SANS SECURITY AWARENESS

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Avyttring av Mobila Enheter

Inledning

Mobila enheter, så som telefoner, smarta klockor och surfplattor fortsätter att utvecklas och förnyas i rasande takt. Som ett resultat av detta ersätter en del personer sina mobila enheter så ofta som varje år. Olyckligtvis inser dom inte hur mycket personuppgifter som kan finnas sparade på dessa enheter. Nedan går vi igenom vad som kan finnas lagrat i din mobila enhet och hur du säkert rensar den innan avyttring. Om din mobila enhet tillhör din arbetsgivare eller innehåller arbetsrelaterad information, var noga med att kontrollera vilka procedurer som gäller innan du gör dig av med enheten.

Din information

Mobila enheter lagrar mer känslig data än vad många inser, ofta betydligt mer än på din dator.

⚠

- **Var du bor, arbetar och platser du besöker**
- **Kontaktuppgifter till alla i din adressbok, inklusive familj, vänner och medarbetare**
- **Samtalshistorik över inkommande, utgående och missade samtal samt din röstbrevlåda**
- **SMS eller chatsessioner från applikationer som secure chat, spel och sociala media**
- **Webbläsarhistorik, webbsökningar, cookies och cachade sidor**
- **Personliga fotografier, videor och ljudinspelningar**
- **Sparade lösenord och åtkomst till dina konton. T.ex. din bank, sociala media eller e-post**
- **Hälsorelaterad information som din ålder, puls, träningshistorik eller blodtryck**

Återställ din enhet

Oavsett hur du väljer att avyttra din mobila enhet, som att donera den, byta in den mot en ny, ge den till en familjemedlem, sälja eller slänga den behöver du säkerställa att all känslig information är raderad. Att endast radera data är inte tillräckligt, istället bör du radera all data på din enhet på ett säkert sätt. Det enklaste sättet att göra det är att återställa din enhet till fabriksinställningar. Hur man återställer en enhet varierar beroende på tillverkare och modell men nedan finns stegen för de två vanligaste enheterna Apple iOS och Android. För att öka säkerheten ytterligare, se till att din enhet har kryptering påslagen innan du återställer den. På de flesta moderna enheterna görs det enklast genom att aktivera skärmlåset (vilket du förhoppningsvis redan har aktiverat). Slutligen rekommenderar vi att du gör en backup av din enhet innan du återställer den.

- Apple iOS Devices: Settings | General | Reset | Erase All Content and Settings
- Android Devices: Settings | Privacy | Factory Data Reset

SIM & Externa kort

I tillägg till din enhet behöver du också överväga vad du ska göra med ditt SIM-kort (Subscriber Identity Module). Ett SIM-kort är vad mobila enheter använder för att ringa ett samtal eller skapa en dataanslutning. När du har återställt din enhet innehåller SIM-kortet fortfarande information om ditt konto hos teleoperatören och är kopplad till dig. Om du behåller ditt telefonnummer och flyttar till en ny enhet kan du prata med din operatör om flytt av ditt SIM-kort. Du kan också fysiskt förstöra SIM-kortet för att hindra att någon får åtkomst till din information, kontouppgifter eller återanvänder kortet och utger sig för att vara du. Slutligen vill vi informera att vissa Android-enheter använder SD-kort (Secure Digital) för utökad lagring. Ta bort dessa externa lagringskort från din mobila enhet innan du avyttrar den. Dessa kort kan ofta återanvändas i nya mobila enheter, eller användas som lagring på din dator. Om återanvändning inte är möjligt rekommenderar vi att du precis som med SIM-kortet, fysiskt förstör det.

Om du är osäker över något av ovanstående steg eller om din mobila enhet återställs på annat sätt kan du gå till butiken där du köpte den och få hjälp av en utbildad tekniker. Om du överväger att slänga din enhet, fundera på att donera den istället. Det finns många utmärkta välgörenhetsorganisationer som tar emot begagnade enheter och många butiker har kärl för återvinning av mobila enheter.

Gästskribent

Christopher Crowley *(@CCrowMontance) är en oberoende konsult som verkar i Washington DC med fokus på security operations. Han twittrar och bloggar dessutom då och då. Håll utkik efter hans kommande bok om Security Operation Centers (SOCar). Han är också senior instruktör vid SANS Institute.*

Källor

SANS Course: Pen Testing Mobile Devices:	https://sans.org/sec575
SANS Course: Advanced Smartphone Forensics Course:	https://sans.org/for585
FTC Advice on Disposing Your Mobile Device:	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device

OUCH! Publiceras av SANS Security Awareness och distribueras under Creative Commons BY-NC-ND 4.0-licens. Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Erik Täfvander & Johan Ahlberg

Visolit