTTPS friendly? Come posso migrare i miei contenuti da HTTP a HTTPS?

Privacy

- **HTTP:** un hacker in ascolto passivo sulla wifi **può vedere** i siti che navigo.
- **HTTPS:** un hacker in ascolto passivo sulla wifi **non può vedere** i siti che navigo perchè i dati trasmessi sono crittografati ent-to-end, quindi illeggibili senza la chiave di decodifica.

Integrità dei dati e autenticazione

- **HTTP:** un hacker attivo **può modificare** un sito, ad esempio deviando i suoi link interni verso pagine *trappola*. Tu credi di aver cliccato sul link ufficiale che porta alla tua banca invece finisci su un sito clonato.

- **HTTPS:** un hacker attivo **non può creare un sito fantoccio** di un portale certificato HTTPS perchè non ha il **certificato di autenticità.**

Attraverso il **tunnel TSL** tra utente e sito web:

- Un hacker attivo e passivo **non può** *mettersi in ascolto*
- Un hacker attivo e passivo **non può** modificare i dati trasmessi
- Un hacker attivo **non può** impersonare il destinatario

Valutazioni PRE migrazione

Prima di migrare verso il protocollo HTTPS è importante porsi alcune domande in modo da pianificare ed implementare al meglio tutti gli step necessari.

TLS e velocità

- I certificati **sono costosi**?
- Il protocollo HTTPS non **rallenta il sito**?
- Quali sono le **best practices** nella configurazione del server?

HTTPS e SEO Friendly

- Come posso migrare il contenuto esistente?
- Come posso rendere il sito SEO friendly?
- Quali sono gli errori da evitare?

Implementazione TLS

Consigli per l'implementazione del TLS. La checklist dell'amministratore di sistema:

- Acquista un certificato TLS a 2048-bit
- Configura TLS sul tuo server
- Verifica la configurazione TLS del tuo server
- Monitora le performance: resumption rates, etc…
- Ottimizza la configurazione del server: dimensioni della cache, etc…
- Analizza SPDY & HTTP 2.0

Acquista un certificato TLS a 2048-bit

- Singolo host: tasktip.com (Gratis, $10+)*
- Multi-dominio: tasktip.com, cdn.tasktip.com, tasktip.us (Gratis, $30+)*
- Wildcard: tasktip.com (Gratis, $100+)

*La maggior parte dei siti richiede un certificato per host singolo o multi dominio.

Info e costi dei certificati:

- Certificati gratuiti per attività non-commerciali ottenibili da StartSSL
- Certificati gratuiti per progetti open-source ottenibili da GlobalSign
- Certificati commerciali e multi-dominio costano da $ 30 in su

Configura TLS sul server

- Non seguire guide diverse. Fai riferimento al wiki di Mozilla "Server Side TLS" per le migliori best practice di configurazione per Apache, Nginx, HAProxy, AWS e altri web server popolari.
- Verifica la configurazione con l'ottimo tool di Qualys

PRO TIPS:

1. Abilitare e dare priorità alla suite ECDHE cipher suite* aumenta il carico sulla CPU. Il keepalive HTTP e la *session resumption* permettono di ridurre il carico sulla CPU
2. Le moderne implementazioni di TLS basate su software che girano su comuni CPU, sono abbastanza rapide da gestire pesanti carichi di traffico via HTTPS senza il bisogno di usare un hardware di cifratura dedicato

TLS + SPDY = siti più veloci!

Miglioramenti nel caricamento delle pagine con SPDY abilitato:

	Google News	Google Sites	Google Drive	Google Maps
Mediana	43%	27%	23%	24%
95° percentile	44%	33%	36%	28%

Incrementi a doppia cifra rispetto la normale connessione HTTP grazie al miglior sfruttamento delle risorse.

SPDY è supportato da Chrome, Opera, Firefox, IE e Safari.

SPDY porta diversi vantaggi anche al web server:

- Le richieste SPDY utilizzano **meno risorse** sul web server
- Le richieste SPDY richiedono **meno memoria** ma un pochino più di CPU

- Le richieste SPDY richiedono **meno processi** di lavoro in Apache

Altri vantaggi:

- I certificati sono economici
- Ci sono ottimi strumenti per verificare la configurazione
- TLS può essere ottenuto via software senza dover investire in hardware costoso
- TLS resumption, false-start, etc, aiutano a ridurre la latenza
- TLS permette di implementare SPDY e HTTP/2
- SPDY e HTTP/2 migliorano il caricamento delle pagine
- SPDY e HTTP/2 utilizzano meno risorse

Migrare ad HTTPS

Tutti i **segnali di indicizzazione devono essere coerenti**, questo significa verificare che gli URL indicati nei link, tag, meta, script, ecc, stiano puntando alle stesse medesime risorse (o URL). Non linkare un CSS a volte con HTTP e a volte con HTTPS, il segnale mandato a Google non sarebbe coerente.

La checklist del Webmaster

- Configura HTTPS sul server
- Aggiornare il contenuto del sito verso le nuove risorse sotto HTTPS
- Aggiornare i link interni puntandoli a HTTPS
- Verificare il file robots.txt
- Verificare la coerenza della tag rel=canonical, rel alternate, …
- Impostare le redirezioni correttamente ed aggiungere HSTS
- Verificare i report e le segnalazioni di Google Search Console

Configurare e verificare la configurazione TLS sul server

Messaggi di errore più comuni:

- **Incorrect hostname:** verificare la configurazione
- **Incomplete certificate chain:** autenticazione troppo lenta
- **Expired certificate:** certificato scaduto, segnati un reminder!

Correggere gli URI

Non usare HTTP nell'URL indicato nelle risorse, inserisci solo // per lasciar decidere al webserver da dove reperire la risorsa.

```
NO:
<script src="http://example.com/script.js"></script>
<a href="http://example.com/bar">

SI:
<script src="//example.com/script.js"></script>
<a href="//example.com/bar">... (Protocol relative URIs)
```

Hardcoded HTTP URI's in HTTPS hosted with ♥ by **GitHub** **view raw**

Redireziona gli URL HTTP verso le risorse in HTTPS

Utilizza redirezioni 301 per guidare utenti e spider verso l'URL HTTPS.
user/bots –> HTTP URL –> 301 –> HTTPS URL (pagina con tag rel canonical)
Ricordati: le redirezioni sono fondamentali, non mantenere live due versioni della stessa pagina in HTTP e HTTPS. Per approfondire il discorso sulle migrazioni SEO friendly ti consiglio questa guida .
Considera sempre:

- Vecchi link interni ed esterni che puntano ad HTTP
- Pagine salvate nei preferiti, pagine condivise sui social, etc che puntano ad HTTP

Elimina catene di redirezioni non necessarie

meglio puntare direttamente alla risorsa finale, evitando catene di redirezioni

- **NO catene di redirect:**
  - http://esempio.com –> http://www.esempio.com –> https://www.esempio.com

- **Si redirect singoli:**
  - http://esempio.com –> https://www.esempio.com
  - http://www.esempio.com –> https://www.esempio.com
  - https://esempio.com –> https://www.esempio.com

HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) è un meccanismo di politica di sicurezza proposta per il web dove un web server dichiara di interagire col browser usando solamente una connessione sicura (come HTTPS). La politica è comunicata dal server all'user agent attraverso il campo di un'intestazione di risposta HTTP chiamato "Strict-Transport-Security" (Sicurezza di trasporto ristretto). La politica specifica un periodo di tempo durante il quale l'user agent accederebbe al server solo in modalità sicura.

Apache

Abilita il modulo Headers su Apache.

```
a2enmod headers

```

```
Configure HSTS Apache  hosted with ♥ by GitHub  view raw
```

Aggiungi un header alle direttive del VirtualHost HTTPS. Max-age è misurato in secondi. Questo header è valido soltanto su un **VirtualHost HTTPS** ed esegue la richiesta di HTTPS per un anno, sotto-domini inclusi.

```
<VirtualHost *:443>
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

```

```
Configure HSTS Apache 2  hosted with ♥ by GitHub  view raw
```

Dovresti aggiungere redirect server-side per aggiornare le connessioni **non-HTTPS** la prima volta che si accede al sito. Aggiungi questa regola al **VirtualHost non-HTTPS**.

```
<VirtualHost *:80>
  [...]
  ServerName esempio.com
  Redirect permanent / https://esempio.com/
```

```
Configure HSTS Apache 3  hosted with ♥ by GitHub  view raw
```

NGINX

Aggiungi questa regola alla configurazione HTTPS del tuo NGINX server block.

```
add_header Strict-Transport-Security max-age=31536000;
```

```
Configure HSTS NGINX  hosted with ♥ by GitHub  view raw
```

Strict-Transport-Security: max-age=10886400; includeSubDomains

- max-age: valore indicato in secondi
- includeSubDomains: valore opzionale

I browser ricordano, per il periodo specificato nel parametro max-age, che devono richiedere in automatico le risorse in HTTPS per tutti il sito e sotto-domini.

- **HSTS elimina la necessità di impostare le redirezioni HTTP → HTTPS**

Permetti a Googlebot di scansionare URL in HTTP e HTTPS

- Non bloccare gli URL HTTP con il robots.txt

Non taggare Noindex gli URL HTTPS

Evita tag meta robots, X-Robots e direttive che possano impedire a Googlebot di leggere la pagina. **HTML**

```
<meta name="robots" content="noindex">
<meta name="googlebot" name="noindex">
```

```
Noindex Meta Robots Googlebot  hosted with ♥ by GitHub  view raw
```

HTTP

```
X-Robots-Tag: noindex
```

```
X-Robots-Tag: noindex  hosted with ♥ by GitHub  view raw
```

Aggiorna i link canonici puntandoli alle risorse HTTPS

```
da:
<link rel="canonical" href="http://esempio.com/ciao">

a:
<link rel="canonical" href="https://esempio.com/ciao">
```

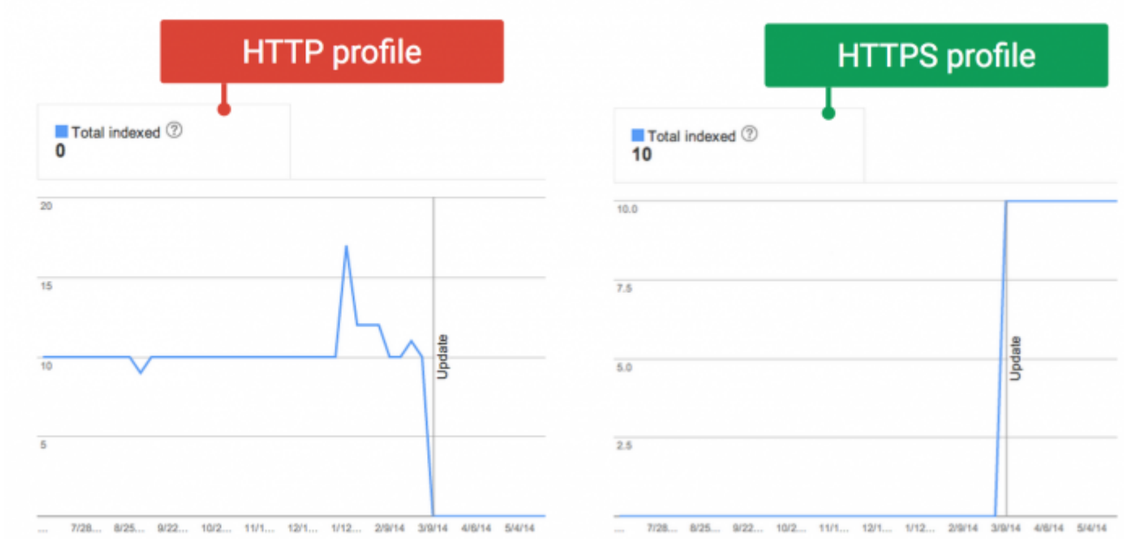
```
HTTP to HTTPS Canonical tag  hosted with ♥ by GitHub  view raw
```

Ricordati di correggere link interni, esterni e tag (canonical, alternate, …) facendoli puntare all'URL HTTPS.

Google Search Console

- Registra tutte le varianti del sito in GSC registrando tutti i profili (www, not-www, ed eventualmente https e mobile m.esempio.com)
- Monitora "Index Status"
- Monitora "Crawl Errors"

Registrare tutti i profili permette di analizzare e diagnosticare attraverso GSC ogni singolo sotto-dominio, dalle statistiche di scansione, l'indicizzazione della sitemap, ai dati delle query.



Statistiche di scansione nei due profili registrati in GSC, prima e dopo la migrazione ad HTTPS

Riassumendo

- TLS: crittografia, autenticazione ed integrità dei dati
- TLS non è lento se ottimizzi il tuo ambiente di sviluppo
- TLS può migliorare il caricamento delle pagine usando meno risorse
- Implementa HTTPS su tutti i siti e in tutte le pagine
- Aggiorna i link nei contenuti, implementa le redirezioni e HSTS
- Invia segnali coerenti a Googlebot

Considerazioni di Maurizio Ceravolo

Il commento di Maurizio Ceravolo

Vorrei aggiungere qualche piccola considerazione all'ottimo articolo di Giovanni.

Personalmente non ho pianificato di passare in HTTPS alcuno dei miei. Per ogni cosa cerco sempre di valutare il rapporto costi/benefici di ogni azione. Passare un sito in HTTPS ha un costo, in termini di lavoro ed in *danni SEO* che si possono fare se non si seguono i consigli di Giovanni. Per me criptare le informazioni se non ci sono dati sensibili dell'utente non ha senso. Come non ha senso inseguire Google nelle sue raccomandazioni premiate con un ipotetico miglioramento del ranking.

Facendo un esempio pratico, se un cliente è un ristorante, come posso giustificare il maggior costo nel passare il sito in HTTPS? All'utente importa qualcosa se un hacker intercettando il traffico wifi vede che sta guardando le foto della pepata con le cozze? Considerando che l'utente medio ha il profilo social pubblico e fa vedere a tutti quando è in vacanza ladri compresi, non credo che la privacy possa essere una sua preoccupazione. Almeno fino a quando la casa è svaligiata.

Il tutto questo c'è quindi un solo unico motivo per cui converrebbe portare il sito del ristorante in HTTPS: Analytics.

Questa specifica del protocollo HTTP http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html#sec15.1.3 dice:

> Clients SHOULD NOT include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol.

Il che vuol dice che i browser non passano il referrer quando si passa da HTTPS a HTTP. E questo ha una conseguenza per Analytics. Il traffico ricevuto da siti in HTTPS non viene riconosciuto come referral, ma bensì come **traffico diretto**. E quindi questo sfalsa i dati che analizziamo. L'unico modo per avere i dati corretti è passare anche il nostro sito in HTTPS.

C'è anche da dire che HTTPS non porta solo vantaggi in termini di sicurezza. Ma anche qualche problema. Emanuele Vaccari in questo suo articolo segnala che l'HTTPS rende più complicato rilevare il malware che passa per i canali pubblicitari. Ovvero gli hacker acquistano pubblicità su qualche circuito e caricano magari un banner in flash che diffonde qualche cosa di malevolo. Se il circuito pubblicitario è in HTTPS, rilevare queste cose è decisamente più complicato.

L'ultima considerazione che vorrei fare è su quale possa essere la diffusione dell'HTTPS. Ho la fortuna di poter condividere qualche dato. Per chi non mi conoscesse, sono uno scaricatore seriale di dati ed amo costruirmi database di informazioni. In questa mia attività ho anche scaricato tutte le schede italiane di Google MyBusiness per farci sopra delle analisi. Grazie a questi dati ad esempio un paio di settimane fa ho scritto un articolo sull'adozione della cookie law delle aziende italiane. E poco dopo ho pubblicato questo post su Google+ andando a cercare sui siti della precedente analisi quanti fossero stati bucati.

Possiamo quindi provare a vedere i miei dati di MyBusiness per capire se le aziende italiane adottano l'HTTPS. Ed il dato è interessante perché sono le aziende italiane che fanno il grosso del fatturato per web agency e freelance del settore.

Le schede di MyBusiness italiane che ho trovato sono 2.339.556. Di queste 708.454 indicano in scheda un url. Di questi url, escludendo quelli che indicano come proprio sito una pagina su un social network, quanti sono quelli in HTTPS? Molto pochi. Sono solo 3.266. Stiamo parlando di meno dello 0.5% delle aziende italiane che hanno un sito secondo MyBusiness. Se lo andiamo ad esaminare il dato è ancora minore.

Queste 3.266 schede spesso condividono il sito. Ad esempio ci sono 240 distributori Total Erg che fanno riferimento allo stesso sito della casa madre. E la stessa cosa succede per le filiali delle banche (e se loro non usassero l'HTTPS, sarebbe decisamente pericoloso). Se vado a contare i domini diversi **ne abbiamo solo 455**. E questi 455 sono in grossa parte siti di grandi aziende. Sono quindi pochi i siti di piccole e medie impresse (il cliente tipico di noi professionisti del settore) che adottano HTTPS.

Articoli correlati che potrebbero interessarti:

- Le migliori estensioni SEO per Google Chrome (14.8)
- Server HTTPS/SSL per applicazioni e landing page su Facebook (14.2)

- Commenti Facebook e G+ persi dopo migrazione da HTTP ad HTTPS (14)
- Analytics SEO, un tool a 360° davvero interessante (12.6)
- La corretta migrazione SEO di un sito web (12.1)
- Come funziona l'Intestazione HTTP X-Robots-Tag (12.1)
- Guida alla SEO tecnica per siti mobile (11.7)
- Cos'è Google Page Speed Service – PSS CDN e a cosa serve (10.4)

FILED UNDER: POSIZIONAMENTO MOTORI DI RICERCA
TAGGED WITH: CSS , GOOGLE ANALYTICS , GOOGLE SEARCH CONSOLE , HTTPS , MIGRARE UN SITO , REDIRECT 301 , SSL , WEB SERVER

About Giovanni Sacheli
Giovanni Sacheli é **consulente SEO** e SEM per Searcus Swiss Sagl ed EVE Milano. Professionista Certificato Google AdWords e grande appassionato di **analisi SEO**tecniche ed ottimizzazioni di siti eCommerce multilingua. Dal 2009 condivide su questo blog le sue esperienze e le nozioni tecniche più interessanti per posizionare siti web su Google.

Commenta con Google+

Per notificarmi il commento su Google Plus devi taggarmi +giovannisacheli.

40 commenti Google+

Aggiungi un commento come Giovanni Sacheli

Commenti più popolari

Giovanni Sacheli tramite Google+ 1 anno fa - Condivisione pubblica
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+7 +1 · Rispondi

Visualizza tutte le risposte (9)

Emanuele Vaccari 1 anno fa +2
Ottimo!

1futurweb 1 anno fa
Molto interessante

Maurizio Ceravolo tramite Google+ 1 anno fa - Condivisione pubblica
Un articolo approfondito di **+Giovanni Sacheli** sulla migrazione da HTTP a HTTPS, ed in coda un po' di numeri miei sull'adozione dell'HTTPS da parte dei siti aziendali italiani.
Ho anche citato **+Emanuele Vaccari** :-D

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+11 +1 · Rispondi

Visualizza tutte le risposte (18)

mauro cataldi 1 anno fa
D

. bo

mauro cataldi 1 anno fa
LIl

Lorenz Crood 5 mesi fa - Condivisione pubblica
Non mi sono mai interessato a questo argomento prima d'ora perchè non do mai troppa importanza a quello che dice Google. Ma Giovanni sa quello che dice e mi sono dovuto ricredere :)

+1 · Rispondi

Martino Mosna tramite Google+ 1 anno fa - Condivisione pubblica

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+6 +1 · Rispondi

Stefano Rigazio tramite Google+ 1 anno fa - Condivisione pubblica

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+3 +1 · Rispondi

Marcello Rabozzi tramite Google+ 1 anno fa - Condivisione pubblica
Da HTTP a HTTPS: quando? Come? Perchè? #daleggereconcalma

Ottima anche la guida passo-passo per la **migrazione SEO di un sito web**: https://www.evemilano.com/2014/12/migrazione-seo/

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+1 +1 · Rispondi

Matteo Landi tramite Google+ 1 anno fa - Condivisione pubblica
Migrazione da **HTTP** a **HTTPS**
Cosa bisogna domandarsi prima di migrare?
Quali sono le best practice da seguire?
Grande interazione questa tra **+Giovanni Sacheli** e **+Maurizio Ceravolo**.
Da salvare nei preferiti all'istante, ora! ;-))

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+2 +1 · Rispondi

Maurizio Ceravolo 1 anno fa *+1*
Felice che ti sia piaciuta:-D

EVE Milano Consulenza SEO tramite Google+ 1 anno fa - Condivisione pubblica
Ultimo articolo online, con il prezioso contributo di **+Maurizio Ceravolo**.

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+2 +1 · Rispondi

Condiviso da **Matteo Morreale** tramite Google+ 1 anno fa - Condivisione pubblica

+1 +1 · Rispondi

Fulger Ion tramite Google+ 1 anno fa - Condivisione pubblica

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+1 +1 · Rispondi

Teresa Zito tramite Google+ 1 anno fa - Condivisione pubblica

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+1 +1 · Rispondi

Domenico Iervolino tramite Google+ 1 anno fa - Condivisione pubblica

Giovanni Sacheli ha condiviso inizialmente questo post
Serve migrare da HTTP a HTTPS?

A chi serve **#HTTPS** e a chi invece non serve? Cosa bisogna domandarsi prima di migrare? Quali sono le best practice da seguire? Oggi cercherò di rispondere a queste domande.

+2 +1 · Rispondi

COMMENTS

Davide
30/09/2015 at 17:12

(Edit)
Ciao, ho una domanda se un sito internet di un hotel utilizza un booking form con pagamenti con carte di credito che utilizza https e lo si inserire sul sito come iframe quindi sulla pagina viene mostrata quella pagina del booking con https. Anche il sito dell'hotel ha bisogno di avere il certificato https oppure va bene tenere http normale, grazie

Rispondi

Giovanni Sacheli
30/09/2015 at 18:02

(Edit)
Ciao Davide, Google fa progressi nell'interpretazione degli iframe ma non è la soluzione più consigliata. Per risponderti bisognerebbe analizzare il form, dipende infatti da come funziona. L'HTTPS potrebbe proteggere i dati inviati dal form ma certamente non protegge l'intera pagina. Bisognerebbe fare dei test, mi viene in mente con Wireshark per analizzare se i dati trasmessi risultano in chiaro o meno.

Rispondi

Davide
01/10/2015 at 01:38

(Edit)
Grazie per la risposta.

Elena
24/05/2016 at 18:10

(Edit)
Buonasera Giovanni,
volevo capire se migrare un sito su HTTPS comporti effettivamente un vantaggio lato SEO oppure no. Se l'HTTPS è un fattore di ranking, perché non migrare qualunque sito su HTTPS? Altro dubbio: fa differenza, lato SEO, avere un certificato SSL gratuito rispetto ad un certificato a pagamento?
Grazie mille.

Rispondi

Giovanni Sacheli
25/05/2016 at 09:46

(Edit)
Ciao Elena, ti ringrazio per aver lasciato il tuo commento. Il protocollo HTTPS a quanto detto da Google è un fattore di ranking ma prima bisogna capire perchè l'ha detto. Google ci tiene a spingere HTTPS per la sicurezza del web e a volte dice che una cosa è (o non è) un fattore di ranking per favorirne la diffusione (o ridurla). Detto questo, il mio blog è sotto HTTPS da 7 mesi ormai, e non ho visto incrementi di ranking particolari. Questo protocollo su un blog serve a poco, su un eCommerce che tratta dati sensibili come le carte di credito è un obbligo (morale) averlo, **ma per la sicurezza degli utenti, non per il ranking.**

Il certificato HTTPS ha un costo, per quello non lo adottano tutti, e rende leggermente più lenta e complessa l'infrastruttura web server per via del processo di criptazione dei dati che la CPU deve fare.

In risposta alla tua ultima domanda ti dico: ci sono automobili utilitarie che costano 9.000 € a altre fuoriserie che costano 3.600.000 € (Lamborghini Veneno Roadster), una differenza abissale vero? Dovuta dalla qualità costruttiva, i costi di ricerca e sviluppo, … Anche nei certificati SSL ci sono fasce di prezzo e "modelli" differenti, da quello gratuito a quello da 20.000 dollari all'anno. Cosa cambia? Il grado di sicurezza. Quale scegliere? Il giusto rapporto per la tua attività. Quello gratuito non trasmette forti segnali di affidabilità, quello da 20k

è probabilmente eccessivo a meno che tu non sia Amazon. Io opterei per un certificato da 100 o 200€ all'anno per un medio sito web. Dipende da quanti soldi fa girare il sito :)

Spero di averti chiarito i dubbi, a presto!

Rispondi

Elena
26/05/2016 at 11:22

(Edit)
Grazie mille Giovanni.
Esaustivo e gentilissimo come sempre.

Erminio Vallesi
05/11/2016 at 13:17

(Edit)
Buongiorno Giovanni.
Complimenti per questa preziosa guida che userò per installare il certificato ssl sul mio blog.

La mia preoccupazione maggiore sono i backlink in entrata. Google consiglia di contattare i webmaster dei siti che hanno creato backlink per fare aggiornare il link in https.

Il mio è un sito di 4 anni, ben posizionato con traffico organico in costante crescita e un buon profilo backlink. Ho molti backlink da siti istituzionali come regioni, provincie e comuni. Ottenere l'aggiornamento dei backlink da tutti i siti sarà sicuramente impossibile. Affidandomi al 301 il mio sito avrà ripercussioni negative lato SEO?

Grazie.

Rispondi

Giovanni Sacheli
05/11/2016 at 13:26

(Edit)
Ciao Erminio, con i 301 ben impostati non corri alcun rischio.

Rispondi

Erminio Vallesi
08/11/2016 at 16:50

(Edit)
Ciao Giovanni e grazie per la tua risposta. Il mio sito è un portale lavoro quindi il passaggio a HTTPS lo farei solo per evitare il messaggio di errore nel browser, per anticipare la concorrenza e per usare HTTP/2. Ho visto che alcuni grandi siti di lavoro sono da poco passati a HTTPS. Mi conviene davvero passare a HTTPS? Grazie ancora.

Giovanni Sacheli
08/11/2016 at 18:25

(Edit)
Il mio parere su https è "via il dente via il dolore". Passando ad HTTPS dovrai dare più attenzione all'aspetto velocità del sito web, quindi prima inizi prima ti togli il pensiero, e avrai più tempo per ottimizzare gli aspetti tecnici. Ormai la strada è segnata, Google vuole https, rimandare non porterebbe alcun vantaggio. Un portale di lavoro immagino comporti l'invio di curriculum e di dati personali, se questi fossero protetti da un protocollo sicuro sarebbe meglio. Non credi?

LASCIA UN COMMENTO.

Autenticato come Giovanni Sacheli . Uscire?

Commento

COMMENTO ALL'ARTICOLO

CONTATTI

Consulenza SEO e Web Marketing
Via Pannilani 37/D, Como, 22100 - Italia
Telefono: (0039) 339-3668879
Email: info (at) evemilano.com
La società titolare di EVE Milano è Searcus Swiss Sagl

Agenzia SEO e SEM specializzata in **Search Marketing**, ti possiamo aiutare con analisi SEO professionali, local SEO e campagne PPC con Google AdWords e Facebook. Abbiamo anche sviluppato uno specifico corso SEO e SEM che si adatta alle tue competenze di partenza e ti guida attraverso le più moderne ed efficaci tecniche di posizionamento sui motori di ricerca .

SEARCH MARKETING

Il core business di EVE Milano è la **consulenza SEO** con focus sull'ottimizzazione tecnica dei siti web per migliorarne il posizionamento nei risultati dei motori di ricerca. Attraverso l'analisi delle parole chiave riusciamo ad identificare le **le keyword più efficaci** per generare traffico naturale. Con l'analisi dei competitor studiamo le mosse vincenti dei TOP player più visibili su Google e abbiamo sviluppato molti altri servizi utili a definire strategie di web marketing vincenti. Per ottenere il massimo da Google è necessario un sito web autorevole con una struttura efficiente e noi possiamo aiutarti con specifiche analisi SEO tecniche e servizi di link building professionali.

PARTNER GOOGLE ADWORDS

Google Partner

Sei interessato ad una consulenza per la gestione campagne AdWords ? Giovanni Sacheli è membro del programma di Certificazione AdWords **Google Partner** per garantire ai propri clienti competenze specifiche ed una professionalità comprovata. Molte Web Agency offrono AdWords nei loro servizi ma soltanto una minima percentuale è certificata da Google. Richiedi una consulenza AdWords professionale e certificata!

CONSULENZA SEO E PPC

- Servizi SEO
- Web Marketing
- Pubblicità su Google
- Pubblicità su Facebook
- Blog Aziendali

CATEGORIE DEL BLOG

- Guide WordPress
- La Fidanzata del SEO
- Posizionamento Motori di Ricerca
- Search Engine Marketing
- Social Media Marketing
- Web Analytics

ARCHIVIO

Archivio

Seleziona mese