Så stjäl (hackarna) kriminella din identitet online (och så skyddar du dig)

Identitetsstöld
Tillhör en av de vanligare brottstyperna i Sverige (och världen) och är tyvärr en typ av brott som ökar.
Här berättar experterna de kriminella knep och hur du skyddar dig mot dem.
Vi tillbringar en allt större del av våra liv på nätet samtidigt som e-handel och andra digitala verksamheter växer sig än större, och i och med detta finns det mycket att vinna på att stjäla någons identitet. Allt från att kunna köpa saker i personens namn till att utpressa personen på pengar.

De **initiala konsekvenserna** kan vara att man förlorar kontrollen över det som bara och endast är ens eget, till exempel tillgång till sin personliga e-post, bankkortsuppgifter, sociala medier och annat viktigt. Det kan dessutom ta lång tid innan man upptäcker vad som pågår och då kan skadan redan vara skedd.
Den som råkar ut för den här typen av brott blir i bästa fall bara av med sitt e-postkonto, men kan i värsta fall få hem räkningar för saker som hen själv inte har beställt eller bli av med sina bankkortuppgifter och pengar.
Men det handlar även om en känslomässig resa. Dels den att ha blivit utsatt för ett brott, dels att integriteten kränks.

Svaga och återanvända lösenord öppnar många dörrar för kriminella.
Ytterligare en problematik när det kommer till identitetsstölder är allt arbete som krävs för att komma tillrätta med situationen. Du kommer att behöva spärra konton, kort, sidor hos olika myndigheter och företag med mera.
Identitetsstölder inverkar på så många plan och nivåer att en enda myndighet eller ett enda företag har svårt att hjälpa den drabbade för att reparera allt det som den kriminella har orsakat. Det är svårt att få hjälp till 100 procent, oavsett vem man vänder sig till.

Hur hittar den kriminella dig?
Frågan är då hur man kan skydda sig mot att någon stjäl ens identitet. Det första är att förstå hur identitetsstöld går till.
Ofta handlar det om att uppgifter om dig har läckt ut på ett eller annat vis.
Antingen genom att du själv haft en otillräcklig säkerhet, exempelvis **att du har haft ett för svagt lösenord, klickat på en skadlig länk eller varit på ett osäkert wifi-nätverk.**
Eller så kan det bero på att ett företag – där du har dina uppgifter sparade – har råkat ut för en dataläcka. Vidare kan skadlig programvara i dator eller mobiltelefon röja dina uppgifter.

Just svaga lösenord är dock den vanligaste orsaken.
Svaga och återanvända lösenord öppnar många dörrar för kriminella och ligger till grund för nästan hälften av alla identitetsstölder i världen idag. De kriminella använder sig av smarta verktyg som avslöjar individers lösenord och i synnerhet då lösenord är för enkla, korta och förutsägbara.
Många människor väljer också att logga in med hjälp av andra tjänsters login som de redan använder, till exempel **Google, Facebook och LinkedIn** (vilket är bekvämt men kan vara farligt). Vilket också innebär att om lösenordet till den tjänsten läcker, står dörren öppen för den kriminella att få direktåtkomst till alla platser där individen loggar in med detta konto.

Lär dig upptäcka risker
Genom att skydda dig själv så långt du kan i din vardag, minimera risken att råka ut för brott. För att minimera risker ska du ha

1.Ett starkt lösenord.
2. Långa, osammanhängande och svårgissade.
3. Minst åtta tecken, men gärna fler.
Dessutom ska du ha **olika lösenord på olika tjänster** för att ytterligare försvåra för den kriminelle.

Om tjänsten ifråga drabbas och ditt lösenord läcker blir följderna betydligt mildare om du direkt vet att du använder ett unikt lösenord på den aktuella tjänsten och som inte fungerar någon annanstans.

En annan bra funktion som många har idag är **multifaktorautentisering** (långt fint ord). Det innebär att du behöver göra mer än en sak vid inloggning, vid sidan av att fylla i ditt lösenord (1 sak). Exempel på det är att svara på en fråga eller få en kod skickad till sin mobiltelefon (sak 2).

Det är också viktigt att du håller koll på när dina **program och operativsystem behöver uppdateras.**
Ha alltid ett **risktänk** när du får länkar, underliga frågor från okända människor eller konstiga meddelanden från bekanta.

Sist men inte minst, kom ihåg att vara försiktig med vad du delar med dig av på olika tjänster.

Summering

1. Använd unika lösenord och ta, vid behov, hjälp av en säker lösenordshanterare (programvara som på ett säkert sätt hanterar krångliga lösenord).
2. Ge aldrig ut dina lösenord eller koder till någon.
3. Träna din ökade medvetenhet kring risker och beteende på nätet - tänk efter innan du klickar eller svarar någon som kan vara en annan än den han/hon utger sig från att vara.
4. Agera likadant i den digitala världen som du skulle ha agerat i verkligheten.
5. Håll dina uppkopplade enheter uppdaterade, använd **säkerhetsprogram** och ha för vana att byta dina lösenord då och då.