

2016-11-22 16:08 CET

Skydda dig mot nätbedrägerier - skapa starka lösenord!

Omkring 10 miljoner svenska konton med lösenord finns tillgängliga på internet, enligt Sveriges televisions program "Dold". Uppgifterna som finns tillgängliga gäller framförallt privatpersoners konton och kan vara hackade för flera år sedan. Här får du information om hur du kan skydda dig och skapa starka lösenord.

Med starka lösenord och ett genomtänkt användande av dina lösenord och koder minskar du risken för att obehöriga kan logga in på sidor som är viktiga för dig, och utge sig för att vara du. Bedragare som lyckats komma över dina lösenord och koder kan till exempel utge sig för att vara du och skicka meddelanden, med dig som avsändare, för att lura närstående att sända pengar till bedragaren.

– Ett bra sätt att skydda sig är att ha många olika lösenord och inte använda samma lösenord på flera olika webbtjänster och var extra noga med lösenord till e-postkonton och dina sociala medier, annars finns det risk att bli utsatt för olika typer av bedrägerier, säger Robert Jonsson, expert på cybersäkerhet på Myndigheten för samhällsskydd och beredskap.

– Det är också mycket viktigt att ha så unika lösenord som möjligt, med många tecken. Blanda gärna stora och små bokstäver, siffror och specialtecken. Vänta också med att byta till ett nytt, starkt lösenord hos din leverantör till dess att du försäkrat dig om att leverantören verkligen har täppt till hålet som orsakat lösenordsläckan. Om hålet inte är tilltäppt kan ju angriparen sitta kvar och vittja det lösenordet också, säger Robert Jonsson.

Tips om hur du hanterar dina lösenord och koder:

- Skapa ett starkt lösenord genom att sätta ihop tre slumpmässiga

ord tillsammans med siffror, specialtecken, stora och små bokstäver. Lösenordet bör vara minst 12 tecken långt.

- Välj aldrig ett lösenord som kan kopplas till dig, exempelvis bilens registreringsskylt eller personnummer.
- Använd inte vanliga ord som "sommar" eller kombinationer som "qwerty" (tecken i en följd på tangentbordet).
- Använd alltid olika lösenord för olika inloggningar och byt regelbundet lösenord för de viktigaste tjänsterna.
- Använd tvåfaktorausautentisering vid inloggning om möjlighet finns. Tvåfaktorausautentisering får man genom att kombinera två säkerhetsmetoder, till exempel att samtidigt ange ett hemligt lösenord och att en pinkod skickas till mobilen. Det finns också fler olika typer av tvåfaktorausautentisering.
- Lämna aldrig ut ditt lösenord till någon annan.
- Ge aldrig någon annan dina koder till din internetbank. Ingen annan än du behöver känna till dem, då det är tekniskt omöjligt för någon annan att logga in på sin bank med dina koder.
- Använd en lösenordshanterare, en programvara/tjänst som skapar och lagrar komplicerade lösenord för att få till unika och svårgissade lösenord.

[Mer information om starka lösenord och hur du hanterar din information säkert hittar du på DinSäkerhet.se](#)

[Personligt test ID-kapning](#)

Myndigheten för civilt försvar är den ledande, inriktande och samordnande myndigheten i det civila försvaret. Myndigheten säkerställer att samhället är förberett för kris, höjd beredskap och krig.

Kontaktpersoner



Myndigheten för civilt försvars presstjänst

Presskontakt

press@mcf.se

010-240 44 44



Anna Wennerström

Presskontakt

Pressansvarig

anna.wennerstrom@mcf.se