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. Se exempelvis Twitters inloggningssida i *kapitel 4.2*. Där visar vi både den äkta versionen av inloggningssidan och en fejkad klonversion som stjäl alla lösenord.

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

15.1 Kontrollera webbadressen i adressfältet

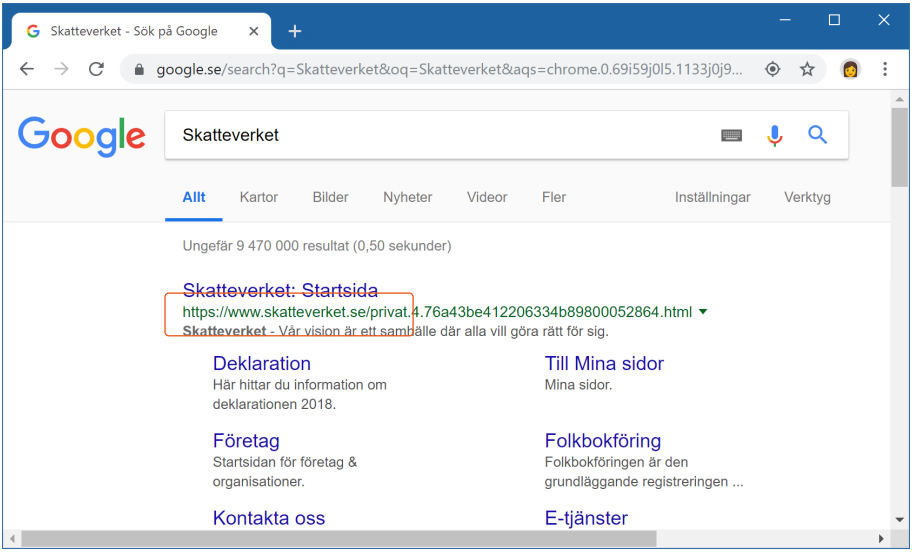
Eftersom det är så lätt för angripare att klona webbsidor måste vi noggrant kontrollera vilken webbadress som står i adressfältet. Vi måste säkerställa att vi befinner oss på den riktiga, officiella adressen. Detta gäller framförallt ifall vi kom till webbsidan genom att klicka på en länk.

> 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

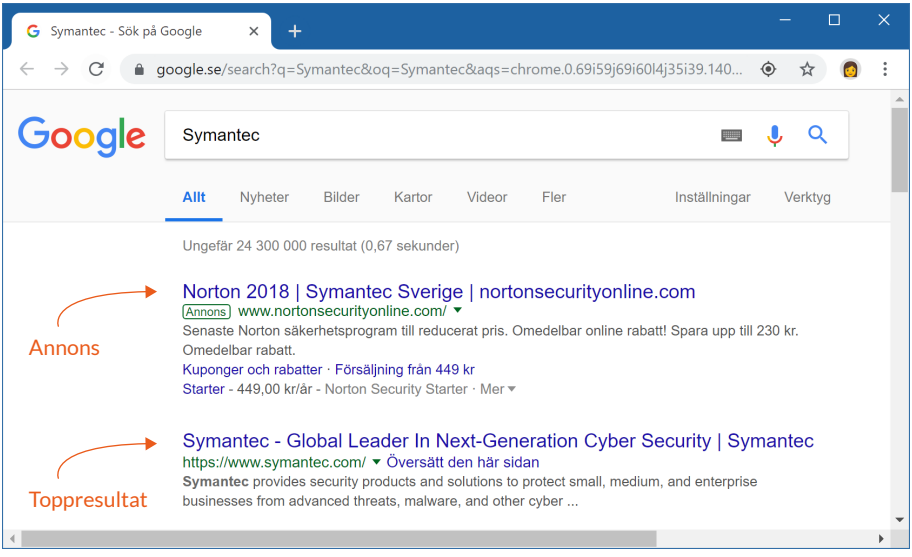
och inte skatteverket.net. En snabb googling eller bingning efter ”Skatteverket” bekräftar att så är fallet. Det första icke-sponsrade sökresultatet leder till skatteverket.se.

> 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.

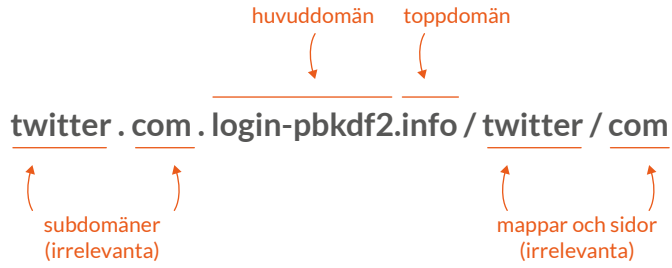
Den som äger ett domännamn kan lägga till hur många subdomäner som helst. En subdomän står alltid före huvuddomänen. Subdomäner brukar användas när ett företag driver flera olika webbplatser som på något vis hör ihop. Aftonbladet har till exempel sin webbplats Aftonbladet TV på subdomänen **tv** (tv.aftonbladet.se).

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.

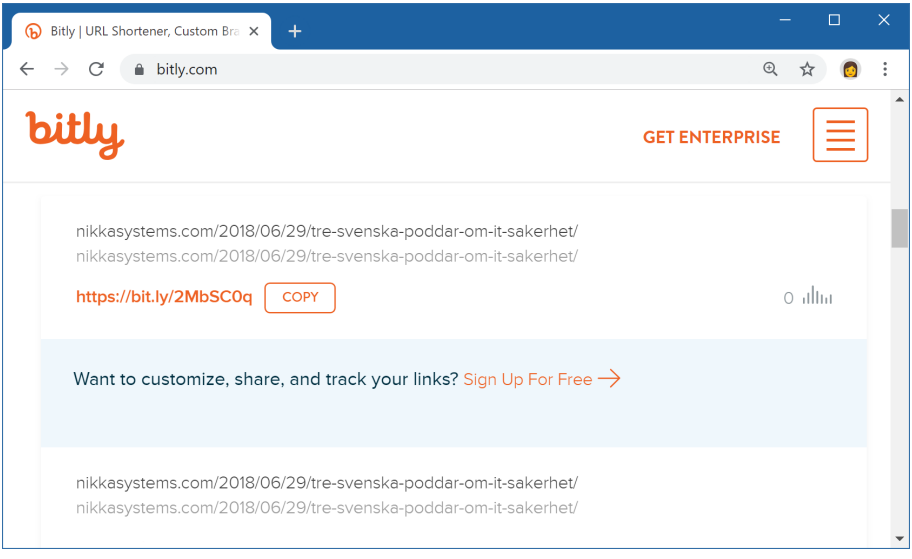
När vi vill kontrollera en webbadress är det enbart huvuddomänen och toppdomänen som är intressanta. Allt som står före och efter är helt irrelevant i sammanhanget. Den som äger huvuddomänen på toppdomänen kan lägga till vad som helst före och efter.



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.