Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

Kassera din Mobila Enhet

Översikt

Mobila enheter, såsom smartphones och tabletter, fortsätter att avancera och förnya sig med en förvånande hastighet. Som ett resultat av detta byter många av oss våra mobila enheter så ofta som var 18 månad. Tyvärr gör alltför många människor helt enkelt av sig med sina äldre mobila enheter med liten tanke på hur mycket personuppgifter deras enheter har samlat. I detta nyhetsbrev kommer vi att täcka vilka typer av personlig information kan finnas på din mobila enhet och hur du kan säkert radera den innan du kasserar eller returnerar din smartphone. Om din arbetsgivare gav dig din mobila enhet, eller om den har organisatorisk data lagrad, se till att kolla med din chef om ordentlig säkerhetskopiering och hanteringsrutiner innan att följer stegen nedan.

Gästredaktör

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) är en konsult baserad i Washington, DC området. Han är huvudinstruktör för SANS Institutets kurs Mobile Device Security and Ethical Hacking (SEC575) och författare av Incident Response Team Management (MGT535).

Din Personliga Information

Mobila enheter lagrar betydligt mer känslig information än du kanske tror, troligen ännu mer än din dator. Typisk information som lagras av en mobil enhet kan innehålla:

- Var du bor, arbetar och platser du besöker ofta
- Kontaktuppgifter till alla i din adressbok, inklusive familj, vänner och arbetskamrater.
- Samtalshistorik inklusive inkommande, utgående och missade samtal
- Text-och röstmeddelanden
- Chattsessioner inom applikationer som spel och sociala medier
- Plats historia baserad på GPS-koordinater eller mobilmast historia
- Surfnings historia, cookies och cachade sidor
- Personliga foton, videor, ljudinspelningar och e-post
- Lagrade lösenord och tillgång till personliga konton, till exempel din internetbank eller e-post
- Tillgång till foton, filer eller information som lagras i molnet
- Hälsorelaterad information, inklusive din puls, blodtryck eller diet

Kassera din Mobila Enhet

Radera Enheten

Som ni kan se , kan det finnas en enorm mängd känslig information på din mobila enhet . Oavsett hur du gör med din mobila enhet, till exempel donerar den, ger den till en annan familjemedlem, säljer den eller till och med kastar ut den, måste du vara säker på att du först raderar all känslig information. Dessutom måste du radera din information om du returnerar din mobiltelefon eller byta den mot en ny. Om du inte gör det, kan den som får din mobila enhet näst ha möjlighet att enkelt komma åt den. Men innan du börjar radera dina data, behöver du troligtvis säkerhetskopiera all data, inklusive bilder, videor och annan information. När du raderar enheten kommer du inte att kunna återställa data som lagras på den.

När du slänger din mobila enhet, se till att göra en fabriksåterställning och ta ut SIM och SD-korten om enheten har dem.

När du har säkerhetskopierat datan måste du radera det på ett säkert sätt. Att bara ta bort filer, bilder, eller data är inte tillräckligt. Data som har raderats kan enkelt återvinnas med hjälp av gratis verktyg som finns på Internet. Istället vill du radera all data på enheten på ett säkert sätt, detta kallas “wiping” på Engelska. Denna procedur skriver faktiskt över din gamla information så att den inte kan återvinnas . Det enklaste sättet att göra detta är att använda enhetens “fabriksåterställnings” funktion. Detta kommer att återställa den till det skick den var i när du köpte den. Vi har funnit att fabriksåterställning är den säkraste och enklaste metoden för att radera data från din mobila enhet. Fabriksåterställning funktionen varierar mellan olika enheter; nedan är stegen för de tre mest populära enheterna.

- Apple iOS-enheter: Inställningar | Allmänt | Nollställ | Radera allt innehåll och inställningar
- Android-enheter: Inställningar | Privacy | Återställ till fabriksinställningarna
- Windows-telefoner: Inställningar | Om | Återställ telefonen

Om du fortfarande har frågor om hur man gör en fabriksåterställning, kolla din instruktionsbok eller tillverkarens webbplats. Kom ihåg att bara ta bort dina personuppgifter är inte tillräckligt eftersom det lätt kan återvinnas.

SIM- & Extärna Lagringskort

Utöver data som lagras på enheten, måste du också tänka på vad du ska göra med ditt SIM (Subscriber Identity Module) kort. Ett SIM-kort är det en mobil enhet använder för att göra en mobiltelefon eller dataanslutning . När du gör en fabriksåterställning på enheten behåller SIM-kort information om ditt konto. Om du behåller ditt telefonnummer och

Kassera din Mobila Enhet

flyttar till en ny enhet, prata med telefonförsäljaren om att överföra ditt SIM-kort. Om detta inte är möjligt, till exempel om den nya telefonen använder en annan storlek SIM-kort, behåll ditt gamla SIM-kort och strimla eller förstör det för att förhindra att någon annan återanvänder det.

Slutligen, några mobila enheter använder en separat SD (Secure Digital) kort för ytterligare lagring av data. Dessa minneskort innehåller ofta bilder, smartphone program och annan känslig information. Kom ihåg att ta bort alla externa lagringskort från din mobila enhet innan kassering (för vissa enheter kan ditt SD-kort gömmas i batterifacket, möjligen under batteriet). Dessa kort kan ofta återanvändas i nya mobila enheter eller kan användas som allmän lagring på din dator med en USB-adapter. Om återanvändning av ditt SD-kort är inte möjligt, precis som med ditt gamla SIM-kort , rekommenderar vi att du fysiskt förstör det.

Om du är osäker på någon av de åtgärder som omfattas av detta nyhetsbrev, ta din mobiltelefon till butiken du köpte den och få hjälp av en utbildad tekniker. Slutligen, om du kastar bort din mobila enhet ber vi dig att överväga att donera den istället. Det finns många utmärkta välgörenhetsorganisationer som accepterar använda mobila enheter.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhets-branchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

NIST SP800-88 Rev. 1: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OUCH! Backups: http://www.securingthehuman.org/ouch/2013#september2013

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson