OUCH! | February 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Forhåndssjekk
- Tapte/stjålne enheter
- Trådløse nett
- Offentlige datamaskiner

Sikker mens du reiser

Oversikt

Vi vil at du skal få mest mulig ut av teknologien til enhver tid, også når du er ute og reiser. I dette nyhetsbrevet skal vi gå gjennom hvordan du kan få kommet deg på nett og brukt enhetene dine på en sikker måte mens du er på reisefot.

Gjesteredaktør

Mark Williams er Enterprise Security Architect ved BlueCross Blueshield of Tennessee. Han er også instruktør hos SANS og president for ISSA i Chattanooga. Han har reist mye, og forstår problemene som kan oppstå når man har med seg de tekniske enhetene sine.

Forhåndssjekk

Nettverket du bruker hjemme eller på jobben er kanskje sikkert, men når du er ute på reise burde du anta at ingen nettverk er til å stole på. Du vet aldri hvem andre som kanskje bruker det, og hva de driver med. Her er noen enkle grep som kan være til mye hjelp i å beskytte deg og dine data før du drar på reise.

- Den tryggeste informasjonen er den du ikke har. Finn ut hva du ikke trenger av informasjon på de forskjellige enhetene du tar med, og fjern den informasjonen. Dette kan betraktelig redusere konsekvensene dersom enhetene mistes, stjeles, eller blir konfiskert i tollen eller av grensevakter.
- Lås dine mobile enheter og/eller laptop med et sterkt passord eller tilsvarende. På denne måten kan ikke folk få tak i informasjonen din selv om enheten kommer på avveie. I tillegg burde du aktivere full-disk kryptering på dine mobile enheter og bærbare datamaskiner. For de fleste mobile enheter er dette automatisk aktivert når du bruker en skjermlås.
- Installer eller aktiver programvare på enhetene dine som gjør det mulig for deg å spore hvor den befinner seg, og fjern-slette innhold på den, skulle den bli mistet eller stjålet.
- Oppdater enhetene, applikasjonene og antivirus-programvare før du drar, slik at du kun kjører de nyeste versjonene. Mange angrep rettes mot systemer med utdatert programvare.
- Ta fullstendig sikkerhetskopi av alle enhetene dine. På denne måten har du fremdeles alle data på et sikkert sted om noe skulle skje med enhetene dine mens du reiser.

© SANS Institute 2017

Sikker mens du reiser

- Før utenlandsreiser bør du sjekke med teleoperatøren din hvordan du kan bruke mobilen i utlandet. Ofte koster det veldig mye å bruke mobildata i utlandet, du vil kanskje derfor ønske å skru mobildata fullstendig av under hele utenlandsoppholdet, eller kjøpe et forhåndsbetalt SIM-kort i landet du reiser til.

For å være sikker når du reiser, bør du sikre enhetene dine før du drar, holde dem fysisk sikre og kryptere all nettaktivitet.

Tapte/stjålne enheter

Når du begynner reisen må du sørge for at enhetene dine er fysisk sikre. For eksempel bør du ikke la enhetene ligge synlig i bilen, ettersom kriminelle enkelt kan knuse ruta og ta alt de kan se av verdi. Selv om kriminalitet definitivt er en risiko, viser en ny studie fra Verizon at det er 100 ganger mer sannsynlig at man mister en enhet enn at den blir stjålet. Derfor burde du ofte dobbeltsjekke at du har fått med deg enhetene når du reiser, for eksempel etter sikkerhetssjekken på flyplassen, når du forlater en taxi eller en restaurant, sjekker ut av et hotellrom eller går av flyet.

Trådløse nett

Å komme seg på nett mens man reiser innebærer ofte å benytte offentlige trådløse nett, som på et hotell, i en kafé, eller på en flyplass. To problemer med offentlige trådløse nett: Du kan aldri helt sikkert vite hvem som har satt dem opp, og du vet aldri hvem andre som bruker dem. Derfor burde du ikke stole på dem, det er faktisk dette som er grunnen til at du gikk gjennom alle de stegene for å sikre enhetene dine før du dro. I tillegg bruker trådløse nett radiosignaler, som vil si at alle som er fysisk i nærheten kan fange opp og overvåke den trådløse kommunikasjonen. Derfor er det viktig at du sørger for at all datatrafikken din går kryptert, dersom du er nødt til å bruke slike nettverk. For eksempel, når du skal inn på en nettside, sørg for at nettsiden er kryptert. Se etter 'HTTPS://' og/eller et hengelåsikon i adressefeltet. I tillegg har du kanskje det som kalles VPN (Virtuelt Privat Nettverk), som krypterer all datatrafikken din når du slår den på. Du kan ha fått det gjennom jobben, eller du kan kjøpe VPN for eget personlig bruk. Om det ikke finnes noen trådløse nett du vil stole på, kan du dele nett fra smarttelefonen din. Advarsel: Som nevnt tidligere kan dette være veldig dyrt når du reiser utenlands, så sjekk med teleoperatøren din først.

© SANS Institute 2017

Sikker mens du reiser

Offentlige datamaskiner

Du må ikke bruke offentlige datamaskiner, slik som de du finner i hotell-lobbyer og internettkafeer til å logge deg inn på nettsider og aksessere sensitiv informasjon. Du kan ikke vite hvem som har brukt den før deg, vedkommende kan ha infisert den med skadelig programvare enten ved et uhell eller med vilje. Om mulig, bruk kun enheter du selv kontrollerer og stoler på. Offentlige datamaskiner er kun bra for å få tak i generell, offentlig informasjon, som værmeldinger eller nyheter. Å logge inn på noen brukerkontoer, som Google-kontoen din, er som en invitasjon til hackere som kanskje følger med.

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

Passordsetninger:	https://securingthehuman.sans.org/ouch/2015#april2015
Sikkerhetskopiering:	https://securingthehuman.sans.org/ouch/2015#august2015
Skadelig programvare:	https://securingthehuman.sans.org/ouch/2016#march2016
Kryptering:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH arkivene / oversettelser:	https://securingthehuman.sans.org/ouch/archives

OUCH! utgis av SANS Securing The Human, 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 ouch@securingthehuman.org.

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS