Positionsdata

Platstjänster, eller Location Services, är samlingsnamnet på de funktioner i mobila enheter som står för positioneringsdata via GPS.

Tänk på att

GPS fungerar även om telefonen är i flygplansläge, och alla appar som kan använda Platstjänster kan spara undan din position tills dess att Internet blir tillgängligt igen. GPS är inte heller det enda sättet för telefonen att veta vart den är, utan andra signaler som mobilnätverk och Wi-Fi kan också användas.

Säkerhetsåtgärder

- **Stäng av enheten**
- **Stäng av platstjänster** för hela enheten
- **Se till att inga appar** har tillgång till platstjänster
- **Stäng av eller ta bort tjänster** i telefonen som kan avslöja position, till exempel Hitta min iPhone
- **Tillåt aldrig hemsidor** att komma åt din platsinformation

Metadata

Metadata är dold information i en fil eller ett meddelande, t.ex. GPS-koordinater i en bild.

Tänk på att:

En fil kan innehålla mer information än du vet om, och genom att skicka den till fel person kan du oavsiktligt avslöja t.ex. information om var du befinner dig. Detsamma gäller när du laddar upp filer.

Säkerhetsåtgärder

- **Stäng av platstjänster**
- **Undvik att ladda upp filer**, t.ex. bilder, på internet. Tänk på att allt du skickar kan innehålla dold information, även MMS och e-postmeddelanden. Ta inga onödiga risker.

Lösenord

och användarnamn

• Starka och unika lösenord

Basera aldrig lösenord på namn, födelsedagar, orter, husdjur eller intressen. Skapa långa lösenord med en kombination av bokstäver, tecken och siffror. Skapa alltid unika lösenord till alla tjänster. Ge inte någon annan tillgång till dina lösenord.

• Använd tvåfaktorsautentisering

• Använd lösenord till alla enheter,

t.ex. laptopen och mobilen.

• Anonyma användarnamn

Använd ett eller flera alias istället för ditt riktiga namn när du skapar konton för appar, email, hemsidor och sociala medier.

Digital kvinnofrid

Digital kvinnofrid är ett samarbete mellan Uppsala Kvinnojour och Sentor.

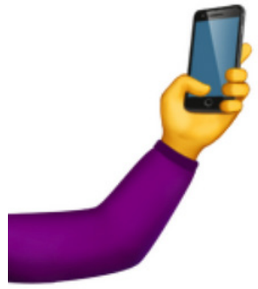
UPPSALA KVINNO JOUR

sentor

Digital kvinnofrid

Säkerhetsrekommendationer

för din smartphone, appar och sociala medier



Rekommendationerna ger inte ett heltäckande skydd, men utgör en bra grund för en ökad digital säkerhet. Säkerhetsrekommendationerna är framtagna av cybersäkerhetsföretaget Sentor.

Sociala medier & appar

Tänk på att

Många appar sparar information, t.ex. platsinformation, som kan läcka. Informationen kan också finnas tillgänglig för personer som du delar konton med eller som har tillgång till dina konton. Många gånger samycker vi till att dela t.ex. platsinformation, till exempel i träningsappar, dejtingappar och sociala medier. Bilder och statusuppdateringar kan också avslöja information om var du befinner dig.

Säkerhetsåtgärder

- **Använd inte delade konton** till tjänster som Netflix och Spotify: andra användare på kontot kan se din IP-adress och aktivitet
- **Byt lösenord** på alla konton om en hotbild uppstår
- **Se över sekretessinställningar** i alla dina appar så att du inte delar information offentligt
- **Stäng av platstjänster** för alla dina appar
- **Ta reda på vilken information** dina appar samlar in och delar
- **Radera onödiga appar**

Mobila molntjänster

T.ex. iCloud, Google cloud och Samsung Cloud

Tänk på att

Information som lagras via molntjänster är tillgänglig från alla enheter som exempelvis är inloggade via iCloud. Det innebär att det går att läsa sms och se bilder från en dator som är ansluten till samma iCloud-konto som din telefon. Molntjänster används också för funktioner som Hitta min iPhone.

Säkerhetsåtgärder

- **Koppla bort enheter** från molntjänster
- **Byt lösenord och e-postadress** på dina befintliga molntjänster

Nätverkssäkerhet

Vad är en IP-adress?

Varje enhet som är ansluten till Internet har en unik IP-adress, som kan liknas vid ett telefonnummer. När du t.ex. besöker en hemsida kan sidan se din IP-adress, på samma sätt som en mottagare kan se vem som ringer.

En IP-adress kan kopplas till en fysisk plats: ofta med ganska dålig precision, t.ex. en stad eller mindre ort, men ibland ner till kvarter.

Vad är VPN?

VPN är en teknik man kan använda för att "studsa" via en annan IP-adress: mottagaren ser då inte den riktiga avsändaren, utan en adress som tillhör VPN-leverantören. VPN skyddar mot vissa hot, men absolut inte alla.

Alla sidor och appar du använder får reda på din IP-adress. Dina enheter sänder hela tiden ut viss information på nätverket, t.ex. datornamn och telefonnamn. Denna information kan vara känslig.

Säkerhetsåtgärder

- **Byt namn** på dina enheter
- **Slå på inkognitoläge** i din webbläsare
- **Rensa webbläsaren** regelbundet
- **Besök inte sidor du inte litar på**
- **VPN skyddar mot vissa hot,** men absolut inte alla. Om du använder VPN, försäkra dig om att du förstår vilket skydd det ger.

Digital kvinnofrid

Mobilt malware,

trojaner och virus

Malware är samlingsnamnet för skadlig kod som t.ex. kan avlyssna eller spåra din enhet. Oftast drabbas du av malware om någon haft fysisk åtkomst till din enhet, eller om appar installerats från icke-officiella källor.

Säkerhetsåtgärder

- **Byt telefon**
- **Fabriksåterställ** din befintliga telefon, om du inte har möjlighet att skaffa en ny
- **Radera alla onödiga appar**
- **Installera aldrig appar** från någon annan källa än App Store eller Google Play
- **Låna aldrig ut din telefon**
- **Installera alltid tillgängliga uppdateringar,** de "täpper till" nya säkerhetshål

Spoofing och identitetsstöld

När någon skickar e-post eller SMS från en falsk avsändare kallas det spoofing. Angripare skickar ofta meddelanden från andra avsändare för att lura offret.

Tänk på att

Angripare ofta skickar meddelanden från falska nummer som tillhör någon offret känner, t.ex. en förälder, ett barn eller en myndighet.

Säkerhetsåtgärder:

- **Lita aldrig på avsändarfältet,** även om ett meddelande dyker upp under en känd kontakt
- **Använd chattappar som Signal eller WhatsApp** istället för SMS