OUCH! | Januar 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Slik sikrer du ditt nettbrett**
- **Slik holder du det sikkert**

Slik sikrer du ditt nye nettbrett

Oversikt

Gratulerer med ditt nye nettbrett! Dette er kraftfull teknologi for å kommunisere med andre, handle på nettet, se filmer, spille spill og gjøre haugevis med andre aktiviteter. Siden nettbrettet ditt sannsynligvis blir en viktig del av livet ditt, den vil kanskje til og med erstatte PC-en din, burde du ta noen nøkkelgrep for å holde nettbrettet ditt og informasjonen din trygg og sikker.

Gjesteredaktør

Lori Rosenberg har omfattende erfaring med å utforme utdanningsmateriell innen informasjonssikkerhet for trening av både ansatte og kunder, og er lidenskapelig når det kommer til å finne nye og engasjerende metoder for å dele denne kunnskapen. Hun finnes på Twitter som **@InfoSecLori**.

Slik sikrer du ditt nettbrett

Det vil kanskje virke overaskende at den største risikoen mot nettbrettet ditt ikke er hackere, men deg selv. Det er mye mer sannsynlig at du mister nettbrettet ditt, glemmer det, eller får det frastjålet enn at noen hacker det. Det første du burde gjøre for å beskytte ditt nettbrett, er å aktivere automatisk skjermlås. Dette vil si at hver gang du ønsker å bruke nettbrettet, må du først låse opp skjermen med enten en sterk tallkode eller et passord, et mønster, eller fingeravtrykket ditt. Dette sørger for at ingen kan få tilgang til nettbrettet ditt hvis det blir mistet eller stjålet. All din personlige informasjon, appene dine, og alt annet du måtte ha lagret på den er beskyttet. Her er noen ekstra tips til hvordan du beskytter nettbrettet ditt, som kan brukes når automatisk skjermlås har blitt aktivert:

1. Installer eller aktiver programvare for å kunne spore nettbrettet via internett. På denne måten kan du koble deg til det og finne ut hvor det er dersom det blir stjålet eller mistet, og i verste tilfelle vil du også kunne fjern-slette all informasjonen på det.
2. Oppdater enheten din, og aktiver automatiske oppdateringer, slik at den alltid kjører den siste versjonen av operativsystemet. Angripere ser alltid etter nye svakheter og sikkerhetshull i programvare, som kontinuerlig blir tettet av utgivere ved at de gir ut patcher. Ved å alltid kjøre siste versjon av operativsystemet, og siste versjon av apper, gjør du det mye vanskeligere for noen å hacke seg inn på enheten.

Slik sikrer du ditt nye nettbrett

3. Vær oppmerksom når du konfigurerer nettbrettet for første gang, spesielt når det kommer til personverninnstillingene. En av de største personvernsutfordringene med et nettbrett er at det kan være mulig for andre å spore deg og vite hvor du befinner deg. Vi anbefaler at du skrur av kommunisering av posisjon for alle apper, for så å skru det på kun for de appene som du føler trenger det. For noen apper er det viktig å vite hvor du befinner deg, f.eks. kart-apper, eller apper som hjelper deg med å f.eks. finne nærmeste restaurant. De fleste apper har ikke behov for å få informasjon om posisjonen din i sanntid.
4. De fleste nettbrett og apper på disse lagrer informasjon i skyen. Derfor er det viktig at du forstår hvor dataene dine befinner seg, og hvordan de er sikret. For eksempel er det siste du ønsker at private bilder skal bli delt på internett, synlige for hele verden, sammen med geolokasjonsdata om hvor bildene er tatt. Som hovedregel burde du skru av deling til nettskyen, og bare skru det på dersom du ønsker å dele noe spesifikt.
5. Nettbrett synkroniserer i større grad appene dine med andre enheter, som smarttelefonen din eller PC-en din. Synkronisering kan være en kjempeflott funksjon, men vær forsiktig med hvilke apper du tillater at synkroniserer informasjon. Ikke bli overrasket hvis du har på synkronisering, og ser nettsider du besøkte på nettbrettet dukke opp i nettleseren på PC-en din på jobben.

Den beste måten å sikre nettbrettet ditt på, er å skru på skjermlås, gå gjennom personverninnstillinger, og holde nettbrettet oppdatert.

Slik holder du det sikkert

Når du har sikret nettbrettet, må du sørge for at det holder seg sikkert. Her er noen nøkkelgrep for å holde nettbrettet sikkert på lang sikt.

- Aldri hack eller jailbreak ditt eget nettbrett. Dette vil omgå og rekke sikkerhetsfunksjonaliteter og gjøre dem ubrukelige, noe som gjør nettbrettet ditt mye mer sårbart for angrep.
- Last bare ned apper du trenger, og bare fra pålitelige kilder. For iPader, last bare ned apper fra iTunes. Disse appene er testet av Apple før de blir gjort tilgjengelige. For Google anbefaler vi at du laster ned apper kun fra Google Play, og for Amazon nettbrett anbefaler vi at du holder deg til Amazon App Store. Det er mulig å laste ned

Slik sikrer du ditt nye nettbrett

apper fra andre steder, men disse er ikke testet på samme måte, og kan være infiserte. Til slutt anbefaler vi deg å avinstallere og slette appen når du ikke lenger bruker den, uavhengig av hvor du fikk tak i den.

- Sørg for at du går gjennom og velger personvernsinnstillingene når du installerer en ny app, akkurat slik som når du opprinnelig konfigurerte nettbrettet. Vær forsiktig med hva du gir hver enkelt app tilgang til. For eksempel, trenger appen du nettopp lastet ned virkelig tilgang til vennene dine og kontaktinformasjonen din? Hvis du er ukomfortabel med tilgangskravene til en app, bør du finne en annen som dekker samme behov. I tillegg burde du regelmessig sjekke tilgangskravene for å forsikre deg om at de ikke har endret seg.

Nettbrettet ditt er et kraftfullt verktøy, som vi vil at du skal bruke og ha det fint med. Bare husk at disse få enkle stegene kan være veldig nyttige for å holde deg og ditt nye nettbrett trygge.

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

Sikker bruk av mobilapplikasjoner:	https://www.securingthehuman.org/ouch/2015#january2015
Passordsetninger:	https://www.securingthehuman.org/ouch/2015#april2015
Bruke nettskyen sikkert:	https://www.securingthehuman.org/ouch/2014#september2014
Avhende mobile enheter:	https://www.securingthehuman.org/ouch/2014#june2014
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