SANS SECURITY AWARENESS

OUCH!

De maandelijkse Security Awareness nieuwsbrief voor jou!

Het afvoeren van mobiele apparaten

Overzicht

Mobiele apparaten, zoals smartphones, smart horloges en tablets, blijven in een verbluffend tempo vooruitgaan en innoveren. Als gevolg daarvan vervangen sommige mensen hun mobiele apparaten minstens elk jaar. Helaas realiseren mensen zich vaak niet hoeveel persoonlijke gegevens op deze apparaten staan. Hieronder bespreken we wat er op jouw mobiele apparaat staat en hoe je dit veilig moet wissen voordat je het weggooit. Als jouw mobiele apparaat door je werkgever is verstrekt, of als er werkgegevens op zijn opgeslagen, moet je eerst met jouw supervisor overleggen over de juiste back-up- en verwijderingsprocedures.

Jouw gegevens

Mobiele apparaten slaan meer gevoelige gegevens op dan veel mensen zich realiseren, vaak veel meer dan op de computer.

⚠

- **Waar je woont, werkt en waar je naartoe gaat**
- **De contactgegevens van iedereen in jouw adresboek, inclusief familie, vrienden en collega's**
- **Telefoongesprekshistorie inclusief inkomende, uitgaande, voicemail en gemiste oproepen**
- **Sms'en of chatsessies binnen applicaties zoals beveiligde chat, games en sociale media**
- **Webbrowsgeschiedenis, zoekgeschiedenis, zoekgeschiedenis, cookies en cache-pagina's**
- **Persoonlijke foto's, video's en audio-opnames**
- **Opgeslagen wachtwoorden en toegang tot jouw rekeningen, zoals je bank, sociale media of e-mail**
- **Gezondheidsgerelateerde informatie, waaronder leeftijd, hartslag, bewegingsgeschiedenis of bloeddruk**

Je apparaat wissen

Ongeacht hoe je je mobiele apparaat weggooit, denk aan doneren, ruilen voor een nieuw apparaat, het aan een ander familielid geven, het doorverkopen of zelfs weggooien, je moet er zeker van zijn dat je eerst al die gevoelige informatie wist. Het eenvoudigweg verwijderen van gegevens is niet genoeg, in plaats daarvan moet je alle gegevens op het apparaat veilig wissen. De eenvoudigste manier om dit te doen is om je apparaat te resetten. De resetfunctie verschilt per apparaat; hieronder staan de stappen voor de twee meest gebruikte apparaten. Een nog veiligere stap is om er zeker van te zijn dat je versleuteling op het apparaat hebt ingeschakeld voordat je het reset. Op de meeste recente mobiele apparaten is de eenvoudigste manier om dit te doen gewoon een screenlock inschakelen (die je hopelijk al hebt ingeschakeld). Tot slot raden wij ten zeerste aan om een back-up te maken van het apparaat voordat je het opnieuw installeert.

- Apple iOS-apparaten: Instellingen | Algemeen | Reset | Alle inhoud en instellingen wissen
- Android-apparaten: Instellingen | Privacy | Fabrieksgegevens resetten

SIM & externe kaarten

Naast het toestel moet je ook nadenken over wat je met je SIM-kaart (Subscriber Identity Module) moet doen. Een SIM-kaart is wat een mobiel apparaat gebruikt om een mobiele of dataverbinding te maken. Wanneer je je apparaat wist, bewaart de SIM-kaart informatie over je account en is aan je gekoppeld. Als je je telefoonnummer bijhoudt en naar een nieuw apparaat verhuist, contacteer dan je telefoonprovider over het overzetten van je SIM-kaart. Als dit niet mogelijk is, bewaar dan de oude SIM-kaart en vernietig deze fysiek om te voorkomen dat iemand anders deze opnieuw gebruikt om zich voor jouw uit te geven. Tot slot maken sommige mobiele Android-apparaten gebruik van een verwijderbare SD-kaart (Secure Digital) voor extra opslagruimte. Verwijder deze externe opslagkaarten van het mobiele apparaat voordat je ze weggooit. Deze kaarten kunnen vaak worden hergebruikt in nieuwe mobiele apparaten, of kunnen worden gebruikt als algemene opslag op een computer met een USB-adapter. Als hergebruik van de SD-kaart niet mogelijk is, dan raden wij aan om deze net als de oude SIM-kaart fysiek te vernietigen.

Als je niet zeker bent over een van de bovenstaande stappen, of als je een ander apparaat resetopties hebt, neem dan je mobiele apparaat mee naar de winkel waar je het gekocht hebt en vraag hulp van een getrainde technicus. Tot slot, als je een apparaat weggooit, overweeg dan om het in plaats daarvan te doneren. Er zijn veel goede doelen organisaties die gebruikte mobiele apparaten accepteren en veel mobiele providers hebben drop-off bakken in hun winkels.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Christopher Crowley *(@CCrowMontance) is een onafhankelijke consultant werkzaam in de regio Washington DC, met de focus op beveiligingsmaatregelen. Hij tweet en blogt af en toe. Kijk uit naar zijn aanstaande boek over Security Operations Centra. Hij is een Senior Instructeur bij het SANS Instituut.*

Bronnen

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