**Digitala fotspår – pusselbitarna som berättar om ditt liv online**

Varje gång vi scrollar på sociala medier, söker på Google, lyssnar på musik eller kollar på en video lämnar vi små spår efter oss. Dessa spår kallas för digitala fotspår och kan liknas vid pusselbitar som berättar mycket om våra online. Att lämna digitala fotspår är en naturlig del av att leva i en uppkopplad värld, men genom att vara medveten om dem kan du ta kontroll över din integritet och öka din säkerhet på nätet.

**Vad är digitala fotspår?**

Digitala fotspår är dataspår som vi lämnar varje gång vi gör något online. De består av all information som skapas och lagras när vi är uppkopplade, vare sig vi gör det medvetet eller inte. Vissa fotspår är ganska tydliga – som att lägga upp en bild på sociala medier eller kommentera en video – medan andra är mer osynliga, som att bara besöka en webbplats eller ha en telefon med påslagen platsinformation.

**Aktiva och passiva fotspår**

Det finns två typer av digitala fotspår: **aktiva** och **passiva**. Aktiva fotspår är de som du själv medvetet lämnar när du interagerar online. Det kan till exempel handla om när du lägger upp bilder, videor eller uppdateringar på Snapchat, Instagram eller TikTok. Dessa fotspår är ofta enkla att kontrollera eftersom du själv bestämmer vad du delar.  
  
Passiva fotspår är data som samlas in om dig utan att du alltid är medveten om det. Dessa kan exempelvis vara din IP-adress som registreras varje gång du är online eller data som webbplatser samlar in om vilka sidor du besöker och hur länge du stannar. Vissa appar samlar även in platsdata – det vill säga information om var du befinner dig – även när de inte används aktivt. Dessa fotspår skapas automatiskt, och det kan vara svårt att ha full kontroll över dem.

**Fler exempel på digitala fotspår**

**Incheckningar**: När du checkar in på platser via sociala medier som Facebook eller Instagram, sparas din plats och kan ses av andra.

**Onlineköp**: Varje gång du handlar online, sparas information om vad du köper, hur ofta och dina betalningssätt.

**Musik- och videostreaming**: Plattformar som Spotify och YouTube sparar data om vad du lyssnar och tittar på, vilket de kan använda för att rekommendera nytt innehåll.

**Navigering och kartor**: Appar som Google Maps och Snapchat kan visa dina besökta platser, vilket kan skapa en detaljerad karta över din vardag.

**Varför är det viktigt att känna till sina digitala fotspår?**

Digitala fotspår används ofta av företag för att lära sig mer om oss och våra intressen. Har du till exempel någon gång märkt att du ser reklam för saker du just sökt på eller pratat om? Det beror på att företag använder dina digitala fotspår för att rikta annonser mot dig och andra med liknande intressen.

Men det är inte bara företag som använder våra digitala spår. För en person som utsätts för våld i en nära relation kan digitala fotspår utgöra en risk, särskilt om den andra personen har tillgång till den utsattes telefon, lösenord och digitala konton. Genom att övervaka platsdata, läsa meddelanden eller spåra aktiviteter online kan en person använda digitala fotspår för att kontrollera och övervaka sin partner.

**Hur kan du minska dina digitala fotspår?**

Att vara medveten om dina digitala fotspår och kontrollera vad du delar är en viktig del av säkerheten online. Det handlar till stor del om att tänka efter innan du postar något eller delar känslig information. Några tips för att minska och ta kontroll över dina digitala fotspår är är att:

**Stänga av platsdelning när den inte behövs**

Många appar använder platsdata även när appen inte används. Genom att stänga av platsdelning i mobilens inställningar kan du minska mängden platsdata som delas.

**Använda inkognitoläge för privat surfning**

Webbläsare har ofta ett "inkognitoläge" eller "privat läge" som inte sparar din surfhistorik, cookies eller inloggningsuppgifter efter att du stängt sessionen. Detta minskar dina passiva fotspår.

**Granska appbehörigheter**

Många appar ber om tillgång till information de egentligen inte behöver, som kontakter, kamera eller mikrofon. Genom att ändra apparnas behörigheter i inställningarna kan du minska mängden data de samlar in om dig.

**Begränsa vad du delar på sociala medier**

Tänk efter innan du lägger upp bilder, incheckningar eller personlig information. Genom att hålla vissa saker privata eller dela dem med en begränsad publik minskar du risken att lämna känsliga fotspår.

**Skapa starka lösenord och använd tvåfaktorsautentisering**

Genom att använda starka och unika lösenord för varje konto och aktivera så kallad tvåfaktorsautentisering ökar du säkerheten och minskar risken för att någon annan får åtkomst till din data.

**Avsluta och ta bort gamla konton**

Många har gamla konton på webbplatser eller i appar som de inte längre använder. Genom att ta bort dessa konton kan du minimera de fotspår du lämnar på internet över tid.