15. Vikten av webb-adressen

Internet är en fristad där vem som helst kan sätta upp en webbplats. Ingen myndighet behöver godkänna vare sig webbadressen, namnet eller innehållet. Falska och klonade webbsidor har därför blivit ett favoritverktyg bland dagens brottslingar. På bara några minuter kan en skicklig angripare kopiera en hel webbplats så att den blir utseendemässigt identisk med originalet.

I detta kapitel går vi igenom hur vi identifierar sådana falska webbplatser. Vårt främsta hjälpverktyg är webbläsarens adressfält.

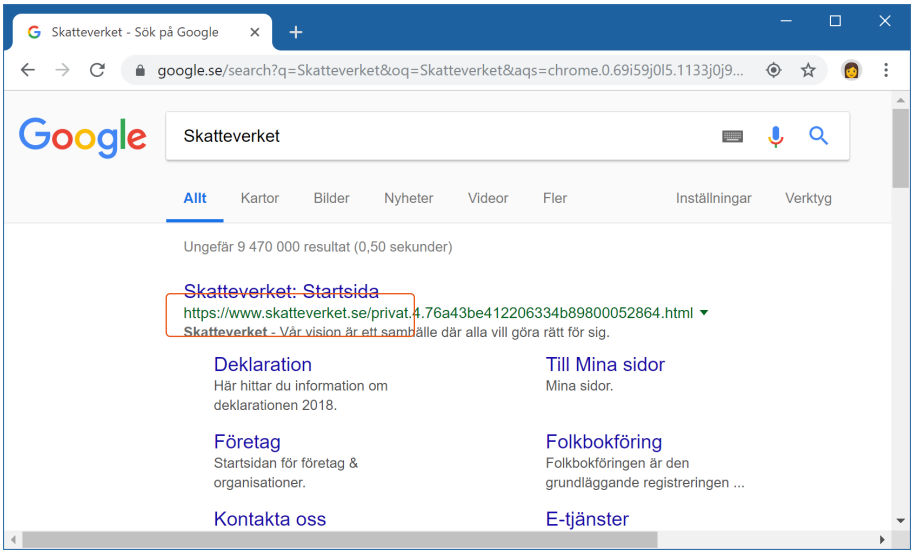
15.1 Kontrollera webbadressen i adressfältet

Eftersom det är så lätt för angripare att klona webbsidor måste vi noggrant kontrollera vilken webbadress som står i adressfältet. Vi måste säkerställa att vi befinner oss på den riktiga, officiella adressen. Detta gäller framförallt ifall vi kom till webbsidan genom att klicka på en länk.

> Varning! Smarta bedragare byter ut en eller flera bokstäver i adressen mot bokstäver som ger en minimal visuellt förändring. Några favorittrick är att byta ut l mot i, m mot rn och w mot vv.

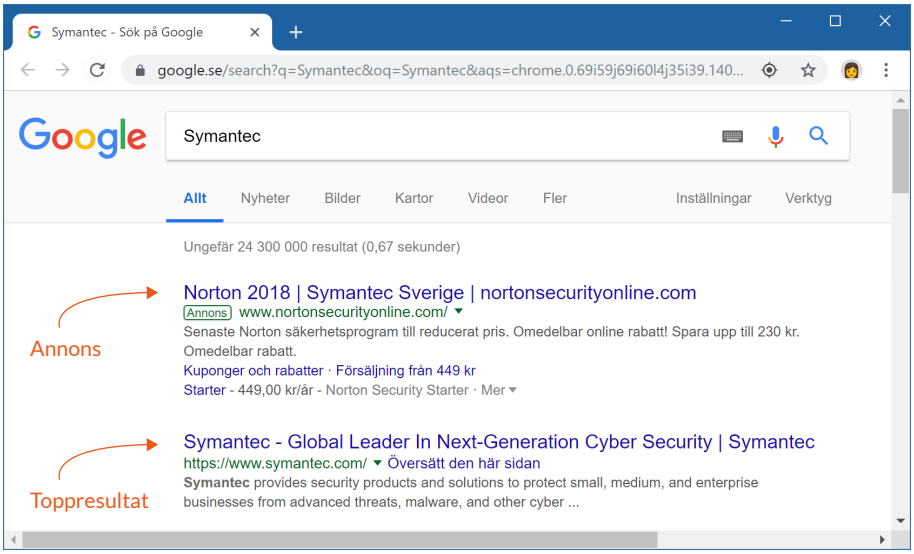
Ibland kan det vara svårt att veta vilken adress som är den rätta. Då finns lyckligtvis sökmotorer till vår hjälp. Sommaren 2015 skickade angripare ut ett mejl som påstods komma från Skatteverket. Mejlet hade en avsändaradress på skatteverket.net och länkade till en webbsida på skatteverket.net. I och med att Skatteverket är en svensk myndighet borde deras webbadress vara skatteverket.se och inte skatteverket.net. En snabb googling eller bingning efter ”Skatteverket” bekräftar att så är fallet. Det första icke-sponsrade sökresultatet leder till skatteverket.se.

> Varning! Besök ej skatteverket.net. Den adressen är fortfarande i bedragarnas ägo.



Google visar att skatteverket.se är den rätta adressen.

För att hamna högt upp i sökresultaten hos Google och Bing måste webbplatsen ha ett gott rykte och många andra webbplatser som länkar till den. Det gör sökmotorernas topplaceringar omöjliga att nå för eventuella angripares webbsidor. Undantag gäller för de eventuella sponsrade resultaten (annonserna) som visas längst upp. Ifall vi söker efter säkerhetsföretaget Symantec hamnar deras riktiga webbplats överst bland sökresultaten, men högst på sidan visas en annons för från företaget Goclickgo Marketing (nortonsecurityonline.com) som anspelar på att de skulle vara Symantec Sverige.



Symantecs riktiga webbplats visas överst bland sökresultaten (under annonsen).

15.2 Förstå webbadressen i adressfältet

Det räcker inte med att enbart kontrollera webbadressen som står i adressfältet. Det gäller att också förstå webbadressen och hur webbadressen hänger ihop med webbplatsen.

När ett företag vill skaffa en webbadress på internet köper de ett domännamn. Det kan till exempel vara nikkasystems.com eller microsoft.se. Domännamnet består av två delar: delen som står före punkten (*nikkasystems* eller *microsoft*) kallas huvuddomän medan delen som står efter punkten (*.com* eller *.se*) kallas toppdomän. Alla länder i världen har minst varsin toppdomän. Sverige har **.se**,

Danmark har **.dk** och Island har **.is**. Det finns också generiska toppdomäner såsom **.com**, **.net** och **.org**. På senare tid har mängden generiska toppdomäner utökats rejält och i skrivande stund finns det över tusen sådana. Ett exempel på en nytillkommen generisk toppdomän är **.systems**. Det är tack vare den som Nikka Systems kan ha domännamnet nikka.systems (utöver nikkasystems.com).

Nationella företag brukar registrera sina företagsnamn under åtminstone en toppdomän medan multinationella företag registrerar sina företagsnamn under flera toppdomäner. I och med att alla domännamn är förknippade med en årlig kostnad är det dock omöjligt för företag att äga domännamn under samtliga toppdomäner (framförallt nu när det finns tusentals toppdomäner). Nikka Systems riktiga domän är nikkasystems.com, men det finns inget som hindrar bedragare att köpa till exempel nikkasystems.eu och lägga upp en klonad version av webbplatsen där.

> Obs! På grund av ovannämnt exempel har vi i förebyggande syfte köpt nikkasystems.eu och skickar vidare besökare därifrån till nikkasystems.com.

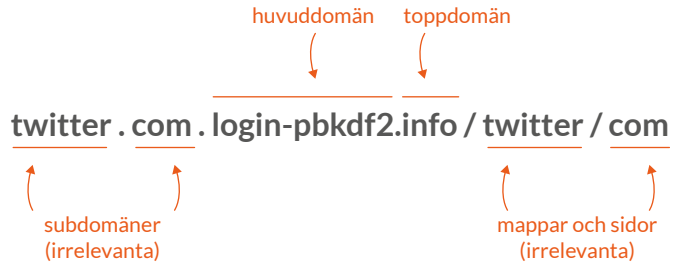
Den som äger ett domännamn kan lägga till hur många subdomäner som helst. En subdomän står alltid före huvuddomänen. Subdomäner brukar användas när ett företag driver flera olika webbplatser som på något vis hör ihop. Aftonbladet har till exempel sin webbplats Aftonbladet TV på subdomänen **tv** (tv.aftonbladet.se).

Sambandet mellan sub-, huvud- och toppdomän

Alla mappar och webbsidor som publiceras på webbplatsen hamnar framför ett snedstreck efter toppdomänen. Där kan den som driver webbplatsen lägga till hur många webbsidor som helst.

Bedragare kan genom vilseledande kombinationer av subdomäner och sidor lägga klonade bluffwebbsidor på webbadresser som påminner om de riktiga. För exemplen i denna bok har vi registrerat domännamnet login-pbkdf2.info. Till det domännamnet kan vi skapa vilka subdomäner vi vill. Vi kan exempelvis skapa fejkade versioner av Twitter och Facebook och publicera dem på twitter.com.login-pbkdf2.info respektive facebook.com.login-pbkdf2.info. Besökare som inte är uppmärksamma ser enbart att webbadresserna börjar på twitter.com eller facebook.com och kan därför luras att ange sina lösenord där.

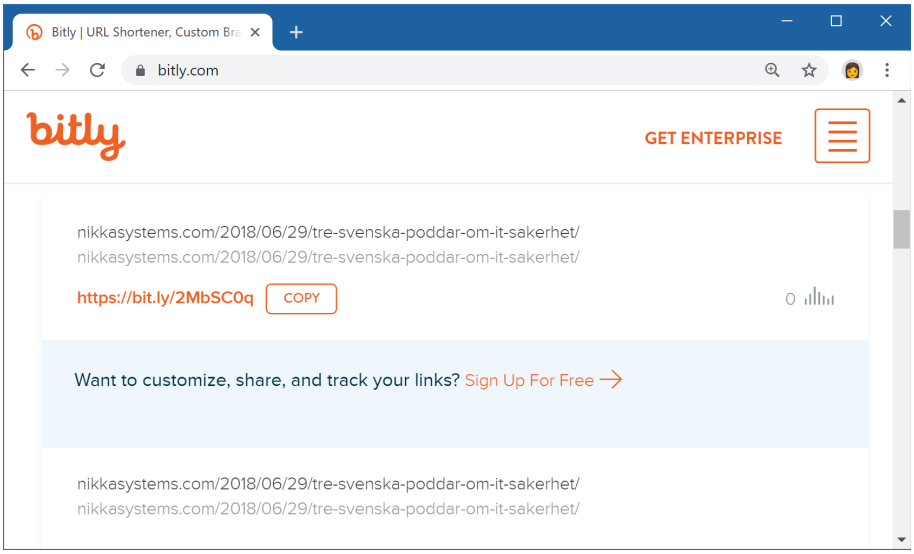
När vi vill kontrollera en webbadress är det enbart huvuddomänen och toppdomänen som är intressanta. Allt som står före och efter är helt irrelevant i sammanhanget. Den som äger huvuddomänen på toppdomänen kan lägga till vad som helst före och efter.



Huvuddomänen och toppdomänen (d.v.s. det som står precis före och efter den sista punkten) är det enda relevanta vid kontroll av en webbadress.

15.3 Kortlänkar

Länkar som börjar med bland annat bit.ly och ow.ly är vanligt förekommande i sociala medier. Bitly (bit.ly) och Hootsuite (ow.ly) driver så kallade kortlänkstjänster som låter oss ersätta långa komplicerade adresser med korta och lättskrivna motsvarigheter. Hos Bitly kan vi skapa en kortlänk som ersätter den långa webbadressen nikkasystems.com/2018/06/29/tre-svenska-poddar-om-it-sakerhet med den mer delningsvänliga länken bit.ly/2MbSC0q.



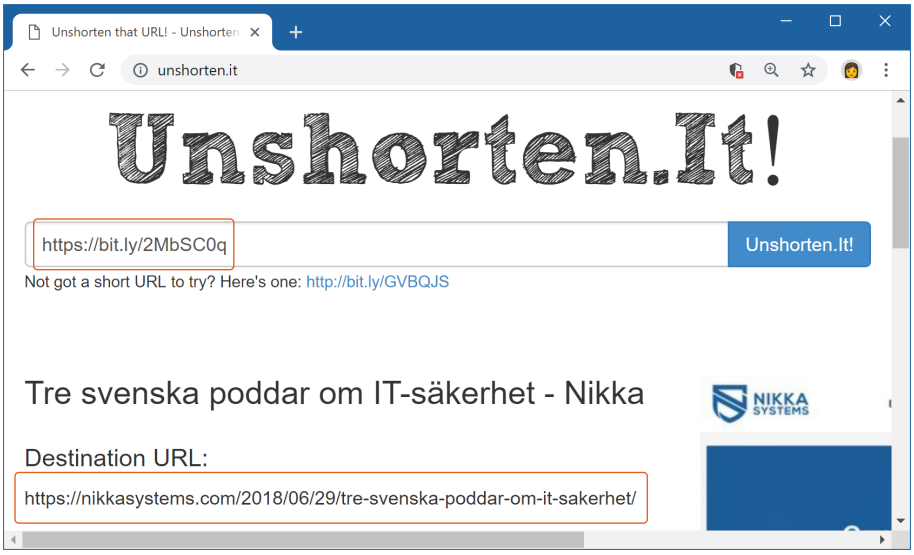
Bitly låter oss skapa kortlänkar till långa webbadresser.

När någon besöker vår nyskapade Bitly-kortlänk kommer han eller hon först till Bitlys webbservrar. Därifrån skickas besökaren omedelbart vidare till vår registrerade målsida.

Många företag driver egna kortlänkstjänster. Nikka System har exempelvis en egen kortlänkstjänst som skapar kortlänkar på domännamnet nikka.systems. Industrijätten ABB skapar kortlänkar på social.abb och elektronikkedjan Kjell & Company skapar kortlänkar på kjll.cm.

Kortlänkar är tyvärr lika populära bland bedragare som vill lura in oss på kapade eller infekterade webbplatser. Kortlänkar är ett effektivt sätt för bedragarna att maskera webbadresserna som vi i själva verket skickas till. Vi bör därför vara skeptiska till alla kortlänkar som delas av källor som vi inte litar på.

Tjänsten Unshorten It (unshorten.it) är ett bra verktyg för att undersöka misstänkta kortlänkar. Där kan vi skriva in kortlänkar och få reda på vilken webbsida de i själva verket leder oss till.



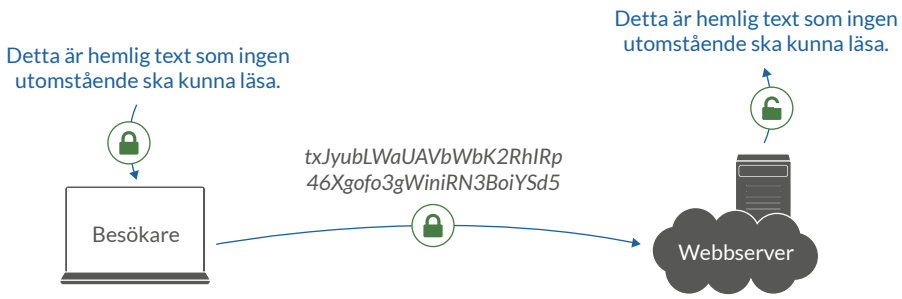
Unshorten It visar vart en kortlänk leder utan att vi behöver klicka på den.

15. Vikten av säkra anslutningar

Vi kan besöka webbplatser på två olika sätt: via **HTTP** eller **HTTPS**. HTTP står för Hypertext Transfer Protocol medan HTTPS står för Hypertext Transfer Protocol Secure (säker HTTP). Vi vill alltid, om möjligt, ansluta via säkra HTTPS. Då kan vi nämligen kommunicera autentiserat och krypterat. I detta kapitel förklarar vi vad det innebär och varför det är så viktigt.

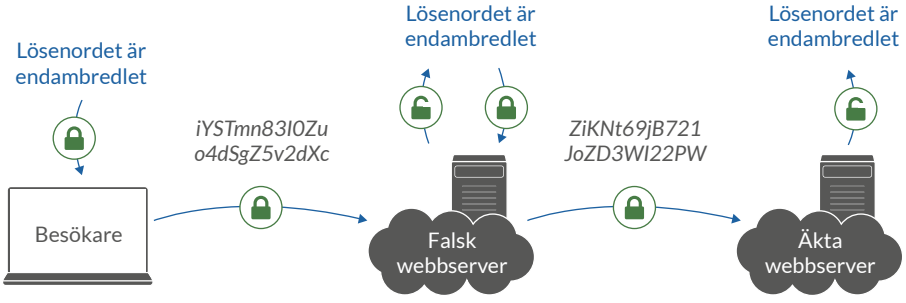
15.1 Autentisering och kryptering

När vi utbyter information med webbplatser på nätet passerar den många nyfikna ögon. Vi krypterar därför känslig information såsom inloggningsuppgifter och kreditkortsuppgifter. Krypteringen gör att inga utomstående parter kan se innehållet i informationen vi utbyter med webbplatsen. Utomstående parter kan enbart se mängden information som vi skickar och tar emot.



Genom att kryptera informationen som vi skickar kan ingen utomstående läsa den.

För att kunna överföra informationen på ett säkert vis räcker det dock inte med att vi krypterar den. Vi måste också autentisera webbservern vi kommunicerar med. Autentisering innebär i detta fall att vi säkerställer webbserverns äkthet. Utan autentisering kan en annan webbserver utge sig för att vara den riktiga, och kryptering fyller föga nytta ifall vi krypterar informationen för fel mottagare.



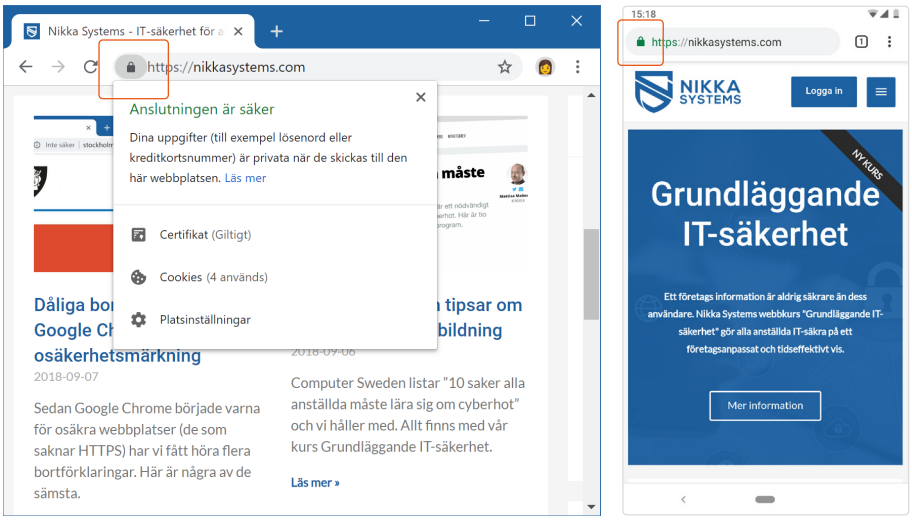
Om vi inte autentiserar webbservern kan vi råka kryptera informationen för en bedragares webbserver.

När en obehörig part avlyssnar trafiken på detta vis kallas det en MITM-attack (se *kapitel 4.2*). Den obehöriga parten ligger då som ett osynligt lager mellan besökaren och den riktiga webbplatsen. Både besökaren och webbplatsen tror att de kommunicerar med varandra, men i själva verket kommunicerar de med mellanhanden som avlyssnar och vidarebefordrar all information.

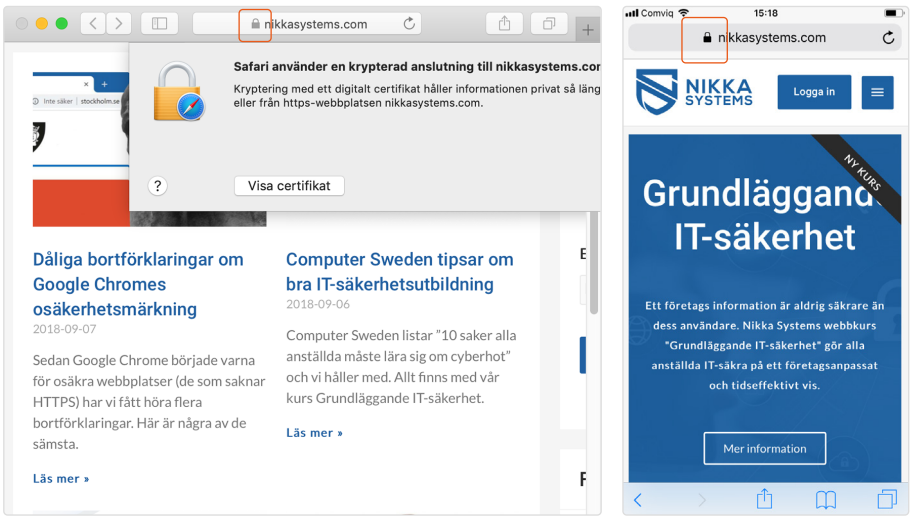
HTTPS löser detta problem. När vi ansluter via HTTPS säkerställer vår webbläsare att den kommunicerar med rätt webbserver och att den gör det över en krypterad anslutning.

15.2 Se skillnad på HTTP och HTTPS

Vår webbläsare indikerar tydligt huruvida vi besöker en webbplats via en osäker anslutning (d.v.s. HTTP) eller en säker, autentiserad och krypterad anslutning (d.v.s. HTTPS). Det exakta indikationssättet varierar mellan olika webbläsare, men gemensamt för Google Chrome, Mozilla Firefox, Microsoft Edge och Apple Safari är att de visar ett hänglås i adressfältet när anslutningen går via HTTPS. Detta gäller både de datorbaserade och mobilbaserade versionerna av webbläsarna.

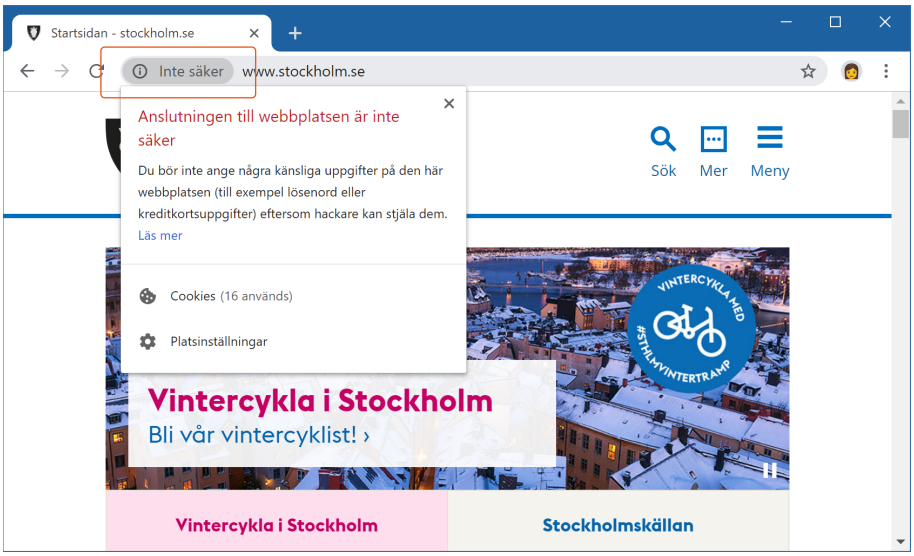


Google Chrome på Windows och Android indikerar säkra HTTPS-anslutningar med ett hänglås.



Apple Safari på Mac OS och IOS indikerar säkra HTTPS-anslutningar med ett hänglås.

Ifall vi ansluter via osäkra HTTP visas inget hänglås i adressfältet. Sedan sommaren 2018 visar Google Chrome däremot den föga smickrande texten ”inte säker” (övriga webbläsare visar än så länge inget alls). Google vill genom detta tilltag få alla webbplatsägare att lägga till stöd för HTTPS, så att vi därigenom får en säkrare webb. Förr i tiden var HTTPS-stöd förknippat med kostnader för webbplatsägaren, men så är inte fallet längre. Alla webbplatser borde därför stödja HTTPS redan idag.



Google Chrome visar tydligt att en webbplats besöks över en osäker anslutning.

Andelen HTTPS-kompatibla webbplatser har ökat stadigt under de senaste åren och fortsätter att göra så. Vid starten av 2014 var det enbart en fjärdedel av alla webbplatsbesök som skedde över säkra HTTPS-anslutningar. September 2018 är förhållandet det rakt motsatta (75 % av besöken sker över säkra HTTPS-anslutningar). Detta framgår av den telemetridata som Mozilla Firefox samlar in från användare som delar med sig av statistik[1].

15.3 Vikten av HTTPS-certifikat

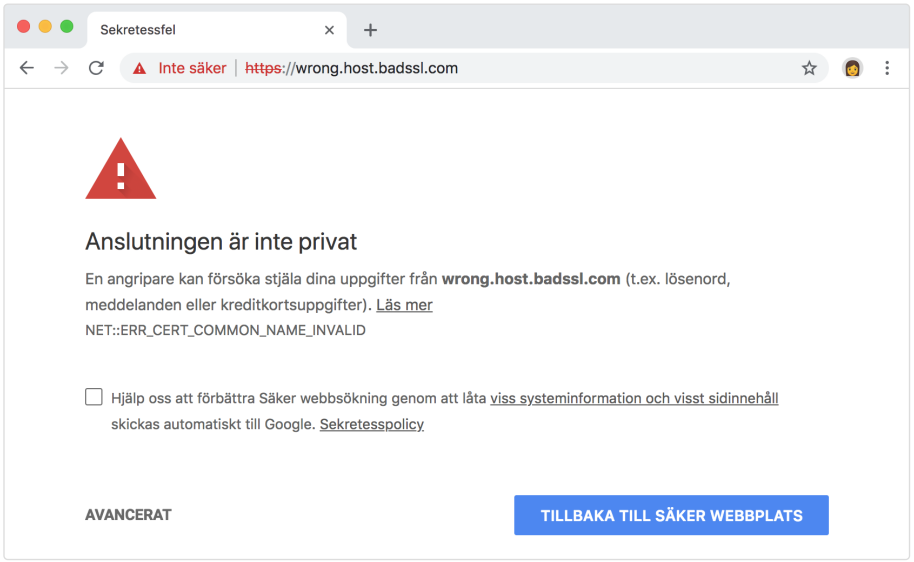
Alla webbplatser som stöder HTTPS har ett så kallat certifikat, vilket vår webbläsare använder för att säkerställa webbplatsernas äkthet. När vi ansluter till webbplatser utan HTTPS-certifikat (inget hänglås i adressfältet) kan vi aldrig vara riktigt säkra på att vi har hamnat rätt. Om vi exempelvis sitter på ett publikt wifi-nät kan en angripare kapa vår anslutning och styra om oss till en kopia av webbplatsen.

Stockholm Stads webbplats (stockholm.se) är en av de största svenska webbplatserna som inte stöder HTTPS i skrivande stund. Det innebär att en angripare kan klona stockholm.se och styra om offrens trafik till sin fejkade version av webbplatsen. Där kan angriparen byta ut informationen som visas eller lura besökarna att avslöja sina lösenord. Vi som besökare har ingen möjlighet att se vad som händer bakom kulisserna.

> Varning! Att anslutningen till en webbplats är säker innebär inte att webbplatsen i sig är säker. Även webbplatser som sprider skadlig kod eller kapar kreditkortsuppgifter kan stödja säkra anslutningar.

15.4 Ta alla varningar på allvar

Varningar i stil med den på nästa bild är en vanlig syn. Den dyker upp när något är säkerhetsmässigt fel i anslutningen.



Ignorera aldrig dessa varningar!

Varningar som dessa måste alltid tas på högsta allvar. De tyder nämligen inte bara på att något *kan* vara fel. De tyder på att något faktiskt *är* fel! Webbläsaren visar dessa varningar när webbplatsens certifikat inte är godkänt. Det kan i sin tur ha flera orsaker. Webbplatsägaren kan ha glömt att förnya certifikatet så att det har passerat sitt utgångsdatum, något som vi besökare knappast kan påverka.

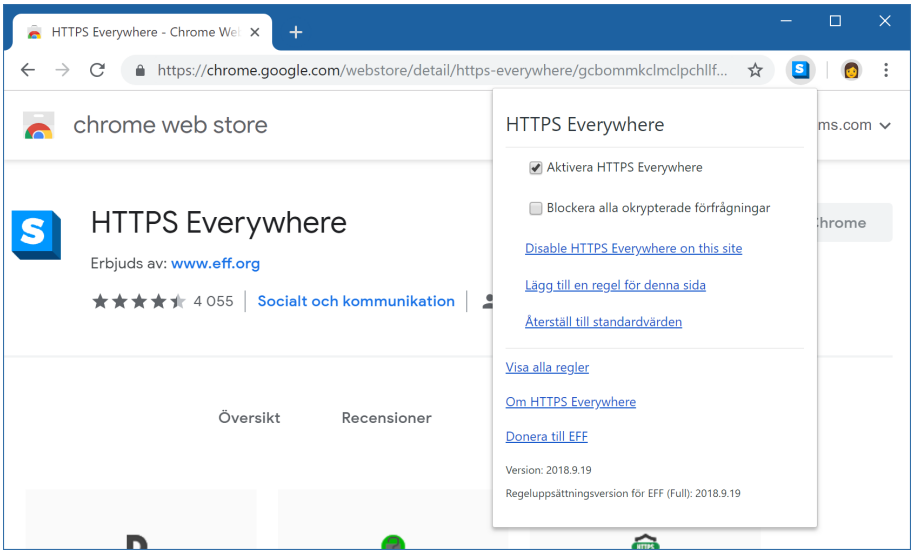
En annan anledning till varningen är att bedragare försöker kapa vår anslutning. Som tidigare nämnts kan kapare göra det obemärkt när vi ansluter via osäkra HTTP. Om de försöker göra samma sak när vi ansluter via säkra HTTPS visas en varning likt den på bilden. Vi måste därför alltid respektera dessa varningar och aldrig ignorera dem.

> Varning! Det finns attackmetoder som gör att även HTTPS-sidor kan kapas utan att det knappt märks. Det gör angriparna genom att lura våra webbläsare att ansluta över HTTP trots att webbplatsen stöder HTTPS. Webbplatsägaren kan förhindra detta på ett enkelt sätt, men trots det saknar fortfarande många webbplatser adekvat skydd.

15.5 Installera HTTPS Everywhere

På grund av gamla kvarlevor ansluter våra webbläsare än idag över osäkra HTTP som standard. Om vi inte uttryckligen skriver https:// i adressfältet besöker vi webbplatserna över HTTP. Som tur är uppgraderar de flesta HTTPS-kompatibla webbplatser oss till säkra HTTPS-anslutningar, men än idag finns det webbplatser som inte gör det per automatik. Vissa webbplatser laddar också in innehåll från tredjepartswebbplatser över osäkra HTTP-anslutningar trots att de hade kunnat göra det över säkra HTTPS-anslutningar.

Webbläsartillägget HTTPS Everywhere hjälper till i väntan på att HTTPS blir standardvalet i våra webbläsare. Med det tillägget aktivt uppgraderas våra anslutningar till HTTPS när så är möjligt. HTTPS Everywhere bygger på öppen källkod och kan installeras kostnadsfritt i både Google Chrome och Mozilla Firefox från respektive tilläggsbutik.



Webbläsartillägget HTTPS Everywhere uppgraderar om möjligt osäkra HTTP-anslutningar till säkra HTTPS-anslutningar.

> Tips! HTTPS Everywhere finns också som ett webbläsartillägg för Mozilla Firefox på Android (IOS-versionen av Mozilla Firefox stöder inte webbläsartillägg).

Detta bokutdrag har justerats för att passa A4-formatet. Mer information om Bli säker-boken finns på nikkasystems.com där också nyheter i text- och poddformat kompletterar den tryckta boken.