

Forebyggelse af kortmisbrug i forbindelse med internet- og distancehandel, og hvad du kan gøre hvis skaden er sket



Udarbejdet i et samarbejde mellem FDIH, PBS og Rigspolitiet NITEC

Der kan svindles – men du kan selv gøre meget, for at forhindre det!

De fleste kunder er ærlige – men desværre kan man også møde kunder der ikke har reelle hensigter. Derfor er det vigtigt, at man som internetforretning er bevidst om at sikre sin forretning, hvad man gør hvis man modtager mistænkelige ordrer, samt hvad man gør hvis skaden er sket.

Nedenstående punkter beskriver i korte træk, hvad du som internetforretning skal være særligt opmærksom på for at forebygge misbrug, samt hvilke muligheder du har, hvis du har gennemført misbrugstransaktioner.

For uddybning af punkterne anbefales at læse "Sikkerhed ved modtagelse af kort – øvrig handel":
www.pbs.dk/da/produkter/internationale-betalingskort/fakta-og-fordele/sikkerhed/Pages/internethandel.aspx

Brug sund fornuft – Vær særlig opmærksom på handler der virker for gode til at være sande.

Kontrollér kundens oplysninger

- Få oplyst et telefonnummer, der kan relateres til kunden
- Kontrollér, at kundenavnet stemmer overens med de registrerede oplysninger på leveringsadressen
- Foretag yderligere verificering af kunder der anvender C/O-leveringsadresser og/eller gratis e-mailadresser (yahoomail, gmail osv.)
- Sammenhold IP-adresse med leveringsadressens geografiske placering
- Send ordrebekræftigelse via mail eller ring til kunden på det oplyste telefonnummer

Jo flere kunderrelaterede oplysninger I har – Jo bedre er jeres mulighed for at verificere kunden!

Kundens adfærd

- Er det en meget dyr vare?
- Er det en meget stor ordre?
- Bestilles samme produkt flere gange?
- Bestilles varerne om natten?
- Bestilles en hastelevering – uanset omkostninger?
- Bestiller samme kunde mange ting over relativ kort periode?
- Beder kunden om opdeling af betalingen på flere kortnumre? (dette er ikke tilladt og ofte ensbetydende med svindel).
- Er der tale om bestillinger fra lande / områder af verden, som I normalt ikke handler med?
- Er der mange afviste transaktionsforsøg i forbindelse med ordren?

Jo mere kundens adfærd afviger fra det normale – Jo større er risikoen for misbrug!

Tekniske foranstaltninger (kontakt evt. din leverandør af betalingsløsning for uddybning af tekniske muligheder)

- Implementering af 3D Secure (læs mere om denne betalingsløsning på <http://www.pbs.dk/da/temaer/sikker-nethandel/Pages/default.aspx>)
- Afvisning af IP-adresser / e-mailadresser, der er relateret til et allerede konstateret misbrug (chargeback)
- Implementering af misbrugsscreeningsværktøj (læs mere om PBS's screeningsværktøj på <http://www.pbs.dk/da/produkter/pbs-epayment/fakta-og-fordele/Pages/ePaymentogsikkerhed.aspx>)

Hvis varen skal leveres til kunden – vær opmærksom på fordele og ulemper ved de forskellige forsendelsesformer.

- Man opnår størst mulig sikkerhed, ved at det firma der leverer varerne, kræver underskrift som sammenholdes med ID papirer på personen som modtager ordren

Du mistænker en ordre til at være relateret til misbrug – hvad kan du gøre?

- Du kan bede om forudbetaling i form af kontooverførsel
- Som forretning bestemmer **du**, hvilke ordrer der skal gennemføres og hvilke der skal afvises

Du modtager en chargeback - hvad kan du gøre?

- Få overblik over hvilken ordre chargebacken refererer til og årsagen hertil. Evt. spørgsmål om den modtagne chargeback kan rettes til PBS Kundeservice -- betalingskort - punkt 7 – spørgsmål til indsigelse/chargeback. Find det på følgende link: <http://www.pbs.dk/da/temaer/kontakt-pbs/kundeservice/Pages/betalingskort.aspx>
- Hvis varen ikke er modtaget, kontakt da det anvendte transportfirma
- Anmeld sagen til politiet. Se nærmere herom nedenfor

Vejledning for netbutikker ved anmeldelse af bedrageri i forbindelse med handel på internettet.

Formålet med denne vejledning, er at du som internetforretning får en forståelse for, hvilke oplysninger du kan bidrage med til efterforskningen, hvis du har været udsat for svindel.

Anmeldelsen kan med fordel udfærdiges skriftligt og skal fremsendes via post til dit lokale politi.

For at sikre et overblik over eventuelle sags sammenhænge på tværs af sager, anmodes du om at fremsende en kopi af den skematiske anmeldelse til mailadressen:

it-kriminalitet@politi.dk eller med post til

Rigspolitiet

Nationalt IT Efterforskningscenter,

Polititorvet 14,

1780 København V

Inden du udfærdiger din anmeldelse til Politiet er der det vigtigt, at du har sikret elektroniske oplysninger der måtte være i sagen. Det kræver, at du kender dit system og ved hvilke oplysninger du kan trække ud af det. Det er her vigtigt, at oplysningerne er korrekte og ikke ved en fejl er blevet ændret, da de eventuelt skal tjene som bevis i en kommende retssag.

Nedenstående punkter beskriver kort hvilke informationer din anmeldelse bør indeholde.

Hvem er det der anmelder?

- Virksomhedens navn, adresse, evt. CVR.nr og web-adresse
- Personen der anmelder, navn, stilling, kontakt oplysninger

Hvad er det du vil anmelde?

- Bedrageri hvor der er betalt med falsk/stjålet kreditkort
- Bedrageri hvor kunden nægter modtagelsen af varen og du kan bevise det modsatte
- Andre forhold

Hvornår er det sket?

- Dato, tid – for hvornår handlen er oprettet/logget i betalingssystemet eller på websiden. Det er her vigtigt at angive hvilken tidszone der er anvendt og evt. fejl i tidsangivelsen i forhold til dansk normaltid

Hvordan er det sket?

- Kort beskrivelse af hændelsesforløbet hvor du med dine egne ord beskriver hvad der er sket

Hvem er det du anmelder?

- Kundens navn, adresse, telefon nr. e-mailadresse
- Kundens IP-adresse
- Leveringsadresse hvis den ikke er identisk med kundens

Yderligere oplysninger

- Oplysninger om varen evt. serie nr.
- Erstatningskrav
- Transaktionsnummer
- Forsendelsesoplysninger
- Har der været e-mail korrespondance eller telefonisk kontakt til kunden

Dokumentation der vedlægges

- Udskrift af ordrebekræftelse eller faktura
- Track & trace med evt. kvittering
- Udskrifter af e-mails med header oplysninger evt. vedlægges elektronisk som fil i .msg format
- Anden dokumentation

Er der mere end en sag er det vigtigt, at sagerne ikke blandes sammen. Det skal af anmeldelsen tydeligt fremgå hvilke oplysninger der hører til hvilken sag. Der kan evt. oprettes et regneark til at skabe overblik.

Anmeldelse

sæt X

Vedrørende:	Bedrageri hvor der er anvendt falsk/stjålet kreditkort	
	Bedrageri i øvrigt	

Undertegnede anmelder hermed at

Forurettede				
Virksomhedens navn:				
Adresse				
Gade + nr		Postnr:		By:
Telefonnummer:		Mobil		
e-mail:				
www. Adresse:				
CVR-nr:				
Anmelder				
navn:				
stilling:				
Adresse:				
Gade + nr.		Postnr:		By:
Telefonnummer:		Mobil		
e-mail:				
CPR-nr:				
Gerningstidspunkt (tidsrum) - husk tidszone				
Fra	Dato		Tid	
Til	Dato		Tid	
Beskrivelse af sagen.				

Beskrivelsen kan evt. fortsættes på ny side

Sagens Person (Kunde oplysninger)

Navn :			
Adresse			
Gade + nr.:		Postnr:	By:
Telefonnummer:		Mobil	
e-mail:			
IP adresse:			
Evt. Leveringsadresse:			
Sagens genstand			
Varens art:		Serienr.	
Ordre nr.			
Varens pris		Erstatningskrav	
Betalingsoplysninger			
Gennemført /afvist			
Transaktionsnr.			
Yderligere oplysninger			
Dokumentation der vedlægges i kopi eller elektronisk på læsbart medie.			
Ordrebekræftelse		Udskrift af e-mails med headeroplysninger	
Track & Trace		Anden dokumentation	

Dato :

.....
Underskrift