OUCH! | Februar 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...



# Holde seg sikker under reise

## Oversikt

I dette nyhetsbrevet vil vi gå gjennom hvordan du kan sikkert koble deg til Internettet og få ting gjort mens du reiser.


## Gjesteredaktør

Steve Armstrong er teknisk ansvarlig for CyberCPR hos Logically Secure, sertifisert SANS instruktør og tidligere kursforfatter hos SANS. Han er aktiv på Twitter som **@Nebulator** og på Google plus: **+SteveArmstrongSecurity**.


## Forhåndssjekk

Nettverket ditt hjemme eller på jobb er kanskje sikkert, men når du er ute på reise kan du ikke anta at nettverket du kobler til er til å stole på. Du vet aldri hvilke andre personer som er på nettet eller hvilken trussel de utgjør. Noen enkle tiltak før du reiser kan hjelpe deg betraktelig med å beskytte dine data mens du reiser. En eller to uker før turen bør du:

- Identifiser hvilke data du ikke trenger å ha på enheten du reiser med og fjern denne dataen. Dette kan betydelig redusere konsekvensen hvis enheten blir stjålet, du mister den eller at den blir beslaglagt av tollen eller av sikkerhetsvakter. Hvis reisen er arbeidsrelatert, spør overordnet om organisasjonen tilbyr alternative enheter som er dedikert til bruk under reise.
- For internasjonale reiser, sjekk hva slags strømtilkobling det brukes i landet du skal til, du må kanskje skaffe deg en strømadapter. Du bør også sjekke med tilbyder, hva slags kostnadsplan du har. Tjenestetilbydere tar ofte ekstra betalt for bruk internasjonalt, du bør vurdere å deaktivere datatrafikk eller bytte tjenesteleverandør for internasjonal reise.
- Installer programvare på enheten så du kan fjernspore hvor enheten er og eventuelt fjernslette informasjonen, hvis det skulle være nødvendig. Mange mobile enheter har allerede denne funksjonaliteten bygd inn, i disse tilfellene må du bare aktivere funksjonen (husk at enheten trenger Internettilgang for at dette skal fungere).

En eller to dager før du reiser:

- Oppdater enhetene, applikasjonene og antivirus programvare, slik at du bruker siste versjon.
- Aktiver alle sikkerhetsinnstillingene på enheten, som brannmur.

# Holde seg sikker under reise

- Lås alle enhetene med et sterkt passord eller passkode. Dette sikrer at andre ikke kan aksessere informasjonen, selv om du mister enheten eller om den blir stjålet.
- Krypter alle enhetene slik at informasjonen ikke kan aksesseres selv om enheten blir tapt. Noen enheter, som iPhone, gjør dette automatisk hvis du setter et passord eller passkode på enheten.
- Ta en full sikkerhetskopi av alle dine enheter. Dette sikrer at du ikke mister informasjonen hvis noe skulle skje med enheten.

*Nøkkelen til å holde seg sikker mens man reiser er å sikre enhetene før man drar hjemmefra, har fysisk kontroll under reise og at man krypterer all trafikk på nettet.*

## Tapte / stjålne enheter

Etter at du har startet reisen må du sørge for at du har fysisk kontroll på enheten. For eksempel, aldri forlat enheten i bilen hvor andre enkelt kan se de, da kan kriminelle enkelt knuse vinduet på bilen og ta med seg alt de ser av verdi. En måte å fysisk sikre enhetene på er å ta med låsekabel slik at du kan låse fast enheter som en bærbare PC-en. Kriminalitet er definitivt en risiko, men det er mye mer sannsynlig at du mister enheten. Ifølge en ti-år lang studie gjort av Verizon er det 15 ganger mer sannsynlig at folk mister enheten enn at den blir stjålet. Derfor er det viktig at du sjekker to ganger at du fortsatt har enhetene dine når er kommet gjennom sikkerhetssjekken, forlater en taxi, restaurant, sjekker ut av hotellrommet, før du går på flyet etc.

## Trådløse nettverk

Internettilgang mens du reiser betyr ofte at du må bruke offentlig trådløse nettverk, som de du finner på et hotell, café, eller flyplassen. Problemet med slike nettverk er at du ikke vet hvem som satt de opp eller hvem som er koblet til nettverket. Dette er grunnen til at du ikke kan stole på disse nettverkene, dette er også en av grunnene til at du tok alle stegene med å sikre enheten før du reiste. Wi-Fi bruker radiobølger til å kommunisere fra enheten din med det trådløse aksesspunktet; dette betyr at alle som fysisk er i samme område som deg kan monitorere kommunikasjonen.

For å hindre at andre kan se datatrafikken din er det viktig at kommunikasjonen din er kryptert. For eksempel når du bruker en nettleser for å koble til et nettsted, sørg for at kommunikasjonen er kryptert (det vil stå https:// i adressefeltet med et bilde av en hengelås). Du har kanskje også en VPN-konto (Virtuelt Privat Nettverk) som vil kryptere all

## Holde seg sikker under reise

nettverkstrafikken. Dette har kanskje blitt utstedt på arbeidsplassen eller så kan du kjøpe VPN-tjenester for privat bruk. Hvis det ikke er noe trådløst nettverk du kan stole på, så kan du bruke datatrafikk på telefonen (som nevnt tidligere, kan dette være dyrt når du reiser internasjonalt, sjekk med tjenesteleverandør først).

## Offentlige datamaskiner

Ikke bruk offentlige maskiner, som datamaskiner i hotell lobbyen, bibliotek eller nettkafeer. Det er umulig for deg å vite hvem som har brukt datamaskinen før deg, de har kanskje infisert maskinen, enten bevisst eller ved et uhell. Hvis mulig, bruk kun enheter du kontrollerer og stoler på for nettaktivitet. Hvis du må bruke en offentlig datamaskin, ikke bruk noen tjenester som krever at du logger inn eller taster inn passord.

## Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos 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 www.norsis.no.

## Ressurser

| | |
|---|---|
| Passord: | http://www.securingthehuman.org/ouch/2013#may2013 |
| To-steg verifisering: | http://www.securingthehuman.org/ouch/2013#august2013 |
| Kryptering: | http://www.securingthehuman.org/ouch/2014#august2014 |
| Sikre ditt nye nettbrett: | http://www.securingthehuman.org/ouch/2013#december2013 |
| Verizon DBIR 2014: | http://www.verizonenterprise.com/DBIR/2014/ |



Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis