



# ❖ SÅDAN FÅR I FLERE KUNDER OG SKABER KUNDETILLID PÅ NETTET

LÆS, HVORDAN NOGLE VIRKSOMHEDER  
SKABER FORBRUGERTILLID, SOM GIVER  
DEM KONKURRENCEFORDELE I DERES  
NETSALG

# ➤ SÅDAN FÅR I FLERE KUNDER OG SKABER KUNDETILLID PÅ NETTET

Læs, hvordan nogle virksomheder skaber forbrugertillid, som giver dem konkurrencefordele i deres netsalg.

Virksomheder, som er på internettet, har brug for kundernes tillid. Det er dyrt at opbygge et godt websted. Og det er endnu dyrere at skabe et brand og udbrede kendskabet til det. Desuden koster det dyrt, hvis kunderne hopper fra allersidst i købsprocessen, fordi de simpelthen ikke har tilstrækkelig tillid til webstedet. Det er skidt for forretningen og kan sammenlignes med at løbe et maraton og så stoppe lige før målstregen.

## OPFATTELSEN AF RISICI

Problemer på internettet får stor opmærksomhed i medierne og gør forbrugerne nervøse. For virksomhederne betyder det, at nogle forbrugere slet ikke handler på nettet. Andre forbrugere er meget kræsne med hensyn til, hvem de handler hos – og de handler ikke på websteder, hvor de ikke føler sig sikre. Andre igen når helt frem til kassen, men hopper fra, hvis de føler, at deres personlige oplysninger ikke er tilstrækkeligt beskyttet.

Get Safe Online, som er en statslig britisk kampagne sponsoreret af VeriSign, har afdækket en række statistiske data om forbrugernes villighed til at handle på nettet. Mens mange forbrugere gerne handler, bruger netbank og køber ferierejser på nettet, er der også mange, der ikke gør. Omkring en tredjedel af den britiske befolkning handler ikke på nettet<sup>1</sup>. Mange forbrugere har været udsat for en computervirus (34%), phishing (22%), netsvindel (15%) og identitetstyveri (21%).

## TILLID GIVER KONKURRENCEFORSPRING

Alle de ting, som ledelsen i en netbutik ønsker at opnå – færre u gennemførte handler, større ordreværdier, fastholdelse af avancer, større afkast af reklamer og konkurrenceevne i kampen med de store varemærker – afhænger af tillid. Og går man ud over ren nethandel, spiller tillid en endnu større rolle. Ved f.eks. finansierings- og forsikringsrelaterede transaktioner skal kunderne give endnu flere oplysninger om sig selv end ved netkøb. Og ved transaktioner med det offentlige bliver oplysningerne både mere detaljerede og mere private. Ville du selv f.eks. indberette din selvangivelse eller gå ind på din sygejournal på et websted, som du ikke har tillid til?

Hvis I kan skabe tillid til netsikkerheden på jeres websted, kan I vende alle disse aspekter til jeres fordel. Tillid kan give jer et konkurrenceforspring.

34%

Mange forbrugere har været udsat for en computervirus

<sup>1</sup> Get Safe Online-rapport 2009: [http://www.getsafeonline.org/nqcontent.cfm?a\\_id=1517](http://www.getsafeonline.org/nqcontent.cfm?a_id=1517).

# FAKTISKE DATA FRA DET VIRKELIGE ERHVERVSLIV

Vi har udført en undersøgelse blandt 719 europæiske it-chefer for at klarlægge, hvad virksomhederne er bekymret for, og hvad de gør for at erobre kunder og skabe tillid på nettet.

I første omgang spurgte vi dem, hvad de mente, at deres kunder var bekymret for. Dette er en god indikator for, hvilke trusler virksomhederne ønsker at komme i forkøbet.

Den største risiko, som kunderne gav udtryk for, var økonomisk tab eller svindel – stærkt efterfulgt af forbryderiske netudbydere. Disse resultater afspejler umiddelbart den generelle mediedækning af netkriminalitet og resultater fra brugerundersøgelser, som f.eks. årsberetningen fra den statslige britiske kampagne Get Safe Online. Det giver anledning til at formode, at it-chefer bør fokusere ekstra meget på at bevise, at deres websted reelt er, hvad det giver sig ud for – at vise over for kunderne, at de trygt kan indtaste deres kreditkortoplysninger på webstedet, og at deres private data ikke vil blive opsnapet af kriminelle.

Da vi dernæst spurgte it-cheferne, hvad de selv var bekymret for, var billedet noget anderledes. Som eksperter på området var de mindre bekymret for identitetstyveri og phishing. Deres største prioritering var i stedet (forståeligt nok) at sørge for, at kunderne føler sig sikre. Men de havde også store problemer af mere praktisk karakter, som f.eks. frygten for uventet udløb af virksomhedens SSL-certifikater som et af de helt store problemer.

Disse bekymringer er fuldt forståelige. Spoof-websteder er en reel trussel, idet 911 brands blev brugt ulovligt på falske websteder i sidste kvartal af 2009<sup>2</sup>. Phishing kan underminere et brands omdømme via falske e-mails og websteder, som benytter velkendte brands. Alle disse fakta giver anledning til at konkludere, at virksomhederne er nødt til at fokusere på at bevise, at deres websted er den ægte vare og ikke en falsk udbyder. Frygten for identitetstyveri er hovedårsagen til forbrugernes manglende tillid til sikkerheden på nettet<sup>3</sup>, og derfor er netbutikker nødt til at kunne påvise, at forbrugernes personlige oplysninger er korrekt beskyttet, f.eks. ved hjælp af kryptering.

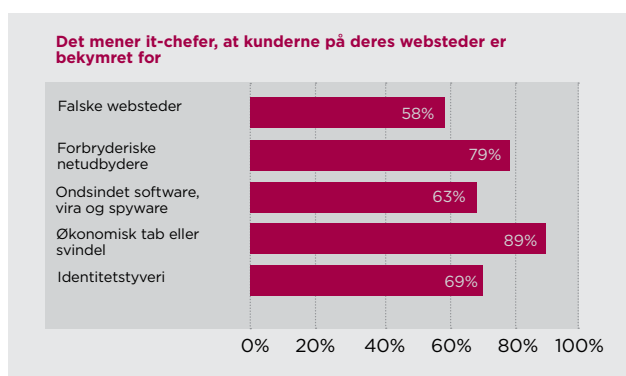
Forældede SSL-certifikater er en kolossal trussel mod forbrugernes tillid, fordi der popper foruroligende (og foruroligende tekniske) fejlmeddelelser op i deres webbrowsere. Det er overraskende nemt at miste overblikket over fornyelsesdatoer, især hvis I har

mange SSL-certifikater at holde styr på. It-afdelingen er nødt til at have effektivt styr på disse og sørge for, at de ikke udløber ved en fejl.

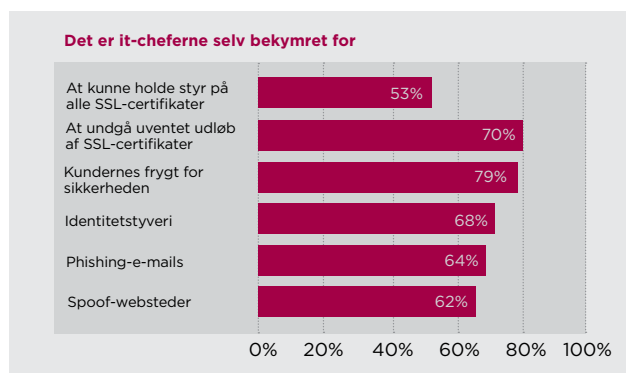
Desuden spurgte vi undersøgelsesdeltagerne, hvilke skridt de tog for at øge tilliden og sikkerheden. Kryptering af fortrolige oplysninger ved hjælp af SSL-certifikater er klart den mest populære foranstaltning. Men overraskende få anvender den sikreste

og mest synlige type SSL-certificering, nemlig SSL-certifikater med Extended Validation (EV). Der er ikke mange, som anvender garantimærker, som f.eks. VeriSign Secured® Seal, og endnu færre oplyser (f.eks. via en webside med ”råd om netsikkerhed”) besøgende om, hvor godt deres oplysninger beskyttes på webstedet. Tilsyneladende går mange webstedsbestyrere glip af en hel del effektive foranstaltninger.

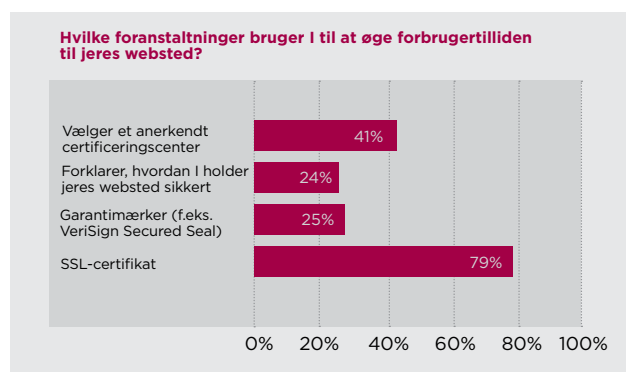
(i)



(ii)



(iii)



<sup>2</sup> Anti-Phishing Working Group, December 2009 [www.apwg.org](http://www.apwg.org)

<sup>3</sup> 2009 analyse foretaget af Synovate/GMI

# FORDELENE MED SSL-CERTIFIKATER MED EXTENDED VALIDATIONS

Hvad betyder tillid til sikkerheden på nettet egentlig? Dels er det et modsvar mod netkriminalitet, som f.eks. identitetstyveri. Dels handler det om at ændre kundernes opfattelse af sikkerheden. Vi har inddelt problematikken i fire kategorier:

- Autentificering af sælger ("vi er dem, vi giver os ud for at være")
- Beskyttelse og kryptering af data ("vi beskytter jeres data")
- Visning af firmanavn ("jeres oplysninger behandles fortroligt")
- Øget kundetillid ("det er sikkert at handle hos os")

SSL-certifikater med Extended Validation (EV) er en opgradering i forhold til de almindelige SSL-certifikater. Med SSL EV bliver firmaets navn og en grøn baggrund vist i adresselinjen i kompatible browsere (f.eks. Internet Explorer 7 og nyere versioner, Firefox 3.0 og nyere versioner og de nyeste smartphones). Brugere får et meget synligt bevis for, at de kan stole på sikkerheden på webstedet.

SSL-certifikater med EV dækker alle fire punkter:

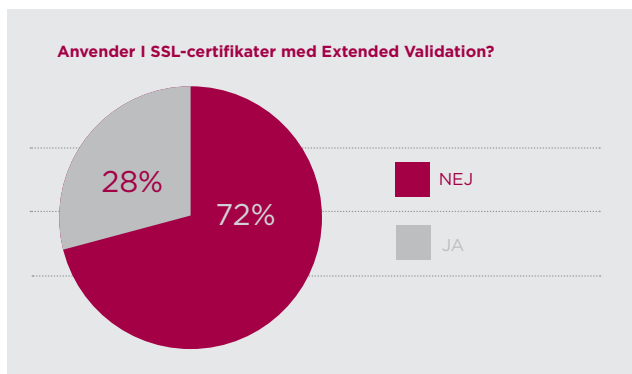
- **Autentificering af sælgeren**  
VeriSign anvender skrappe metoder til autentificering, før der udstedes et certifikat, så besøgende på et websted kan være sikre på, at webstedet ikke er falsk.
- **Beskyttelse og kryptering af data.**  
SSL-certifikater med EV giver den højst mulige krypteringssikkerhed med et SSL-certifikat, idet brugerens data krypteres mellem browseren og webstedets ejer.
- **Visning af firmanavn.** I kompatible browsere viser SSL-certifikater med EV virksomhedens navn i adresselinjen, så brugere kan se, at webstedet tilhører den virksomhed, som de antager, at det tilhører.
- **Øget kundetillid.** Den grønne adresselinje i browseren på et websted, som er beskyttet med et SSL-certifikat med EV, er et synligt og anerkendt bevis for den forhøjede brugersikkerhed.

## OM SSL-CERTIFIKATER MED EXTENDED VALIDATION

SSL-certifikater med Extended Validation er et direkte tiltag mod den stigende svindel på internettet, der underminerer forbrugernes tillid til at handle på nettet. Extended Validation SSL-standarden er en forstærkning af den sikkerhed, der opnås med almindelige SSL-certifikater, og der skiltes tydeligt med den høje sikkerhed i netsikre browsere.

I 2006 godkendte en gruppe førende SSL-certificeringscentre (CA'er) og browserudbydere standardmetoderne for certifikatautentificering og -visning, kaldet "standard Extended Validation". For at udstede et SSL-certifikat, der overholder denne standard, skal et CA anvende metoden for Extended Certificate-autentificering og udføre en Webtrust-kontrol. Autentificeringsprocessen kræver, at CA'et autentificerer certifikatansøgerens domæneejerskab og virksomhedsidentitet samt den enkelte godkenders ansættelse hos ansøgeren og bemyndigelse til at indhente SSL-certifikatet med Extended Validation.

SSL-certifikater med Extended Validation instruerer netsikre webbrowsere i tydeligt at identificere et websteds virksomhedsidentitet. Hvis en bruger f.eks. anvender Microsoft® Internet Explorer 7 til at besøge et websted, som er beskyttet med et SSL-certifikat, der overholder Extended Validation-standarden, bliver webadresselinjen i IE7-browseren grøn. I en rude ved siden af den grønne adresselinje kan der skiftes mellem virksomhedsnavnet som anført i certifikatet og certificeringscentret (f.eks. VeriSign). Firefox 3 understøtter også SSL-certifikater med Extended Validation.



# REELLE RESULTATER

Vores undersøgelse afdækkede, at virksomheder, som indfører SSL-certifikater med EV, øger ordreværdierne, får færre ugennemførte handler og styrker omsætningen. Men den største gevinst er kundernes opfattelse af sikkerheden på virksomhedernes websteder, som anført af et overvældende flertal (70%) af de adspurgte.

Vi oplever de samme resultater igen og igen for vores kunder. Virksomheder, der beskytter deres websted med VeriSign EV SSL, anfører en gennemsnitlig stigning i transaktioner på mere end 20%. De seneste VeriSign-kundecases om brugen af SSL-certifikater med EV, påviser store fordele\*:

- Den britiske elektronikforhandler Misco oplevede et fald på 5% i ugennemførte handler
- Det britiske charterrejsewebsted directline holidays fik 8% flere kunder i forhold til antallet af besøgende
- QuickRooms.com øgede omsætningen på bestilling af hotelværelser med næsten 7%
- Webstedet Papercheck.com, som tilbyder korrekturserviceydelse, oplevede tæt ved en fordobling af registreringer på webstedet (en stigning på 87%)
- CarInsurance.com fik 18% flere kundetilmeldinger på nettet
- Fitness Footwear fik 16,9% flere kunder i forhold til antallet af besøgende og 13,3% færre ugennemførte handler
- CreditKarma.com oplevede 26% flere kunder i forhold til antallet af besøgende

## VERISIGN ANBEFALER

Der er 5 enkle forholdsregler, I kan tage for at øge kundernes tillid til jeres netsikkerhed:

- **Opgrader til EV SSL.** SSL er godt, men SSL med Extended Validation er endnu bedre. Disse certifikater anvendes i stedet for de almindelige SSL-certifikater. De koster lidt mere, og de kræver lidt ekstra arbejde at installere.

- **Vælg et anerkendt certificeringscenter.** Omdømmet for et certificeringscenter (som f.eks. VeriSign) er vigtigt for brugerne. I en undersøgelse gav 88% af de adspurgte udtryk for, at de havde tillid til VeriSign, sammenlignet med de blot 22%, som havde tillid til den næstmest anerkendte leverandør<sup>5</sup>.
- **Anvend et garantimærke.** Suppler SSL-certifikater med EV med ekstra visuel sikkerhedsmærkning, som viser, at I prioriterer kundernes netsikkerhed højt. Det er en fordel, hvis det anvendte garantimærke er bredt anerkendt. Eksempelvis genkender 81% af de briter, som handler på nettet, VeriSign Secured® Seal, hvilket er betydeligt flere end for noget andet garantimærke.
- **Få bedre styr på jeres certifikater.** Gennemgå jeres certifikater for at sikre, at I automatisk bliver varslet om udløbsdatoer. Overvej at samle alle jeres certifikater på en administreret konto. VeriSign Certificate Center kan hjælpe jer med at administrere VeriSign-certifikater via ét centralt sted på nettet. Hvis I har certifikater fra forskellige certificeringscentre, eller hvis I har mange certifikater, anbefaler vi at anskaffe et styringsværktøj som f.eks. VeriSign Managed PKI til SSL.
- **Forklar brugerne, hvordan I beskytter dem på nettet.** I kan øge forbrugertilliden ved at tilføje en side i jeres Hjælp-sektion eller menuen nederst på forsiden, hvor I forklarer, hvordan I beskytter brugerne på jeres websted, f.eks. ved at beskrive, hvad et SSL-certifikat indebærer.

Vi fandt ud af, at de adspurgte i vores undersøgelse i gennemsnit brugte 14% af deres udgiftsbudget på netsikkerhedsforanstaltninger. Det er et betydeligt beløb, men ikke desto mindre er der en lang række virksomheder, som ikke tager disse grundlæggende forholdsregler for at øge kundetilliden til og netsikkerheden på deres websted.

Selvom der skal bruges lidt tid, f.eks. til at ændre designet af en webside for at indsætte et garantimærke, er disse foranstaltninger ikke dyre – hverken overordnet set eller som en post i budgettet til webstedets sikkerhed.

EV SSL er kommet for at blive. De virksomheder, som har indset fordelene, anvender allerede denne certificeringsløsning, og flere og flere forbrugere er opmærksomme herpå og genkender straks certificeringen, når de ser den på et websted. Men der er en lang række virksomheder – deriblandt nogle af jeres konkurrenter – som stadig ikke anvender den. Og som heller ikke træffer andre forholdsregler for at skabe kundetillid til deres netsikkerhed. Konklusionen er, at der er langt mere, der taler for, at virksomheder indfører EV SSL og alle de øvrige foranstaltninger som anbefalet ovenfor, end at de undlader at gøre det. At vinde kundernes tillid giver konkurrencefordele, og det kan VeriSign hjælpe jeres virksomhed med.

# 81%

af de briter, som handler på nettet, VeriSign Secured® Seal.

<sup>4</sup> Siden december 2009 har VeriSign SSL-certifikater med EV ifølge tests udført på en lang række websteder verden over medvirket til en stigning i antallet af besøgende, der vælger at handle på webstederne, fra 5 til 87% og i gennemsnit over 20%

<sup>5</sup> Tec-Ed, januar 2007

---

## OM VERISIGN

VeriSign (noteret på NASDAQ som VRSN) er e-handelsverdenens anerkendte leverandør af serviceydelser til internetinfrastruktur. Flere milliarder gange hver dag hjælper vi virksomheder og forbrugere verden over med at kommunikere og handle trygt ved hjælp af vores metoder til SSL, autentificering, identitetsbeskyttelse og registrering.

VeriSign er det førende certificeringscenter for SSL (Secure Sockets Layer) og leverer løsningerne til sikker e-handel og kommunikation på websteder, intranet og ekstranet. Som medlem af CA/Browser Forum, den frivillige organisation for SSL-certifikater med EV, er VeriSign fortsat den førende leverandør af SSL-certificering i branchen.



### Få mere at vide på [www.Verisign.dk](http://www.Verisign.dk).

\*Resultaterne for jeres virksomhed kan variere i forhold hertil. Specifikke faktorer i disse eksempler kan have spillet ind i forhold til de nævnte resultater. Kontakt VeriSign i dag og hør, hvordan vi kan levere den bedste løsning til jeres netsikkerhedsbehov.

