Dataläckor

Vad är hänt? – Stora dataläckor har nyligen upptäckts. Det gäller bl. a. lösenord/konton från tjänster som **Netflix** och **Facebook**.

OBS! Viktigast att vara medveten om är att dina bankkonton och andra viktiga ekonomiska tjänster är säkra, eftersom de skyddas av BankID.

Experter varnar för att denna information nu kan komma att användas för identitetsstöld och andra cyberattacker som till exempel nätfiske (falska e-postmeddelanden). Det kan leda till en en stor ökning av falska e-postmeddelanden. Som alltid är det viktigt att du är försiktig när du öppnar mejl, speciellt från okända avsändare, klicka aldrig på länkar i mejl som du inte är helt säker på kommer från rätt avsändare och samma sak gäller även SMS.

Bluff-sms

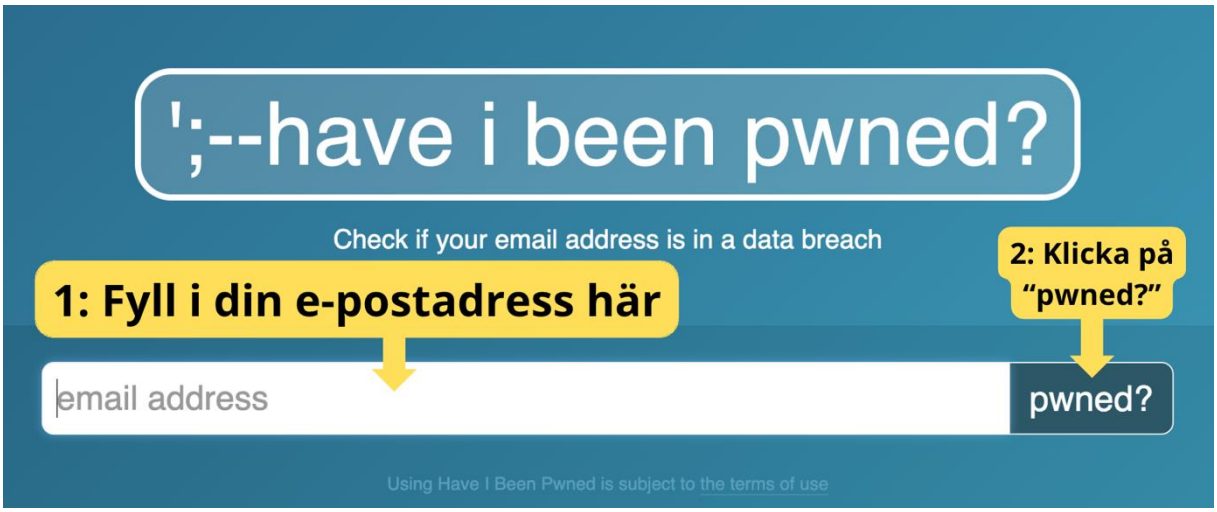
Flera telekomoperatörer har valt att gå samman och skapa ett gemensamt nummer, 7726, för att förbättra bekämpningen av bluff-sms.

Så rapporterar du

Om du har fått ett bluff-sms som gör dig misstänksam och som du vill rapportera behöver du bara vidarebefordra meddelandet till nummer 7726. På så sätt får operatörerna information om sms:et och dess innehåll, och kan förhindra att det skickas till fler personer.

Siffrorna motsvarar ordet SPAM på knappsatsen i telefonen och är globalt etablerat för att rapportera bluff-sms.

Hur kontrollerar du om dina uppgifter är drabbade?
Besök sidan **Haveibeenpwned.com** - Där kan du fylla i din e-post adress och sedan klicka på knappen *pwned för kontroll om dina konton har påverkats. (se bild nedanför)



Efter du klickat på knappen "pwned" så kommer du kunna se om något av dina konton har förekommit i någon dataläcka. Antingen så får du den gröna rutan "Good news" och då är allt okej och du behöver inte göra någonting.

Om du ser en röd ruta på skärmen, var lugn och oroa dig inte. Det är inte en farlig situation.

Här är några tips för vad du ska göra:

1. **Titta på sidan:** Bläddra lite längre ner på sidan. Där kommer du att se en lista över vilka av dina konton som har påverkats.
2. **Ändra lösenord:** Till exempel, om du ser att ditt Facebook-konto är med på listan, betyder det att du bör byta lösenord för Facebook så snart som möjligt.
3. **Om du använder samma lösenord någon annanstans:** Om du använder samma lösenord på andra webbplatser, är det viktigt att du även byter lösenord på dessa sidor.
4. **Skapa starka lösenord:** Använd en kombination av stora och små bokstäver, siffror och specialtecken för att göra dina nya lösenord starkare.

5. **Aktivera tvåfaktorsautentisering:** För extra säkerhet, aktivera tvåfaktorsautentisering på dina konton om det finns tillgängligt för den tjänst du använder.

Tvåfaktorsautentisering – dubbelt så säker inloggning
Det är en inloggningsmetod som innebär att en identitetskontroll görs med hjälp av två skilda former av information. Utöver ett vanligt lösenord måste användaren identifiera sig med ytterligare en faktor, ett exempel är när du använder ett bankid.
