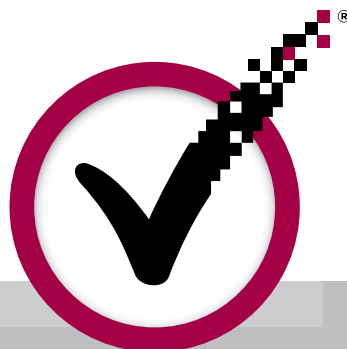




RAPPORT



## **SKAFFA KUNDER OCH BYGG UPP FÖRTROENDE PÅ NÄTET**

ALLT SOM SMARTA FÖRETAG GÖR FÖR  
ATT BYGGA UPP OCH ANVÄNDA SIG AV  
FÖRTROENDE FÖR ATT SKAPA SIG EN  
KONKURRENSFÖRDEL PÅ NÄTET

# SKAFFA KUNDER OCH BYGG UPP FÖRTROENDE PÅ NÄTET

Allt som smarta företag gör för att bygga upp och använda sig av förtroende för att skapa sig en konkurrensfördel på nätet.

Företag som har en webbplats måste ha kundernas förtroende. Det kostar pengar att bygga upp en bra webbplats. Ännu mer att bygga upp och marknadsföra ett varumärke. Det är ett kostsamt misstag att förlora kunderna i sista steget bara för att de inte känner sig tillräckligt trygga att köpa något. En riktigt dålig affär är vad det är. Det är som att springa maraton och stanna strax före mållinjen.

## UPPFATTNINGAR OM RISKERNA

Problem på Internet får mycket uppmärksamhet i medierna och kunderna är oroliga. Det innebär att en del inte handlar alls på nätet. Vissa är väldigt noga med vilka de handlar av och ratar webbplatser som inte får dem att känna sig trygga. Andra tar sig ända fram till kassan men avslutar inte transaktionen om de misstänker att deras personuppgifter inte är väl skyddade.

På fem år har den svenska distanshandeln mer än fördubblat sin omsättning. Enligt Postens rapport<sup>1</sup> omsätter den nu drygt 28 miljarder och står för 4,6 procent av den svenska detaljhandeln. Samtidigt rapporteras det att nätfisket nådde nya rekordnivåer 2009 och växte med 62 procent jämfört med nivåerna 2008<sup>2</sup>.

## FÖRTROENDE ÄR EN KONKURRENSFÖRDEL

Allt som e-handlare vill åstadkomma - få fler att fullfölja sina köp, öka ordervärdena, behålla marginalerna, öka avkastningen på marknadsföringen eller konkurrera med stora varumärken - kräver förtroende. På andra områden än näthandeln är förtroendefrågan ännu viktigare. Ekonomiska eller försäkringstransaktioner kräver att kunderna avslöjar mer information än när de handlar något på nätet. Inom offentlig sektor är det ännu mer krävande. Skulle du deklarera eller titta på din sjukjournal på en webbplats du inte litade på?

Om du kan göra din webbplats mer trovärdig kan du dra fördel av denna oro. Förtroende kan vara en konkurrensfördel.

62%

växte nätfisket med 2009 jämfört med året innan

<sup>1</sup> Posten AB 2010 (<http://hugin.info/134112/R/1408544/361291.pdf>).

<sup>2</sup> Brandjacking Index - 2009 - The Year in Review, MarkMonitor, Inc.

# RIKTIGA FÖRETAG, VERKLIGA DATA

Vi genomförde en enkät som vände sig till 143 IT-chefer i Sverige eftersom vi ville förstå vad företagen var bekymrade över och vad de hade gjort för att skaffa sig kunder och bygga upp förtroendet på nätet. Först frågade vi dem vad de trodde att kunderna oroade sig för. Det är en god indikation på vilket slags hot som företagen försöker värja sig mot.

Den risk som ansågs vara allvarligast var falska företag, tätt följd av finansiella förluster. De här resultaten återspeglar väl mediebevakningen av nätkriminalitet och resultat från kundenkäter. Indikerar att IT-cheferna bör ägna särskilt stor uppmärksamhet åt att visa att webbplatsen är vad den påstås vara, att visa kunderna att de tryggt kan ge sina kreditkortsuppgifter på webbplatsen och att deras uppgifter inte kommer att snappas upp av brottslingar.

När vi frågade vad IT-cheferna själva var oroliga över blev svaret ett annat. Experterna var mindre oroliga för identitetsstöld och nätfiske. Det viktigaste (förståeligt nog) ansågs vara att se till att kunderna kände sig trygga. Men praktiska bekymmer kom också högt upp på skalan. Exempelvis var oron stor för att ett SSL-certifikat oväntat skulle upphöra att gälla.

Det är berättigade orosmoln - falska webbplatser är ett växande hot. 911 varumärken kapades under det sista kvartalet 2009<sup>3</sup>. Nätfiske genom falska e-postmeddelanden och webbplatser där välkända varumärken används förstör förtroendet. Allt detta tyder på att företagen bör ägna kraft åt att bevisa att webbplatsen är legitim och inte tillhör en bedragare eller kriminell. Rädslan för identitetsstöld är huvudorsaken till bristande förtroende bland användare på nätet<sup>4</sup>, så webbplatsägarna måste visa att personuppgifter skyddas ordentligt, till exempel genom kryptering.

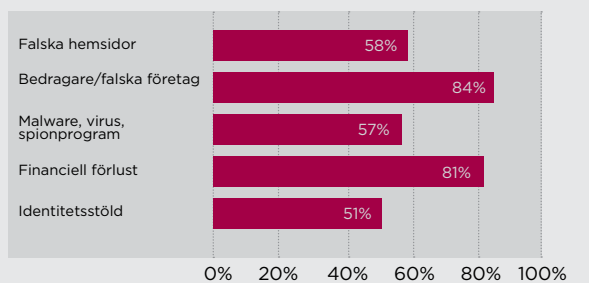
Utgångna SSL-certifikat är ett enormt avbräck för förtroendet, eftersom de skapar skrämmande (ibland skrämmande tekniska) felmeddelanden i webbläsarna. Det är förvånansvärt lätt att glömma att förnya, särskilt om man har många SSL-certifikat att hantera. IT-cheferna måste hantera dem effektivt och se till

att de inte upphör att gälla utan att någon märker det.

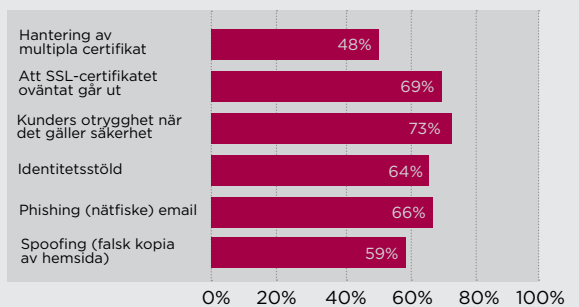
Vi frågade även vilka åtgärder enkättagarna vidtog för att öka förtroendet och säkerheten. Det populäraste var utan tvivel att kryptera känsliga uppgifter med SSL-certifikat, men förvånansvärt få använde den säkraste och

mest synliga varianten av SSL-certifikat: Extended Validation (EV) SSL-certifikat. Få använde förtroendemärken som sigillet VeriSign Secured<sup>®</sup> Seal och ännu färre förklarade för besökarna hur de skyddades, till exempel med en sida med säkerhetsråd. Det tycks som om de webbansvariga har ett par tips kvar att lära sig.

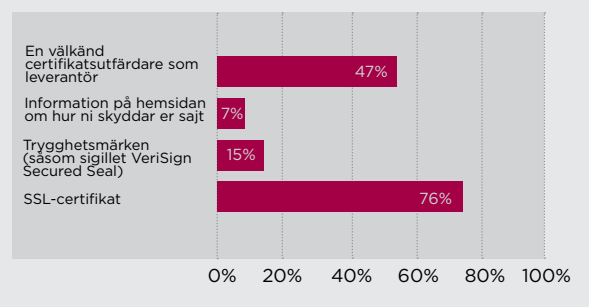
Vad IT-chefer tror att deras kunder oroar sig för mest



Vad oroar IT-chefer mest



Vilka säkerhets- och trygghetsåtgärder har ni er på er sajt?



<sup>3</sup> Anti-Phishing Working Group, december 2009, [www.apwg.org](http://www.apwg.org)

<sup>4</sup> Undersökning av Synovate/GMI 2009

# FÖRDELAR MED EXTENDED VALIDATION SSL-CERTIFIKAT

Vad innebär förtroende och tillit egentligen? Dels handlar det om en reaktion på nätkriminalitet såsom identitetsstölder. Dels om att förändra kundernas syn på säkerhet. Vi har delat upp dessa problem i fyra kategorier:

- Autentisering av säljaren ("vi är de vi utgör oss för att vara").
- Skydd och kryptering av data ("vi skyddar dina uppgifter").
- Förstärkning av varumärket ("vi respekterar ditt privatliv").
- Ökad tillit ("du kan tryggt handla hos oss").

Extended Validation (EV) SSL-certifikat är en utökad variant av vanliga SSL-certifikat. Med ett sådant visas företagets namn mot en grön bakgrund i adressfältet i kompatibla webbläsare såsom Internet Explorer 7 och senare versioner, Firefox 3.0 och senare och i de senaste smartphone mobiltelefonerna. Användarna ser klart och tydligt att webbplatsen går att lita på.

Certifikaten hanterar alla fyra punkterna ovan:

- **Autentisering av säljaren.** VeriSign bekräftar innehavarens identitet enligt industrins hårdaste krav innan ett certifikat utfärdas, så att användarna av webbplatsen kan vara säkra på att den inte är förfalskad.
- **Skydd och kryptering av data.** EV SSL-certifikat erbjuder den högsta krypteringsstyrkan som går att få med ett SSL-certifikat, så att användarnas uppgifter är skyddade på vägen mellan webbläsaren och webbplatsägaren.
- **Förstärkning av varumärket.** I kompatibla webbläsare visas EV SSL-certifikat upp tillsammans med företagets namn i webbläsarens adressfält, så att användarna kan se att webbplatsen tillhör företaget som de tror att den tillhör.
- **Ökad tillit.** Det gröna adressfältet för en webbplats som skyddas av ett EV SSL-certifikat ser användarna som ett tydligt och betrott tecken på utökad säkerhet.

## OM EXTENDED VALIDATION SSL-CERTIFIKAT

Extended Validation SSL-certifikat skapades som en reaktion på ökningen av antalet Internetbedrägerier, som urholkade allmänhetens förtroende för nättransaktioner. Extended Validation SSL-standarden ställer högre krav på verifieringen av SSL-certifikat och certifikaten visas tydligt i säkra webbläsare.

År 2006 godkände ledande SSL-certifikatutfärdare (CU) och webbläsartillverkare en standardpraxis för verifiering och visning av certifikat som kallas Extended Validation-standarden. En CU som vill utfärda ett SSL-certifikat som efterlever standarden måste använda den utökade metoden för att verifiera certifikat och genomgå en granskning av Webtrust. Verifieringsprocessen kräver att CU:n kontrollerar organisationens identitet och att den som ansöker om certifikatet verkligen äger domänen. Dessutom kontrolleras att den ansökande verkligen är anställd på företaget och har behörighet att införskaffa Extended Validation SSL-certifikatet.

Extended Validation SSL-certifikat ger mycket säkra webbläsare information som krävs för att tydligt identifiera en webbplats organisationsidentitet. Om du exempelvis besöker en webbplats som skyddas av ett SSL-certifikat som uppfyller Extended Validation-standarden med Microsoft® Internet Explorer 7 eller högre blir adressfältet i webbläsaren grönt. En ruta bredvid det gröna fältet växlar mellan att visa namnet på företaget som återfinns i certifikatet och certifikatutfärdaren (t.ex. VeriSign). Firefox 3 stöder också Extended Validation SSL.

# RESULTAT FRÅN VERKLIGHETEN

Vår enkät visar att företagen som använde EV SSL-certifikat fick ökade ordervärden, färre avbrutna transaktioner och ökad försäljning, men den största vinsten var att kunderna ansåg att webbplatsen var säkrare. En överväldigade majoritet av alla som svarade (66 procent) meddelade detta.

Dessa resultat återkommer ständigt hos alla våra kunder. Företag som skyddar sina webbplatser med VeriSign EV SSL rapporterar en genomsnittlig ökning av transaktionerna med mer än 20 procent<sup>5</sup>. Fallstudier med VeriSigns kunder som använder EV SSL-certifikat visar betydande resultat:<sup>6</sup>

- Efter att Scandinavian Design Online AB införde Extended Validation SSL-certifikat ökade deras onlineförsäljning med åtta procent under de första två månaderna efter det
- För Misco, återförsäljare av elektronik, minskade antalet avbrutna transaktioner med fem procent.
- Directline holidays konverteringar ökade med åtta procent.
- QuickRooms.coms försäljning ökade med nästan sju procent.
- Papercheck.com nästan fördubblade anmälningarna från nätet (en ökning med 87 procent).
- För CarInsurance.com ökade nätköpen med 18 procent.
- Fitness Footwears omvandlingar ökade med 16,9 procent och antalet avbrutna transaktioner minskade med 13,3 procent.

## VERISIGNS REKOMMENDATIONER

Du kan öka användarnas förtroende och tillit i fem enkla steg:

- **Uppgradera till EV SSL.** SSL är bra men Extended Validation SSL är bättre. De ersätter vanliga SSL-certifikat, kostar inte mycket mer och är inte krångligt eller tidskrävande att inrätta.
- **Välj en betrodd certifikatutfärdare.** Certifikatutfärdarens rykte är viktigt för användarna. I en undersökning svarade 88 procent att de litade på VeriSign jämfört med bara 22 procent för den näst mest betrodda utfärdaren<sup>7</sup>.
- **Använd ett förtroendemärke.** Förstärk EV SSL-certifikatet med ytterligare kännetecken som visar att du sätter värde på kundernas säkerhet. Det hjälper om förtroendemärken av det här slaget är välkända.
- **Förbättra certifikathandlingen.** Granska dina certifikat så att du är säker på att du får automatiska varningar i god tid innan de upphör att gälla. Fundera över att samla alla certifikat i ett hanterat konto. VeriSigns certifikatcenter hjälper dig att hantera VeriSigns certifikat centralt på nätet. Om du använder certifikat från flera certifikatutfärdare eller har många certifikat kan du investera i ett hanteringsverktyg som VeriSign Managed PKI för SSL.
- **Förklara för användarna hur du skyddar dem.** Lägg till en sida under "hjälp" eller en punkt på sidfotens meny där du förklarar hur du skyddar användarna, till exempel genom att beskriva hur ett SSL-certifikat fungerar. Det hjälper till att lugna användarna.

Vi upptäckte att de som svarade på enkäten i genomsnitt lade 11 procent av sin webbudget på säkerhet. Det är en avsevärd summa, men ändå vidtog många företag inte dessa enkla steg för att öka kundernas förtroende till webbplatserna.

Även om de kräver en viss investering i tid, till exempel för att ändra siddesignen för att lägga till ett förtroendemärke, är de inte dyra i sig själv eller i förhållande till webbplatsens totala säkerhetsbudget.

EV SSL är här för att stanna. Smarta företag använder dem redan och kunderna får allt större kunskaper om fördelarna med dem och ser omedelbart när de används på en webbplats. Men många företag – däribland några av dina konkurrenter – använder dem ännu inte. De gör heller inget av allt det andra för att öka användarnas förtroende och tillit. Därför är det enda förnuftiga att börja använda EV SSL och vidta alla de andra rekommenderade åtgärderna. Att vinna kundernas förtroende och tillit är en konkurrensfördel och VeriSign kan hjälpa dig att göra det.

# 8%

ökade Scandinavian Design Onlines onlineförsäljning två månader efter att de implementerat EV SSL

<sup>5</sup> I december 2009 visade test som utfördes på dussintals webbplatser runtom i världen att VeriSign EV SSL-certifikat hjälpte till att öka antalet omvandlingar med mellan 5 och 87 procent. Medelvärdet var över 20 procent.

<sup>6</sup> Resultatet för ditt företag kan bli ett annat. Faktorer som utmärker just dessa kunder kan ha bidragit till deras resultat.

<sup>7</sup> Tec-Ed, januari 2007.

## OM VERISIGN

VeriSign (NASDAQ: VRSN) är en pålitlig leverantör av Internetinfrastruktur tjänster för den digitala världen. Våra SSL-, autentiserings-, identitetsskydds- och registertjänster hjälper företag och kunder i hela världen att kommunicera och bedriva handel med förtroende, miljarder gånger dagligen.

VeriSign är den ledande certifikatutfärdaren inom SSL (Secure Sockets Layer) och möjliggör säker e-handel och kommunikation på webbplatser, i intranät och i extranät. VeriSign leder alltjämt SSL-certifikatbranschen som medlem av CA/Browser Forum, en frivillig sammanslutning som för närvarande är inriktad på EV SSL-certifikat.



**Besök [www.Verisign.se](http://www.Verisign.se)  
om du vill ha mer information.**

© 2010 VeriSign S.A.R.L. Alla rättigheter förbehålles. VeriSign, VeriSigns logotyp, cirkelsymbolen, VeriSign Secured och andra varumärken, servicemärken och designs är registrerade eller oregistrerade varumärken som tillhör VeriSign och dess dotterbolag i USA och andra länder. Alla övriga varumärken tillhör sina respektive innehavare.

