Gode råd om sikkerhed på internettet

Nedenfor gives en række gode råd og retningslinier til internetforretninger, der tager imod betalingskort. De gode råd tager udgangspunkt i de erfaringer, PBS International A/S indtil nu har fået i forbindelse med internethandel.

Kontrol af kundens oplysninger

I SSL løsningen er der ikke altid sikkerhed for, at kortet tilhører den, som betaler med det, og det er umiddelbart ikke muligt for PBS International at verificere kunden over for din forretning.

Du kan selv gøre meget for at minimere risikoen for misbrug

- Få oplyst et telefonnummer ved ordren, som kan sammenlignes med leveringsadressen.
- Ved alternativ leveringsadresse bør det kontrolleres, at det oplyste telefonnummer passer med betalingsadressen og ikke leveringsadressen.
- Ved levering til en c/o-adresse er en eventuel efterforskning besværliggjort. Bed derfor altid om yderligere oplysninger.
- Ved ordrer med mangelfulde oplysninger bør du altid kontakte kunden for at få flere oplysninger.
- Er der den mindste mistanke: Ring til kunden for bekræftelse af ordren. (For at denne kontrol har værdi, er det påkrævet, at telefonnummeret kan verificeres)
- Brug den sunde fornuft – Hvis det lyder for godt til at være sandt er der måske noget om snakken!
- Undgå enhver form for anonymisering af kunderne. Jo mere anonymitet – Jo større er risikoen for misbrug!
- Helt generelt bør man jævnligt analysere sine internationale kunder med henblik på at afdække en eventuel stigende interesse fra specielle lande / geografiske områder

Kontrol af den anvendte IP adresse (kan du ikke finde IP adressen – kontakt din betalingsløsningsleverandør)

Den geografiske placering af IP adresser kan kontrolleres på nettet (f.eks. www.db.ripe.net/whois)
Ved kontrol af IP adresser bør man være opmærksom på følgende:

- Er der match mellem IP adressen´s geografiske placering og leveringsadressen?
- Er der sammenfald i benyttede IP adresser? (F.eks. stigende antal ordrer fra forskellige kunder med tilnærmelsesvis matchende IP adresser)

Det kan i øvrigt anbefales, at blokere for IP adresser, der er relateret til misbrug (kontakt din betalingsløsningsleverandør for at høre nærmere om mulighed for blokering af IP-adresser)

Afsenders e-mail adresse

Vær opmærksom på ordrer fra afsendere med gratis e-mail adresse, da afsenderen ikke kan spores. Bed derfor om kundens private e-mail adresse.

International handel
Misbrug af betalingskort på nettet er et globalt fænomen. Internetforretninger kan risikere at blive ramt af misbrug blandt andet ved fremsendelse af varer på tværs af landegrænser. Du skal specielt være opmærksom på fremsendelse af varer til "Risiko-lande". Betegnelsen "Risiko Lande" kan ikke fast defineres, da det afhænger af udviklingen i misbrug.
Du bør derfor være opmærksom på, om ordrerne virker realistiske f.eks. mobiltelefoner sendt fra Danmark til Ghana eller en cykler sendt til Singapore!

Kunders adfærd
Vær opmærksom på:

- Nye kunder
- Ordrer, der er markant større end gennemsnittet
- Ordrer, hvor samme produkt bestilles flere gange
- Ordrer, der omhandler det / de dyreste produkter
- Kunder der ønsker hasteordrer – uanset omkostningerne
- Mange ordrer fra samme kunde over en relativ kort periode
- Ordrer, hvor der ikke er match mellem Leverings- og betalingsadresse

Afviste transaktionsforsøg
Såfremt det er teknisk muligt, bør man have oplysninger om alle transaktionsforsøg, herunder afviste transaktioner. Disse oplysninger bidrager til et samlet overblik over kundernes adfærd. F.eks. indikerer mange afvisninger forud for en godkendt betaling som regel, at der er tale om forsøg på misbrug.

(Denne form for misbrug kan reduceres betragteligt, såfremt man fastsætter grænser for, hvor mange transaktioner den enkelte kunde må foretage i en given periode)

3D Secure
Udover den interne kontrol af kunderne, bør man som forretning understøttes af sikkerhedsstandarden 3D Secure.
Fordelene ved 3D Secure er, at man som forretning, minimere sine økonomiske risici betragteligt.
Dog er det væsentligt at pointere, at 3D Secure ikke fritager forretningen for den interne kontrol .
Læs i øvrigt mere om 3D Secure på hjemmesiden www.pbsinternational.dk

Vær opmærksom på, at jo flere overvågningsparametre / sikkerhedskontroller der benyttes, jo større er chancen for at undgå / minimere risikoen for misbrug!

Brug af kontrolcifre
Du skal stille muligheden for brug af kontrolcifre til rådighed. Det betyder, at kortindehaveren udover kortnummer og udløbsdato kan opgive betalingskortets kontrolcifre ved kortbetaling på internettet.

Kontrolcifre er et trecifret tal - typisk de tre sidste cifre i en talrække - som er trykt bag på

betalingskort. Når kortindehaveren, i forbindelse med betaling med kort, oplyser kontrolcifrene, tjekker PBS International, at kontrolcifrene på dansk udstedte kort kommer fra samme betalingskort som det oplyste kortnummer og udløbsdato.

Når det drejer sig om udenlandsk udstedte kort, så er det ikke PBS International men kortudsteder, der tjekker, at kontrolcifrene stammer fra samme betalingskort som det oplyste kortnummer og udløbsdato - i den udstrækning, kortudsteder understøtter brugen af kontrolcifre.

PBS International tjekker, at kontrolcifrene på dansk udstedte kort kommer fra samme betalingskort som udløbsdato og kortnummer. Hvis det ikke er tilfældet, bliver transaktionen afvist. Dermed bliver din forretnings risiko for tab som følge af misbrug reduceret.

Det skal dog understreges, at det er din forretning, der dækker eventuelle tab forårsaget af misbrug af kortet - jf. betalingskortaftalen med PBS International.

Hvilke kort gælder det?

Der er kontrolcifre på alle Visa/Dankort samt alle dansk udstedte Eurocard/MasterCard, og de udgør en væsentlig del af alle betalingskort i Danmark. Der er endvidere kontrolcifre på de fleste udenlandsk udstedte Eurocard/MasterCard, Visa og JCB-kort.

Kontrolcifrene må ikke gemmes

Det er ikke tilladt at lagre eller på anden måde gemme kontrolcifrene, når betalingstransaktionen er gennemført. Det er din forretnings ansvar at sikre, at dette ikke sker.

Forretningens ansvar ved brug af SSL løsningen (jf. betalingskortaftalen)

- Der skal anvendes betalingssoftware, der er testet og godkendt af PBS International.
- Der skal årligt leveres en revisorattesteret ledelseserklæring, der bekræfter, at sikkerhedskravene til system, opbevaring m.m. overholdes, og der foreligger de nødvendige forretningsgange i forbindelse hermed.
- Din forretnings website skal som minimum leve op til de krav, der er angivet i betalingskortaftalen med hensyn til oplysninger m.m.
- Din forretning skal altid søge autorisation i forbindelse med køb..

Forretningens risici ved brug af SSL løsningen (jf. betalingskortaftalen)

Ved anvendelse af SSL løsningen har din forretning risikoen for 3. mandsmisbrug, uanset om det drejer sig om Dankort eller danske og udenlandske kreditkort. Det betyder med andre ord, at hvis rette kortindehaver på tro og love erklærer, at han/hun ikke har foretaget transaktionen, vil hele beløbet blive tilbageført fra din forretnings konto.

Derudover er der ligesom i den fysiske verden en begrænset dækningsgaranti på Dankort og Visa/Dankort på 1.000 kr. Det betyder, at hvis der ikke er dækning på kortindehavers konto, vil beløb over 1.000 kr. blive trukket på din forretnings konto. Dækningsgarantien gælder naturligvis ikke ved 3. mandsmisbrug.

Produkter og serviceydelser, som ikke kan sælges under den internationale betalingskortaftale

Vær opmærksom på, at forretninger med salg af pornografiske film, billeder eller lignende, som fremvises eller downloades via nettet mod betaling med et betalingskort, ikke kan anvende betalingskortaftalen til internationale betalingskort fra PBS International A/S. Det gælder også klubber m.m., som giver adgang til samme ydelser gennem salg af medlemsskaber.

Ligeledes kan virksomheder indenfor spil, lotteri, inkasso eller lignende heller ikke gøre brug af en betalingskortaftale til internationale kort.