

OUCH!

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

# Sikker netthandel

## Oversikt

Jula nærmer seg for mange av oss, og snart vil millioner av mennesker være på utkikk etter den perfekte julegaven. Mange foretrekker å handle på nett for å finne gode tilbud og unngå bråkete folkemengder. Dessverre vil cyberkriminelle også være aktive på denne tiden av året. De lager falske nettbutikker og bruker også andre metoder for å svindle folk. I denne utgaven forklarer vi hvordan du kan handle på nettet på en sikker måte, og dermed unngå å bli et offer for svindel.

## Falske nettbutikker

Cyberkriminelle lager falske nettbutikker som etterligner utseende til ekte nettbutikker, eller som misbruker navn og varemerke til kjente nettbutikker og kjeder. Når du søker etter de beste tilbudene på nett, kan det hende at du havner på en slik falsk side. Hvis du handler på slike nettsider kan du ende opp med å få tilsendt forfalskede produkter eller tyvgods, eller det kan hende at du ganske enkelt ikke får det du kjøper. Beskytt deg selv mot falske nettbutikker:



Om mulig, hold deg til nettbutikkene du allerede kjenner til, stoler på, og har handlet hos før. Lagre nettbutikker du har besøkt før og stoler på som favoritter.



Se opp for priser som er markant bedre enn de du finner på de vanlige nettbutikkene. Hvis et tilbud virker for godt til å være sant, så er det som regel det.



Vær på vakt hvis en nettbutikk ligner en du har brukt før, men domenet eller navnet er litt annerledes. F.eks. kan det tenkes at du er vant til å handle fra Amazon, viss domene er amazon.com. Dersom du da skal handle på en nettbutikk som ligner på Amazon, men domenet er amaz0n.com med en '0' istedenfor en 'o', bør du styre unna.



Skriv inn navnet eller nettadressen til nettbutikken i en søkemotor for å se hva andre har sagt om den. Vær på utkikk etter ord og uttrykk som f.eks. «svindel» eller «falsk».



Bruk et unikt passord for alle dine brukerkontoer på nett. Dersom du sliter med å huske alle de forskjellige passordene, kan du ta i bruk et passordhåndteringsprogram, også kjent som en password manager.

## Svindlere på legitime sider

Vær på vakt selv når du handler på pålitelige nettsider. Enkelte nettsteder baserer seg på at privatpersoner og andre selskaper står for varesalget heller enn nettsiden selv. Enkelte av disse kan ha onde hensikter og være ute etter å svindle folk. Slike nettsider er som markeds plasser i den fysiske verden, enkelte selgere er mer til å stole på enn andre. Sjekk hver selgers rangering før du avtaler et kjøp. Vær på vakt for selgere som er nye på nettstedet, eller som selger varer til unormalt lave priser. Se over nettstedets bruksvilkår for kjøp fra slike tredjeparter. Om du er i tvil, kjøp varer som selges direkte av nettstedet selv, eller om det ikke lar seg gjøre, fra en offisiell forhandler.

## Betaling på nett

Se over transaksjonene fra bank- og kredittkort jevnlig, slik at du kan oppdage mistenkelige trekk. Dersom det er mulig, aktiver varsling over e-post, SMS, eller app hver gang det skjer et trekk fra kortet du bruker til netthandel. Dersom du finner mistenkelig aktivitet, ring banken du har kortet hos med en gang og meld fra. Bruk heller kredittkort på nett enn bankkort. Med bankkort trekkes pengene direkte fra din egen konto, dersom du blir svindlet vil det da være mer utfordrende å få tilbake pengene. Et annet alternativ er å bruke velkjente tjenester for nettbetaling, som PayPal, slik at du slipper å oppgi kortnummeret til nettbutikken du handler hos. Du kan også vurdere å bruke et gavekort ved den aktuelle nettbutikken.

Bare fordi en nettbutikk har bra design og et profesjonelt utseende, betyr det ikke at nettsiden er til å stole på. Hvis nettsiden gjør deg ukomfortabel, så la være å bruke den. I stedetfor, gå til en velkjent side du kan stole på, som du har brukt før uten problemer. Du får kanskje ikke et like utrolig tilbud, men du er i større grad sikret å ende opp med et legitimt produkt, og unngår å bli svindlet.

## Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

## Gjesteredaktør

*Lenny Zeltser er IT-sikkerhetssjef ved Axonius og seniorinstruktør og forfatter for SANS-instituttet.*

*Du kan følge ham på Twitter som [@lennyzeltser](#), og lese bloggen hans på [zeltser.com](#).*



## Ressurser

Sosial manipulering: <http://www.sans.org/u/X7k>

Svindel gjennom sosiale medier: <http://www.sans.org/u/X7p>

Passord gjort enkelt: <http://www.sans.org/u/Xu9>

*OUCH! utgis av SANS Security Awareness, og er distribuert under [Creative Commons BY-NC-BD 4.0 lisensen](#). Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Redaksjon: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Oversatt av: NorSIS*