Sådan sikrer du din smartphone

https://www.telmore.dk/shop/smartphoneunivers/smartphone-sikkerhed

Har du en smartphone og vil du gerne passe godt på den? Læs her, hvordan du tager kampen op mod ondsindende vira og hackere med ufine hensigter. Lær, hvordan du beskytter din smartphone bedst muligt. Vi linker til en række artikler, der forklarer om sikkerhed og foreslår nyttige apps, der hjælper dig, hvis uheldet er ude.

9 tips til at sikre din smartphone
Læs 9 tips til at sikre din smartphone. IT- og Telestyrelsen giver gode råd om passwordbeskyttelse, apps, opdateringer og muligheden for at fjernstyre din mobil, hvis den skulle blive stjålet.
Læs 9 tips til beskyttelse af din smartphone **Se side 2**

Hvad er mobilvirus og hvordan undgår du det
Læs om, hvordan du kan få virus på din mobil og ikke mindst, hvordan du undgår det. Læs også, hvad du skal gøre, hvis du er så uheldig, at få virus ombord på din mobil. De gode råd kommer fra IT- og Telestyrelsen.
Læs mere om mobilvirus

Specielt til dig med Android
Har du en mobiltelefon, der kører på Android, så har Computerworld bragt en artikel, der har en række gode råd - specielt til dig med Android. Få detaljeret vejledning til optimal beskyttelse af din mobil.
Se desuden Nortons liste over farlige trusler til Android
Læs artiklen Sådan sikrer du data på din Android-telefon **Side 3-6 (6 råd)**

Specielt til dig med iPhone
Har du en iPhone, kan du læse mere om, hvordan du sikrer den. I Computerworlds artikel får du deltaljeret vejledning til at beskytte din mobil.
Læs artiklen Sådan sikrer du din iPhone

Mobilbank
Mange banker tilbyder nu, at du kan bruge mobilen som "netbank". Du skal blot hente en mobilbank-app hos fx App Store eller Android Market. Læs mere om sikkerheden hos din egen bank og husk desuden: 1) Vis aldrig din mobilbank-kode til andre. 2) Hvis du bruger nøglekort, så sørg for, at ingen har adgang til det. 3) Efterlad ikke din mobil på bordet, hvis den er logget på mobilbank. 4) Kontakt omgående din bank, hvis du har mistanke om misbrug.

Fugt dræber din smartphone
Den største risiko for din smartphone er faktisk hverken virus eller hackere. Fugtskader er en af de hyppigste årsager til, at en smartphone bukker under. Læs, hvordan du undgår fysiske skader på din smartphone.
Sådan passer du på din smartphone

Sikkerhed på smartphones

I takt med at smartphones har fået flere funktioner, og på nogle områder kan det samme som en bærbar pc, bør såvel almindelige brugere som virksomheder være meget opmærksomme på de udfordringer, der hører med til at benytte smartphones

Når man som bruger og virksomhed vælger smartphones, er der visse sikkerhedsfunktioner, man bør overveje at aktivere, hvis smartphonen anvendes til at tilgå vigtige data.
Hvordan kan jeg som bruger sikre min smartphone?

1. **Anvend adgangskoder**
   Aktiver brug af en adgangskode, som skal indtastes, hver gang smartphonen benyttes. Sørg for at ændre de fabriksindstillede standard adgangskoder. Herved reduceres risikoen for, at telefonen umiddelbart kan misbru-ges ved tab.

2. **Aktiver kryptering**
   De fleste smartphones kan kryptere såvel telefonens hukommelse og ekstra datamedier (f.eks. SD kort). Hermed sikres, at adgangskodesikring ikke umiddelbart kan omgås.

3. **Hold styresystemet på din smartphone opdateret**
   En smartphone bør holdes opdateret, så sikkerhedshuller løbende lappes. Flere smartphones tilbyder periodisk brugeren en opdatering, som man bør acceptere.

4. **Installer kun applikationer du har tillid til**
   Vær kritisk over for de applikationer du ønsker at installere. Installer kun applikationer du har tillid til. Brug en søgemaskine til at finde information om applikationerne først, og læs hvad andre brugere har oplevet med applikationen.

5. **Aktiver mulighed for at fjernslette alt indhold**
   Mange smartphones tilbyder en mulighed for at slette alt indhold og endda låse telefonen, via en hjemmeside. På denne måde kan du slette data på den telefon, hvis den bliver stjålet eller du taber den.

6. **Lås SIM-kortet til telefonen**
   På nogle smartphones er der mulighed for at låse SIM-kortet til telefonen. Denne funktion findes kun på visse modeller, men sikrer, at andre ikke kan tilgå data på din telefon blot ved at sætte nyt SIM-kort i.

7. **Sluk for Bluetooth, når det ikke benyttes**
   Med Bluetooth tændt er man udsat for, at brugere i nærheden potentielt kan tilgå data på telefonen. Ved at slukke for Bluetooth, når man ikke bruger det, forhindrer man, at man udsættes for angreb via Bluetooth.

8. **Når din smartphone anvender Wi-Fi, vær sikker på, at det trådløse net er krypteret**
   De fleste smartphones kan tilsluttes lokale trådløse net (Wi-Fi). Hvis det-te net ikke er krypteret, kan dine passwords til hjemmesider og e-mail aflyttes. Er du i tvivl, så undlad at benytte Wi-Fi fra din smartphone.

9. **Brug antivirus**
   Der optræder i dag flere former for virus, som angriber smartphones. Undersøg muligheden for at installere og anvende et antivirusprogram. Disse programmer findes typisk på den ”markedsplads”, hvor du køber eller installerer dine programmer fra.

Sådan sikrer du data på din Android-telefon

Har du købt en Android-mobil, er du ikke alene - Googles Android-platform er populær som aldrig før. Men hvordan sikrer du dine data, hvis du skulle miste din dyrebare telefon? Få **6 gode råd** her.

Computerworld News Service: Googles software-butik, Android Market, har for første gang været ramt at et større malware-angreb.

Den populære applikation "DroidDream" viste sig at være inficeret med ondsindet kode designet til at stjæle brugernes personlige informationer, og Google blev tvunget til at anvende den indbyggede "kill-switch" for at slippe af med den problematiske applikation.

Men på det tidspunkt havde den allerede inficeret i tusindvis af Android-smartphones.

Googles Android-platform har aldrig været mere populær. Faktisk sidder Android i dag på 31 procent af det amerikanske smartphone-marked, hvilket gør styresystemet til det mest populære i landet, fortæller ComScore.

Android har aldrig tidligere udgjort så markant et mål for hackere og andre lyssky typer, der vil profitere på platformens popularitet. Det er med andre ord på høje tid at forholde sig til sikkerhed på Android på en smart måde.

De følgende seks tips og tricks hjælper dig med netop det.

1. Beskyt din Android med et password - Nu!
Hvis man kun skulle gøre én ting for sikkerheden på sin Android-mobil, så skulle det absolut være at beskytte den med et password. Det lyder enkelt, men et stærkt password - eller selv et simpelt password - kan beskytte dig og din smartphone fra langt de fleste trusler.

Hvis en person med ondt i sinde ikke kan komme forbi din password-skærm, så er både data og alt andet på enheden som hovedregel sikret.

Afhængigt af din Android-model vil du have en række forskellige password-muligheder, som alle bliver tilgået på samme måde.

Gå ind i menuen Indstillinger og scroll ned til det afsnit, der hedder Sikkerhed eller lignende. Klik herefter på *Indstil skærmlås,* og du vil blive præsenteret for en stribe forskellige password-muligheder, afhængigt af modellen.

En Motorola Atrix 4G og HTC Desire HD tilbyder for eksempel password-muligheder med Pattern Lock (Mønster på f.eks. Sony Ericsson), hvor du kan opsætte et særligt mønster til at låse telefonen op med; en PIN-kode-lås, der bruger tal til at sikre dit håndsæt samt en password-lås, hvormed man kan anvende både tal og bogstaver. Motorola Atrix 4G har desuden en biometrisk baseret Fingerprint Lock, der bruger Atrix's fingeraftrykslæser til autentificering.

Selv om fingeraftryks-muligheden er den mest sikre ... så er jeg ikke helt tryg ved at aflevere mine biometriske informationer til Googles servere, så jeg vælger i stedet password-lås. I forhold til sikkerheden er Fingerprint Lock

mest sikker, efterfulgt af password-lås, PIN-kode-lås og endelig Mønster-lås. Men alle de forskellige låsemuligheder giver bedre sikkerhed, end hvis man ikke har et password overhovedet.

(Bemærk: Hvis du vælger mønster-muligheden, så er det en god idé med jævne mellemrum at polere sin touchscreen, eftersom mønstret ved gentagelse kan efterlade spor på skærmen, som hackere kan se og bruge til at komme ind på enheden med.)

Når du har valgt dit Android-password, bør du sætte din timeout for skærmen til et relativt lavt niveau, så din enhed af sig selv lukker ned og låser, kort tid efter du har forladt den.

For at gøre det åbner man Indstillinger, scroller ned og vælger Visning. På den følgende skærm finder man punktet *timeout for skærmen* og vælger en værdi - jeg vil foreslå et minut eller mindre for maksimal sikkerhed.

2. Skræddersyet Locked Home Screen med ejer-information
Forestil dig, at du glemmer din smartphone på et værtshus. En god samaritaner finder enheden og vil gerne levere den tilbage til ejermanden ... men telefonen er låst, og skærmen viser ikke andet end en smuk, men ubrugelig, havudsigt.

Det scenarium forekommer hele tiden, og hvis flere smartphone-ejere skrev deres informationer på skærmen, så ville langt flere tabte enheder formentligt blive returneret til den rigtige ejer.

Desværre indeholder Android ikke nogen indbygget mulighed for at skrive ejer-informationer på den låste skærm, ligesom andre mobile platforme, som for eksempel Research In Motions (RIM) BlackBerry OS. Men der findes flere tredjeparts-applikationer, der kan gøre det for dig.

Min foretrukne metode til at tilføje ejer-informationer til Androids låste skærm: Applikationen Phone Found - Owner Info, som kan findes gratis på Android Market. For at bruge den åbner man bare softwaren, finder Edit-knappen og tilføjer sine kontaktinformationer.

Derefter kan man åbne applikationens indstillinger og vælge hvilke informationer, man gerne vil have fremvist på enhedens låste skærm.

3. Lad være med at roote din Android-enhed
At 'roote' sin Google Android-enhed betyder, at man fjerner en del af de restriktioner, som producenten og udbyderen har lagt hen over telefonen for at gøre det nemmere for dem blandt andet at installere og levere de applikationer og tjenester, som de gerne vil have dig til at anvende.

Rooting åbner desuden for system-level adgang til telefonens kerne-ressourcer, og det er ikke en god ting, set fra et sikkerhedsperspektiv, eftersom det samtidig fjerner en række sikkerhedselementer, der er blevet installeret for at beskytte telefonen fra malware og andet potentielt farligt kode.

Med mindre du er udvikler eller har et usædvanligt godt kendskab til Android og en vis risikovillighed, så bør du IKKE roote din Android-enhed. Aldrig nogensinde!

Det kan godt være, at det betyder begrænset adgang til visse seje, skræddersyede applikationer og tjenester, og at det forhindrer dig i at benytte uofficielle tredjeparts-applikationsforretninger. Men til gengæld betyder det også væsentlig højere sikkerhed, eftersom applikationer som hovedregel ikke kan opnå system-level adgang uden en root.

Konklusionen er: Lad være med at roote din Android-enhed. Hvis du ikke kan lade være, skal du vide, at det samtidig betydeligt reducerer telefonens eksisterende sikkerhedsmuligheder.

4. Hold dig til det officielle Android Market
Det er en god ide at være yderst selektiv i forhold til de steder, hvor man kan downloade applikationer til Android. Computerworld har blandt andet givet et bud de bedste gratis apps.

Jeg vil anbefale, at man holder sig til udelukkende at downloade fra Googles Android Market, trods det at hele DroidDream-situationen beviser, at heller ikke Android Market er 100 procent fri af malware og ondsindede applikationer.

(Efter episoden med DreamDroid har Google dog lovet at forbedre sikkerheden i Android Market.)

I ny og næ downloader jeg applikationer til Android fra andre steder end Android Market, men jeg er altid bevidst om de potentielle risici, og jeg anvender altid en antivirus-scanner efter download for at højne sikkerheden.

Læs Business Centers guide om, hvordan du tjekker en app inden du downloader den til din mobil.

Som tommelfingerregel er det altid en god idé at hente Android-software direkte fra Googles Android Market.

5. Google Android Antivirus
En god mobil antivirus-applikation kan scanne nye Android-downloads for åbenlyse tegn på fuskeri, som for eksempel underlige anmodninger om tilladelser og downloads. Og der findes en række antivirus-apps både gratis og mod betaling på Android Market.

Jeg kan ikke personligt garantere for deres effektivitet, men helt generelt så er det bedre at køre med en af de populære antivirus-applikationer end ingen overhovedet.

Den applikation, jeg har brugt mest, er Lookout Mobile Security. Lookout findes som gratis download med en basal antivirusscanner. Man kan også opgradere Lookout med mere dybdegående sikkerhedsfunktioner, men den gratis version burde dække almindelige brugeres basale behov.

En anden gratis antivirus-mulighed er applikationen med det beskrivende navn Antivirus Free.

Selv hvis man vælger ikke konstant at køre med en Android antivirus-applikation, er det stadig en god idé at downloade en, så man med jævne mellemrum kan scanne sin enhed for potentielt farlige apps.

6. Android Wireless Connectivity og sikkerhed

Som hovedregel er det altid en god ide at afkoble enhver ubrugt trådløs forbindelse på sin Android smartphone. Du bør, med andre ord, slukke for din Wi-Fi, når du forlader dit hjem og ikke regner med at være i nærheden af et andet trådløst netværk resten af dagen. Når du er færdig med at bruge dit Bluetooth headset i bilen, skal du slukke for Bluetooth.

Det vil ikke bare spare på batteriet, men også mindske risikoen for, at folk med lyssky hensigter kan spore eller koble sig til din enhed, uden at du ved det.

Derudover bør man altid slukke for Wi-Fi auto connect - hvis den mulighed findes på enheden - for at sikre, at du ikke automatisk kobler til offentlige netværk, hvorigennem andre kan få adgang til dine data.

Sluk for Wi-Fi auto connect ved at åbne *Indstillinger*, vælg muligheden *Trådløs og Netværk* og derefter *Wi-Fi indstillinger*. Hvis din enhed indeholder en auto connect-mulighed, så burde den ligge her. Slå funktionen fra.

På *Trådløs og Netværk*-skærmen kan man desuden finde Bluetooth-indstillingerne. Åben Bluetooth-indstillinger og slå Bluetooth fra, hvis ikke det allerede er gjort.

Klik derefter på *Device Name* og sørg for at ændre enhedens navn til noget, der er unikt og har forbindelse til dig. Det vil mindske fremtidig forvirring, hvis du ønsker at tilkoble din smartphone til en anden enhed via Bluetooth.

Hvis din Android-enhed understøtter mobile hotspot-funktioner, så bør du desuden sikre dit personlige netværk. Du starter med at åbne *Trådløs og Netværk*-indstillingerne igen, hvorefter du scroller ned og vælger Mobilt Wi-Fi-hotspot eller Portable Wi-Fi hotspot. Så aktiverer du Wi-Fi hotspot-funktionerne og klikker på Indstillinger for Mobilt Wi-Fi-hotspot.

Når hotspot-funktionerne er blevet aktiveret, burde din WiFi Hotspot Settings-side give dig mulighed for at konfigurere trådløse hotspot.

Åben menuen, giv dig selv et unikt navn, vælg WPA2 PSK-sikkerhed i dropdown-menuen og lav et password til netværket. Gem dine ændringer og du har et sikkert WiFi hotspot.

Det er en god øvelse at sørge for at slukke for sit WiFi hotspot, når det ikke er i brug, så uautoriserede parter ikke kan gå på dit netværk og æde dit månedlige dataforbrug eller skabe adgang til informationer i din enhed.

Oversat af Marie Dyekjær Eriksen