SANS SECURITY AWARENESS
WelcomeSecurity Enabling value through it security
OUCH! | November 2017
Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Falske onlinebutikker
- Din computer / mobile enhed
- Dit kreditkort

Sådan handler du sikkert online

Oversigt

Julen nærmer sig for mange af os, og snart vil millioner af mennesker rundt om i verden forsøge at købe de perfekte gaver. Mange af os vil vælge at shoppe online i vores jagt efter gode tilbud og for at undgå lange køer og flokke af utålmodige julehandlende. Desværre er dette også tidspunktet på året, hvor mange IT-kriminelle opretter falske online butikker for at snyde og stjæle fra andre. Nedenfor forklarer vi risiciene ved at handle online og hvordan du kan få et fantastisk tilbud på en sikker måde.

Gæsteredaktør

Lenny Zeltser laver sikkerhedsprodukter ved Minerva Labs og underviser i bekæmpelse af malware ved SANS Institute. Lenny er aktiv på Twitter som **@lennyzeltser** og skriver en sikkerhedsblog på **zeltser.com**.

Falske onlinebutikker

Mens mange onlinebutikker er legitime, er der nogle falske hjemmesider, der er oprettet af IT-kriminelle. IT-kriminelle opretter disse falske hjemmesider ved at kopiere udseendet af rigtige websider eller ved at bruge navne på velkendte butikker eller mærker. De bruger derefter disse falske websider til at snyde folk, der søger den bedste mulige handel. Når du søger online efter de absolutte laveste priser, skal du vide at disse hjemmesider er målrettet en som dig. Når du vælger en hjemmeside hvorfra du vil foretage dit køb, skal du være forsigtig med at købe ved websteder, der reklamerer med priser, der er markant billigere end andre steder eller websider, der tilbyder produkter der er udsolgt i resten af landet. Årsagen til, at deres produkter er så billige eller tilgængelige, er, fordi det du modtager ikke er ægte, kan være forfalsket eller stjålet, eller i nogle tilfælde bliver det aldrig leveret. Beskyt dig selv ved følgende:

- Når det er muligt, køb fra websider, som du allerede kender, stoler på og som du tidligere har handlet ved.
- Kontroller, at websiden har en legitim postadresse og et telefonnummer til salgs- eller supportrelaterede spørgsmål. Hvis websiden ser mistænkelig ud, skal du ringe til og tale med et menneske. Hvis du ikke kan få fat i nogen til at tale med, er det et tegn på, du har at gøre med en falsk hjemmeside.
- Se efter indlysende advarselsskilte som tilbud, der er for gode til at være sande eller dårlig grammatik og stavning.
- Vær meget mistænksom hvis en hjemmeside er en eksakt kopi af en webside, du tidligere har brugt, men websidens domænenavn eller navnet på butikken er lidt anderledes. For eksempel kan det være du er vant til at handle

Sådan handler du sikkert online

online hos Amazon, hvis hjemmeside er https://www.amazon.com. Vær meget mistænksom, hvis du befinder dig på websider som foregiver at være Amazon, som http://store-amazoncom.com.

- Indtast butikkens navn eller web-adresse i en søgemaskine og se, hvad andre mennesker har sagt om hjemmesiden. Søg efter udtryk som "bedrageri", "fidus", "aldrig igen" eller "falsk." Manglende anmeldelser kan også være et tegn på, at hjemmesiden er meget ny og muligvis ikke troværdig.
- Før du køber varer, skal du sikre dig, at din forbindelse til hjemmesiden er krypteret. De fleste browsere viser en krypteret forbindelse med en lås og/eller bogstaverne HTTPS i grøn lige før websidens navn.

Beskyt dig når du handler på nettet ved kun at handle på betroede hjemmesider med et veletableret ry.

Husk, at bare fordi websiden ser professionelt ud, betyder det ikke, at det er legitimt. Hvis du ikke er fortrolig med hjemmesiden, skal du ikke bruge den. I stedet skal du finde en velkendt hjemmeside, du stoler på eller en, som du tidligere har brugt. Det kan godt være, at du ikke finder det bedste tilbud, men du er meget mere tilbøjelig til at ende med et legitimt produkt og undgå at have dine personlige og økonomiske data stjålet.

Din computer / mobile enhed

Ud over at shoppe på legitime hjemmesider, bør du sikre dig at din computer og mobile enheder er sikre. IT-kriminelle vil forsøge at inficere dine enheder, så de kan høste dine bankkonti, kreditkreditoplysninger og adgangskoder. Følg nedenstående trin for at holde dine enheder sikret:

- Hvis du har børn i dit hus, bør du overveje at have to enheder, en til dine børn og en til de voksne. Børn er nysgerrige og interagerer med teknologi, som følge heraf er de mere tilbøjelige til at inficere deres egen enhed. Ved at bruge en separat computer eller tablet kun til online-transaktioner, såsom netbank og nethandel, reducerer du chancen for at blive inficeret.
- Installer altid de nyeste opdateringer og kør up-to-date anti-virus software. Dette gør det meget sværere for en IT-kriminel at inficere din enhed.

Sådan handler du sikkert online

Dit kreditkort

Gennemgå regelmæssigt dine kreditkortopgørelser for at identificere mistænkelige køb, især efter at du har brugt dine kort til at foretage mange online-køb eller brugt et nyt online-websted. Nogle kreditkortudbydere kan underrette dig via e-mail eller SMS, hver gang der opkræves et beløb på dit kort eller når beløbet overstiger et bestemt beløb. En anden mulighed er at have ét kreditkort kun til online handel, på den måde hvis det er kompromitteret, kan du nemt ændre kortet uden at påvirke nogen af dine andre betalingsaktiviteter. Hvis du mener, at der er begået bedrageri, skal du straks kontakte dit kreditkortselskab. Det er også derfor, du skal bruge kreditkort til alle online handler, undgå at bruge betalingskort, når det er muligt. Debetkort trækker pengene direkte fra din bankkonto. Hvis der er begået bedrageri, kan det være meget sværere at få pengene tilbage. Endelig bør du overveje kreditkort, der genererer et unikt kortnummer til hver eneste nethandel, gavekort eller bruge kendte betalingstjenester, som f.eks. PayPal, som ikke kræver, at du oplyser dit kreditkortnummer til sælgeren.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Tidligere udgivelser

Social engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Fire gode råd om sikker brug af computere:	https://securingthehuman.sans.org/ouch/2016#october2016
Securing Your Home Network (ikke oversat til dansk:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

Licensinformation

Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity