SANS SECURITY AWARENESS
NorSIS Norsk senter for informasjonssikring
OUCH! | November 2017
Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Falske nettbutikker**
- **Din datamaskin / mobile enhet**
- **Ditt betalingskort**

Sikker netthandel

Oversikt

Juletiden nærmer seg, og snart vil millioner av mennesker over hele verden begynne å lete etter den perfekte gaven å kjøpe. Mange av oss vil da velge å handle på nettet, for å finne bra tilbud, og unngå lange køer og utålmodige folkemengder. Dessverre er dette også årstiden hvor mange cyberkriminelle lager falske nettbutikker for å svindle og stjele fra andre. Her forteller vi om risikoene ved netthandel, og hvordan du kan benytte deg av det utrolige tilbudet på en sikker måte.

Gjesteredaktør

Lenny Zeltser lager sikkerhetsprodukter hos Minerva Labs, og lærer bort skadevarebekjempelse ved SANS instituttet. Lenny er aktiv på Twitter som **@lennyzeltser**, og skriver sikkerhetsblogg på **zeltser.com**.

Falske nettbutikker

Selv om mange nettbutikker er legitime finnes det noen falske som er satt opp av cyberkriminelle. De lager disse falske nettsidene ved å kopiere utseende til ekte nettbutikker, og benytte navnene til velkjente kjeder og merker. De benytter seg så av disse svindelsidene til å lure folk som ser etter gode tilbud. Når du søker på nett etter de aller laveste prisene kan du oppleve å bli ledet inn på et slikt falskt nettsted. Når du skal velge nettsted å kjøpe fra, bør du derfor være på vakt ovenfor nettbutikker med priser som er dramatisk lavere enn alle andre, eller som tilbyr varer som er utsolgt de fleste andre steder. Grunnen til at det er så billig og tilgjengelig, er at det du kjøper ikke er legitimt, er forfalsket eller tyvgods, eller i mange tilfeller ikke blir levert i det hele tatt. Beskytt det selv på følgende måte:

- Hold deg så langt det er mulig til nettbutikker du kjenner til og stoler på, som du har handlet hos før uten problem.
- Sjekk at nettsiden har en legitim postadresse og et telefonnummer for salg eller kundeservice. Om en nettside virker mistenkelig, ring dem for å få snakke med et menneske. Dersom det ikke er mulig å få til det, er det et tegn på at det kan være en falsk nettside.
- Se etter åpenbare faresignaler som tilbud som er for gode til å være sanne, eller dårlig språk.
- Det er veldig mistenkelig når en nettside fremstår som en eksakt kopi av en velkjent nettside du har brukt før, men med små forskjeller i nettstedsdomenet eller navnet. Du er for eksempel kanskje vant til å handle hos Amazon,

Sikker netthandel

som har nettadressen https://www.amazon.com. Men vær veldig på vakt om du opplever å havne på nettsider som utgir seg får å være Amazon, som http://store-amazoncom.com.

- Søk på nettbutikkens navn i en søkemotor for å finne ut av hva andre har sagt om den. Se etter utrykk som «svindel», «aldri mer» og «falsk», og for utenlandske aktører, engelske uttrykk som «fraud», «scam», «never again» og «fake». En mangel på anmeldelser kan tyde på at nettsiden er veldig ny, og kanskje ikke er til å stole på.
- Sørg for at tilkoblingen din til nettbutikken er kryptert før du foretar et kjøp. De fleste nettlesere viser at tilkoblingen er kryptert med et hengelåsikon og/ eller bokstavene HTTPS i grønt like før navnet på nettsiden i adressefeltet.

Beskytt deg selv ved å kun handle på pålitelige nettsider med et godt etablert rykte.

Husk at en nettside ikke nødvendigvis er legitim bare fordi den ser proff ut. Om du ikke er komfortabel med nettsiden, ikke bruk den. Istedenfor kan du finne en velkjent nettside du stoler på eller har brukt uten problem tidligere. Du finner kanskje ikke et like fantastisk tilbud, men du ender sannsynligvis opp med et legitimt produkt, og slipper å få personopplysninger og betalingsinformasjon stjålet.

Din datamaskin / mobile enhet

I tillegg til å handle i legitime nettbutikker, burde du sørge for at din datamaskin eller mobile enhet er sikker. Cyberkriminelle vil forsøke å infisere enhetene dine med skadelig programvare for å kunne stjele informasjon om bankkontoer, betalingskort, og passord. Ta grep for å holde enhetene dine sikre:

- Har du barn i huset, vurder å ha minst to enheter. En for voksen, og en for barna. Barn er nysgjerrige og utforskende med teknologi, derfor er det mer sannsynlig at de kan komme til skade for å infisere sine egne enheter. Ved å bruke en separat datamaskin eller mobil enhet kun for transaksjoner på nett, som nettbank og netthandel, reduserer du risikoen for å bli infisert.
- Installer alltid de nyeste oppdateringene, og kjør oppdatert antivirus-programvare. Dette gjør det langt vanskeligere for cyberkriminelle å infisere enheten din.

Sikker netthandel

Ditt betalingskort

Følg jevnlig med på kontoutskriften eller fakturaen for kortet du bruker for å kunne avsløre mistenkelige trekk, særlig etter at du nettopp har gjort mange kjøp på nett, eller tatt i bruk en ny nettbutikk. Noen leverandører tilbyr en tjeneste der du får et e-postvarsel hver gang kortet brukes, eller bruken overstiger et gitt beløp. Et annet alternativ er å ha et eget kort kun for netthandel. Da kan du enkelt bytte ut kortet om det blir kompromittert, uten at det påvirker andre betalingsaktiviteter. Ring banken eller kredittkortselskapet med en gang dersom du mistenker at du har blitt utsatt for svindel. Dette er også grunnen til at det er en fordel å bruke kredittkort fremfor bankkort for netthandel. Med bankkort trekkes pengene direkte fra din bankkonto, om du blir utsatt for svindel kan det da være langt vanskeligere å få tilbake pengene sine. Til sist, vurder å bruke kredittkort der det genereres et unikt kortnummer for hvert nettkjøp, bruk gavekort, eller bruk en velkjent betalingsløsning som f.eks. PayPal, der du ikke er nødt til å oppgi kortnummeret ditt når du skal handle.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

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.

Ressurser

Sosial manipulering:	https://securingthehuman.sans.org/ouch/2017#january2017
Fire viktige sikkerhetstiltak:	https://securingthehuman.sans.org/ouch/2016#october2016
Slik sikrer du hjemmenettverket ditt:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Dagens sikkerhetstips:	https://www.sans.org/tip_of_the_day.php

Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS