OUCH!

SANS SECURITY AWARENESS

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Hvordan kvitte seg med mobile enheter

Oversikt

Innovasjon og utvikling av mobile enheter som mobiler, smartklokker og nettbrett går fremover i et forrykende tempo. Som et resultat av dette bytter folk ofte mobiler, noen så ofte som hvert år. Dessverre innser folk ofte ikke hvor mye personlig informasjon som finnes på disse enhetene. Under vil vi gå gjennom hva som kan ligge lagret på en mobil enhet, og hvordan du burde gå frem for å få slettet det fullstendig før du kvitter deg med den. Dersom du fikk enheten av arbeidsgiver, eller har jobbrelatert informasjon lagret på den, må du forhøre deg med arbeidsgiver om rutiner for sikkerhetskopi og avhending først.

Informasjonen din

Mobile enheter lagrer mer sensitiv data enn mange er klar over, og ofte mye mer enn datamaskinen din.

⚠

- **Hvor du bor, jobber, og steder du besøker.**
- **Kontaktinformasjon for alle i kontaktlisten din, inkludert familie, venner og kolleger.**
- **Telefonlogg inkludert innkommende, utgående og tapte anrop, samt svarermeldinger.**
- **Tekst- og chattemeldinger fra apper for chatting, spill, og sosiale medier.**
- **Hvilke nettsider du har besøkt og hva du har søkt på, cookies og nettsider som er cachet.**
- **Personlige bilder og videoer, og eventuelt lydopptak.**
- **Lagrede passord og tilgang til brukerkontoer som sosiale medier og e-post.**
- **Helserelatert informasjon, som alder, puls, treningsvaner og blodtrykk.**

Sikker sletting

Uavhengig av hvordan du kvitter deg med mobilen, om du donerer den, bytter den med en ny modell, gir den bort til et familiemedlem, selger den, eller ganske enkelt kaster den, må du først slette all den sensitive informasjonen. Bare å slette på vanlig måte er ikke nok, istedenfor må du bruke sikker sletting for å få vekk alt. Den enkleste metoden for å gjøre dette er å tilbakestille enheten til fabrikkinnstillingene. Hvordan dette gjøres varierer fra enhet til enhet, under forklarer vi fremgangsmåten for de to vanligste enhetene. En enda sikrere løsning er å sørge for at enheten din er kryptert før du tilbakestiller den. På de fleste nye mobiler er det

nok å aktivere skjermlås (som du forhåpentligvis allerede har gjort). Til slutt vil vi anbefale på det sterkeste at du tar sikkerhetskopi før du tilbakestiller enheten.

- **Apple iOS-enheter: Innstillinger | Generelt | Tilbakestill | Slett alt innhold og innstillinger**
- **Android-enheter: Innstillinger | Avansert | Alternativer for tilbakestilling | Slett alle data (tilbakestilling til fabrikkstandard)**

SIM og eksterne lagringskort

I tillegg til selve enheten, må du også tenke over hva du skal gjøre med SIM-kortet. SIM-kortet er nødvendig for at mobilen skal kunne bruke telenettet, som ringing, SMS og mobildata. Når du tilbakestiller enheten vil SIM-kortet fremdeles ha informasjon om deg og ditt abonnement. Det enkleste er å bare ta med SIM-kortet og gjenbruke det i den nye telefonen. Men om det ikke er mulig, snakk med teleoperatøren din om nytt SIM-kort, og fysisk ødelegg det gamle, slik at det ikke kan misbrukes. Noen mobile enheter har også et SD-kort for ekstra lagring som kan tas ut. Sørg for å fjerne slike før du kvitter deg med enheten, de kan ofte gjenbrukes med den nye enheten, eller de kan brukes for generell lagring med en datamaskin, ved hjelp av en USB-adapter. Dersom det ikke er aktuelt å gjenbruke SD-kortet anbefaler vi at du fysisk ødelegger det, akkurat som med SIM-kortet.

Dersom du er usikker på noe av det vi har gått gjennom, eller dersom innstillingene på din mobile enhet er annerledes, ta den med til butikken du kjøpte den i og få hjelp der. Og til slutt, dersom du planlegger å kaste enheten, vurder å donere den istedenfor. Mange veldedige organisasjoner tar imot brukte mobiler.

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.

Gjesteredaktør

Christopher Crowley *(@CCrowMontance) er en uavhengig konsulent i området ved Washington DC, og fokuserer på sikkerhetsoperasjoner. Han tweeter og blogger av og til. Vær på utkikk etter den kommende boka hans om sikkerhets-operasjonssentre. Han er en av SANS instituttets seniorinstruktører.*

Ressurser

SANS-kurs: Pen Testing Mobile Devices:	https://sans.org/sec575
SANS-kurs: Advanced Smartphone Forensics Course:	https://sans.org/for585
Nettvett.no: Sikker sletting:	https://nettvett.no/sikker-sletting/