Berlingske Media forbedrer IT sikkerheden for brugere og annoncører ved at skifte til HTTPS*

Berlingske Media forbereder at SSL sikre alle sites på tværs af Berlingske Media. Ved at skifte til HTTPS, er der nogle betingelser for annoncering som ændres. Se her, hvad det betyder for dig som annoncør.

Hvad er forskellen mellem HTTP og HTTPS?

Hver gang du besøger et website foretages en række http- forespørgsler til en server. Når man tilføjer et *s* laver man i stedet en sikker forbindelse, så den data der sendes er krypteret. HTTP og HTTPS fungerer stort set på samme måde, men hovedforskellen er, at HTTPS anvender en SSL forbindelse (Secure Sockets Layer) til at flytte data mellem webserver og webbrowser. SSL er en sikkerhedsteknologi, som sørger for, at alle informationer og data sendes via en krypteret forbindelse, når de flyttes fra A til Z og dermed forbliver private.

Hvorfor skifter Berlingske til HTTPS?

Ud over den øgede sikkerhed er der også andre fordele ved at skifte til https:

1) Kryptering: Når en besøgende kommer ind på et website, er der ingen udefrakommende, der kan følge med i, hvad den besøgende laver på siden.
2) Databeskyttelse: Data der vises til den besøgende, kan ikke ændres, uden det opdages. Autentificering/godkendelse: Man er sikker på, som bruger, at man ser det rigtige website.

Hvad betyder det for mig som annoncør?

Når du server annoncemateriale til sikre miljøer, såsom websider, der begynder med https://, (Fx https://www.b.dk/) er det vigtigt at bekræfte, at annoncerne er forenelige med miljøets sikkerhedsindstillinger. Hvis ikke materialet er kompatibelt kan browser og apps vise advarsler om blandet indhold, eller blot undlade at vise kreativet. Derfor er det vigtig, at der kun leveres HTTPS / SSL-kompatible bannere.

Sådan kontrollerer du om et banner er SSL-kompatibelt:

Som udgangspunkt er det vigtigt, at alle billeder, scripts, filer, osv. der loades i dit banner, kaldes med HTTPS som protokol – og ikke med HTTP://
Man kan med Google Chrome få en oversigt over de connections, som et banner laver.

I Chrome kontrolleres banneret således: (Illustration 1)

1. Tryk F12 i Chrome
2. Vælg vinduet "*security*"
3. Åben/refresh banneret i vinduet.
4. Chrome laver en oversigt over alle connections der laves og deler dem op i henholdsvis HTTP og HTTPS.

Andre måder at teste banneret: (Illustration 2)

1) Tryk F12 i din browser, så du åbner udviklingsværktøjerne. Vælg fanen ”*Konsol”*
2) Åben dit banner i vinduet. Sørg for at hente banneret via HTTPS
3) Kig i konsollen efter advarsler om *mixed content*. Hvis det er tilfældet, forsøger banneret at kalde en server via en http-forbindelse der bliver blokeret. Dette kan lede til store diskrepanser og at banneret aldrig bliver vist.

Illustration 1: Google Chrome security

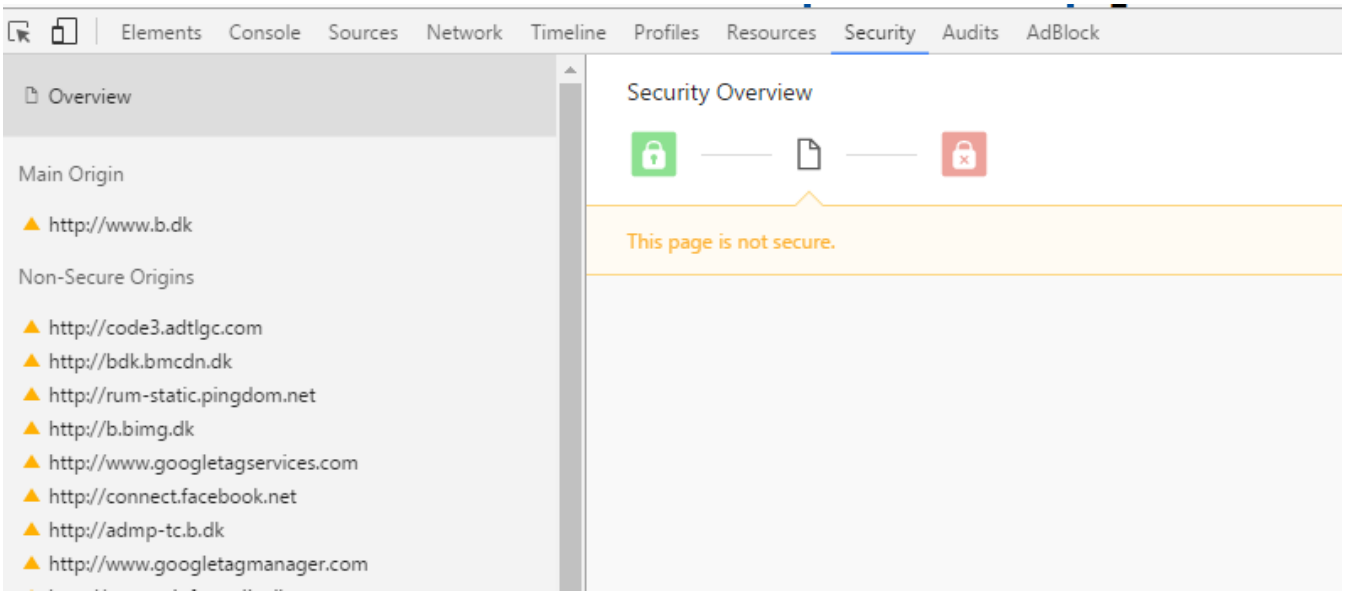
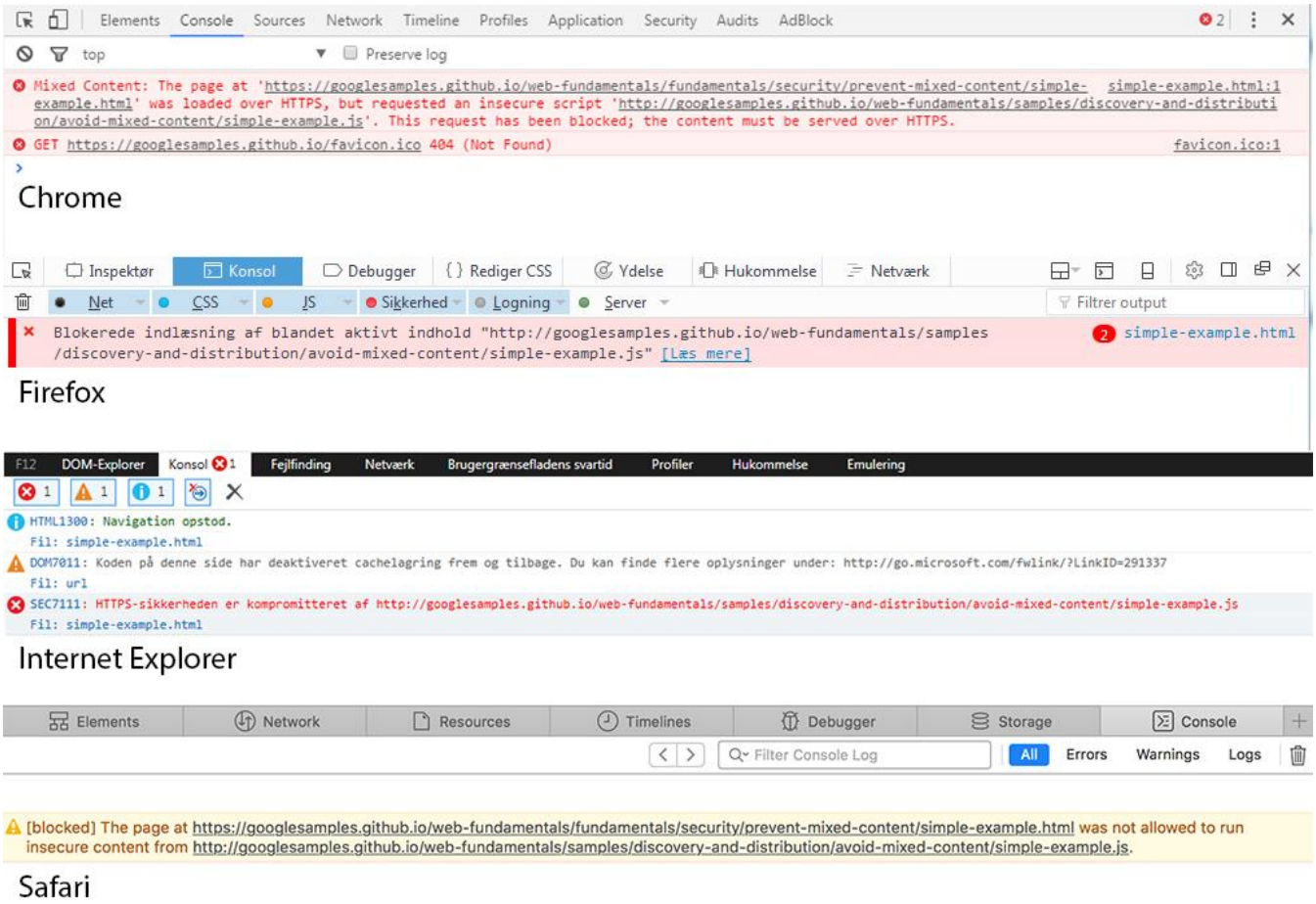


Illustration 2: Eksempler på mixed content



* Hyper Text Transfer Protocol *Secure*