OUCH!

SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed

Sådan sikrer du dine mobile enheder

Overblik

Dine mobile enheder er en fantastisk og nem måde at kommunikere med venner, shoppe eller benytte dig af din netbank, se film, spille spil og udføre et utal af andre aktiviteter. Da dine enheder er en så vigtig del af dit liv, er der nogle enkle ting du kan gøre for at holde dig og dine enheder sikre.

Sikring af dine enheder

Det kan komme som en overraskelse at den største sikkerhedsrisiko for din mobile enhed ikke er hackere, men højst sandsynligt er dig selv. Risikoen for at du taber eller glemmer en mobil enhed er større end for at der er nogen der hacker den. Den første ting du skal gøre for at beskytte dine enheder, er at aktivere automatisk låsning af skærmen, ofte kaldet et screenlock. Dette betyder, hver gang du vil bruge din enhed, skal du først låse op for skærmen, f.eks. med en stærk adgangskode eller dit fingeraftryk. Dette hjælper med at sikre, at hvis din enhed går tabt eller bliver stjålet, kan ingen få adgang til den. Herudover er der flere tips til beskyttelse af dine enheder:

Opdatering

Aktivér automatisk opdatering på dine enheder, så de altid benytter den nyeste version af operativsystemet og apps. IT-kriminelle søger altid nye svagheder i software, og leverandører udgiver konstant nye opdateringer og patches for at rette dem. Ved altid at benytte det nyeste operativsystem og apps gør du det meget sværere for alle at hacke dine enheder.

Fjernstyring

Installer eller aktiver software til fjernstyring af din mobilenhed via internettet. På denne måde kan du oprette forbindelse til din enhed hvis du taber den, glemmer den eller får den stjålet. Du kan finde dens placering, eller i værste fald fjerne alle dine oplysninger på den.

Tillidsværdige apps

Download kun de apps, du har brug for, og fra betroede kilder. For iPads eller iPhones betyder det at du skal downloade apps fra Apple App Store. For Android download apps fra Google Play og Amazon-tablets med Amazon App Store. Du kan muligvis downloade apps fra andre steder, men disse er ikke kontrolleret og er langt mere

tilbøjelige til at blive inficeret. Før du downloader en app bør du tjekke at den har mange positive anmeldelser og opdateres aktivt af sælgeren. Hold dig væk fra helt nye apps, apps med få anmeldelser eller apps der opdateres sjældent. Endelig, uanset hvor du fik din app fra, når du ikke længere har brug for eller aktivt bruger appen, anbefaler vi, at du sletter den fra din enhed.

Beskyttelse af personlige oplysninger

Når du installerer en ny app, skal du sørge for at gennemgå mulighederne for privatindstillinger. F.eks. skal den app, du lige har hentet, virkelig have adgang til alle dine venner og deres kontaktoplysninger? Vi anbefaler også, at du deaktiverer positionssporing for alt, og derefter kun aktiver for de apps, du føler, har brug for det. Hvis du er utryg med en apps krav, skal du finde en anden, der opfylder dine behov. Derudover skal du regelmæssigt kontrollere tilladelserne for at sikre, at de ikke er ændret.

Sikkerhedskopiering

Sikkerhedskopier altid dine data. For mobile enheder sikkerhedskopieres mange af dine oplysninger ofte automatisk, f.eks. dine fotos eller meddelelser. Sikkerhedskopieringer gemmer også din konfiguration, apps og andre enhedsoplysninger, hvilket gør det meget nemmere at gendanne hvis du har mistet en enhed eller ved overgang til en ny enhed.

Arbejde

Når du er på arbejde, skal du være ekstra forsigtig. Tag aldrig billeder eller video, der ved et uheld kan indeholde følsomme oplysninger, som f.eks. billeder af whiteboards eller computerskærme.

Dine mobile enheder er et kraftfuldt værktøj, som vi vil have dig til at nyde og bruge. Bare ved at følge disse få enkle råd når du langt med at holde dig og dine enheder sikre.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Ressourcer

Passphrases:	https://www.sans.org/u/A3E
Backup/Recovery:	https://www.sans.org/u/A3z
Sikker bortskaffelse af mobile enheder:	https://www.sans.org/u/A3u
Sikker brug af mobile apps:	https://www.sans.org/u/A3p
SANS Tip om dagen:	https://www.sans.org/tip_of_the_day.php

Licensinformation