OUCH! | November 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

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

Sikker netthandel

Vær forsiktig i denne sesongen

Julesesongen nærmer seg, og millioner av mennesker verden rundt vil være på utkikk etter den perfekte gaven. Mange vil velge å handle på nettet for å få bedre tilbud, og for å unngå lange køer og utålmodige folkemengder. Dessverre er dette også de kriminelles favorittårstid for svindel på nettet og finanssvindel. Denne måneden forteller vi om farene ved å handle på nettet, og forskjellige metoder du kan bruke for å beskytte deg selv.

Gjesteredaktør

Jonathan Homer (**JonathanLHomer**) er en anerkjent leder i Cyber Security Awareness industrien og er aktiv innen både regjeringen og privat sektor. Jon har spesialisert seg på publikum engasjement og ledende trening teknikker.

Falske nettbutikker

Selv om de fleste nettbutikker er ekte, er det noen som ikke er det, de er falske nettsider som er laget av kriminelle. Kriminelle lager disse falske nettsidene ved å kopiere utseende til, eller bruke merkenavnet til kjente nettbutikker. De bruker så disse nettsidene til å svindle folk som ser etter det beste tilgjengelige tilbudet. Når du søker på nettet etter de absolutt laveste prisene kan du komme til å havne på en av disse falske nettsidene.

Når du skal velge en nettside å kjøpe noe fra, vær obs på nettsider som reklamerer med priser som er dramatisk billigere enn noen andre steder, eller nettsider som tilbyr produkter som er utsolgt overalt ellers. Grunnen til at det de tilbyr er såpass billig eller tilgjengelig, er fordi det du mottar ikke er ekte, fordi det er tyvgods eller en forfalskning, eller så får du ikke noe i det hele tatt. Gjør dette for å beskytte deg selv:

- Forsikre deg om at nettsiden har en ekte e-postadresse eller telefonnummer for salgsspørsmål og generell hjelp. Hvis nettsiden ser mistenkelig ut, ring og snakk med et menneske.
- Se etter åpenbare varselsignaler som dårlig grammatikk og stavefeil.
- Vær veldig mistenksom hvis nettsiden ser ut til å være en eksakt kopi av en kjent nettside som du har brukt før, men domenenavnet eller navnet på nettbutikken er litt annerledes. Du er for eksempel kanskje vant til å gå til nettsiden https://amazon.com for all shopping fra Amazon. Da bør du være veldig mistenksom hvis du havner på en nettside som gir seg ut for å være Amazon, med URL-en http://store-amazon.com.

Sikker netthandel

- Søk på nettbutikkens navn eller URL i en søkemotor, og se hva andre folk har sagt om nettsiden fra før. Se etter utrykk som «svindel», «aldri igjen», eller «falsk». En mangel på anmeldelser er heller ikke et godt tegn, fordi det indikerer at nettsiden er veldig ny.

Husk, bare fordi nettsiden ser profesjonell ut, behøver ikke det bety at den er ekte. Du bør ta deg tid til å undersøke dersom noe ved nettsiden virker mistenksomt. Dersom du føler deg utrygg med nettsiden, burde du ikke bruke den. Istedenfor kan du bruke en godt kjent nettside som du kan stole på, eller en du selv har brukt og kjenner til fra før. Du finner kanskje ikke like gode tilbud, men det er mye større sjanse for at du ender opp med et lovlig og godt produkt, og at du slipper betalingsanmerkninger.

Hold deg beskyttet på nettet ved å kun handle på nettsider med et godt etablert rykte.

Din datamaskin / mobile enhet

I tillegg til å handle fra legitime nettsider, bør du forsikre deg om at datamaskinen din eller mobilen/nettbrettet ditt er sikker å bruke. Cyberkriminelle vil forsøke å infisere enhetene dine, slik at de kan samle inn informasjon om bankkontoene dine, kredittkortinformasjonen din, og passord. Ta disse grepene for å holde enhetene dine sikre:

- Vurder å ha to enheter dersom du har barn i huset. Én for barna og én for de voksne. Barn er nysgjerrige og interaktive med teknologi, og som et resultat av det er det større sjanse for at de infiserer sin egen enhet. Ved å bruke en separat datamaskin eller nettbrett kun for nettbank og netthandel, reduserer du sjansen for å bli infisert. Hvis separate enheter ikke er en mulighet bør du ha separate brukerkontoer på den delte enheten. Pass på at barna ikke har administrator-rettigheter.
- Handle bare i nettbutikk eller bruk nettbanken når du er på et trådløst nettverk som du kan stole på, slik som hjemmenettet ditt. Bruk av offentlige nett som på en internett-kafé kan være bra for å lese nyheter, men ikke for å få tilgang til nettbanken din.
- Installer alltid de nyeste oppdateringene, og kjør oppdatert antivirus-programvare. Dette gjør det vanskeligere for cyberkriminelle å infisere enheten din.

Ditt kredittkort

Hold øye med kontoutskriften din slik at du kan identifisere mistenkelige transaksjoner. Du bør gjennomgå kontoutskriften

Sikker netthandel

jevnlig, minst én gang i måneden. Noen kredittkortselskaper og banker har mulighet til å sende deg varsler på SMS hver gang det blir gjort et trekk fra kortet ditt, eller hvis et trekk blir gjort som er større enn et visst beløp. En annen mulighet er å ha et kort kun for netthandel, på den måten kan du enkelt bytte ut dette hvis det blir kompromittert, uten at det vil påvirke andre betalingsaktiviteter. Ring kredittkortselskapet eller banken med en gang hvis du tror du har blitt utsatt for svindel, og forklar situasjonen. Dette er også en grunn til at kredittkort er bedre for netthandel enn bankkort. Med bankkort trekkes pengene rett fra bankkontoen din, og hvis du da blir utsatt for svindel kan det være langt vanskeligere å få pengene dine tilbake.

Til slutt bør det også nevnes at det finnes ny teknologi som gjør det mulig for deg å betale uten å eksponere kortnummeret ditt. Vurder å bruke kort som genererer et unikt kortnummer for hvert kjøp på nettet, eller bruk godt kjente betalingsløsninger som PayPal, som ikke krever at du oppgir kortnummeret til den du kjøper fra.

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 http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på https://norsis.no.

Ressurser

Fem steg for å holde seg sikker:	https://www.securingthehuman.org/ouch/2014#october2014
Sikre ditt hjemmenettverk:	https://www.securingthehuman.org/ouch/2014#january2014
Sikre ditt nye nettbrett:	https://www.securingthehuman.org/ouch/2013#december2013
SANS Dagens sikkerhetstips:	https://www.sans.org/tip_of_the_day.php

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Oversatt av: Mats Authen