

OUCH!

Det månedlige nyhedsbrev om IT-sikkerhed til dig

# Sådan kommer du sikkert af med dine mobile enheder

## Oversigt

Mobile enheder, såsom smartphones, smarte ure og tabletter, fortsætter med at forny sig med en forbløffende hastighed. Som følge heraf erstatter nogle mennesker deres mobile enheder årligt. Desværre ved folk ofte ikke, hvor mange personlige data der findes på disse enheder. Vi vil gerne hjælpe dig med at forstå, hvad der kan være på din mobilenhed, og hvordan du sletter det sikkert, før du kasserer enheden.

## Dine informationer

Mobile enheder gemmer mere data, end du tror og langt mere end din computer.



- Hvor bor du, arbejder og steder du besøger
- Kontaktoplysningerne på alle i din adressebog, herunder familie, venner og kolleger
- Telefonopkaldshistorik, herunder indgående, udgående, telefonsvarbeskeder og ubesvarede opkald
- Tekst- eller chat-sessioner inden ind applikationer som sikker chat, spil og sociale medier
- Web browsing historik, søgehistorik, cookies og cachelagrede sider
- Personlige fotos, videoer og lydoptagelser
- Gemte adgangskoder og adgang til dine konti, f.eks. din bank, sociale medier eller e-mail
- Sundhedsrelateret information, herunder din alder, puls, træningshistorie eller blodtryk

## Slette alt på din enhed

Uanset hvordan du bortskaffer din mobilenhed, såsom at donere den, bytte den til en ny, give den til et andet familiemedlem, videresælge det eller endda smide det ud, skal du være sikker på at du først sletter alle de dine oplysninger. Det er ikke nok bare at slette dataen, i stedet skal du slette alle dataene på din enhed på en sikker måde. Den nemmeste måde at gøre dette på er at nulstille din enhed. Nulstilfunktionen varierer mellem enheder; nedenstående er trinene for de to mest almindelige enheder. Et endnu sikrere trin er at sikre, at du har enhedskryptering aktiveret på din enhed, før du nulstiller den. På de nyeste mobilenheder er den nemmeste måde at gøre dette på, blot at aktivere et skærmlås (hvilket forhåbentlig du allerede har aktiveret). Endelig anbefaler vi på det kraftigste, at du sikkerhedskopierer din enhed, før du nulstiller den.



- Apple iOS-enheder: Indstillinger | Generelt | Nulstil | Slet alt indhold og indstillinger
- Android-enheder: Indstillinger | System | Nulstilling

## SIM og eksterne hukommelseskort

Ud over din enhed skal du også overveje, hvad du skal gøre med dit SIM-kort. Et SIM-kort er, det en mobil enhed bruger til at foretage en mobil- eller dataforbindelse. Når du sletter alt på din enhed, beholder SIM-kortet oplysninger om din konto og er bundet til dig. Hvis du beholder dit telefonnummer og blot skifter enhed, skal du kontakte din telefonudbyder og bede dem om at overføre dit SIM-kort. Hvis dette ikke er muligt, skal du beholde dit gamle SIM-kort og ødelægge det fysisk for at forhindre en anden i udgive sig for at være dig og få adgang til dine oplysninger eller konti. Endelig bruger nogle Android-mobilenheder et SD-kort som ekstra lagerplads. Fjern disse eksterne hukommelseskort fra din mobilenhed før bortskaffelse. Disse kort kan ofte genbruges i nye mobilenheder eller kan bruges som hukommelseskort til din computer med en USB-adapter. Hvis genbrug af dit SD-kort ikke er muligt, så anbefaler vi dig, som med det gamle SIM-kort, at du ødelægger det fysisk.

Hvis du ikke er sikker på hvordan du udfører nogen af ovenstående trin, eller hvis du har en anden indstillinger på enheden, skal du tage din mobile enhed til den butik, du har købt den, og få hjælp fra en uddannet tekniker. Endelig, før du smider en enhed væk, så overvej at donere den i stedet. Der er mange gode velgørende organisationer, der accepterer brugte mobilenheder, og mange mobile udbydere har drop-off-bakker i deres butikker.

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>.

## Gæsteredaktør

**Christopher Crowley** ([@CCrowMontance](#)) er en uafhængig konsulent i Washington DC-området med fokus på sikkerhed i driften. Han tweeter og blogger lejlighedsvis. Hold øje med hans kommende bog om SOC ("Security Operations Center"). Han er en senior instruktør på SANS Institute.



## Hvis du vil vide mere

FTC Råd omkring bortskaffelse af mobile enheder:

<https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>

*OUCH! er udgivet af SANS Security Awareness og distribueres under [Creative Commons BY-NC-ND 4.0 license](#). Du er velkommen til at videregive dette nyhedsbrev eller bruge det i dit eget arbejde med IT-sikkerhed så længe du ikke ændrer i nyhedsbrevet. Hvis du har spørgsmål til oversættelsen eller andet er du velkommen til at kontakte [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity*