FRIVILLIGA RESURSGRUPPEN

SÄKERHET PÅ SOCIALA MEDIER

Sociala medier är ett väldigt effektivt medium som skapar helt nya möjligheter inom kommunikation, men precis som på Internet i allmänhet är det viktigt att vara medveten om att den informationen man lägger ut är publik på nätet, och att ha en god nivå av säkerhetsmedvetande. Det här dokumentet innehåller några råd om vad du bör tänka på när det gäller säkerhet.

Informationen kan vara till nytta för dig som individ. För dig som är ansvarig för sociala mediekonton för en FRG är det givetvis särskilt relevant att hålla en hög grad av säkerhet för organisationens konto, som ju är en del av FRG:s ”ansikte utåt”.

Nedanstående information är anpassad för användare av den digitala marknadsförings- och kommunikationsplattformen för FRG. Dokumentet finns nedladdningsbart på www.civil.se/FRG/ under ”Sociala medier”.

ALLMÄNT

När du använder sociala medier, iakttag försiktighet precis som på Internet i allmänhet:

- Välj starka lösenord som bara du kan identifiera, och förvara dessa säkert. Ett bra lösenord innehåller i regel minst 8 tecken och gärna både små och stora bokstäver samt siffror eller specialtecken i kombination. Undvik att använda personliga uppgifter i lösenord som andra kan gissa sig till (namn, födelsedatum, etc)
- Minska risken om någon obehörig skulle få tag på ett lösenord - använd inte samma lösenord för olika konton utan unika lösenord för respektive konto.
- Byt lösenord regelbundet.
- Använd inte samma lösenord till olika konton, utan olika lösenord – på så sätt minskar du risken om någon skulle komma åt ett av dina lösenord.
- Lämna inte ut ditt lösenord till andra.
- När du skriver in ditt lösenord för att logga in på en sida eller i en applikation, kontrollera att hemsideadressen för sidan verkligen stämmer – så att du är på den officiella sidan och inte på en ”bluffsida”. Detta är särskilt viktigt att vara försiktig med om du får e-postmeddelanden som frågar om ditt lösenord.
- Se till att du är insatt i säkerhetsinställningar för de applikationer du använder.
- Se till att ha säkra återställningsalternativ (många tjänster låter dig ha ett telefonnummer eller en alternativ e-postadress för att enkelt återställa lösenordet om du glömmer det eller får problem med inloggning).
- Var medveten om att bilder och text du lägger ut på sociala medier kan laddas ner av vem som helst på nätet, om du inte valt att göra din profil privat. Oavsett, var omdömesfull i vilket material du lägger ut online.

Skapat av Patrik Vuorio, VolunteerPower Sweden (www.volunteerpower.se), december 2014.
Anpassade dokument har tillhandahållits till Civilförsvarsförbundet för användning i FRG-verksamheten i samband med projektet **Digital marknadsförings- och kommunikationsplattform för FRG**.

FRIVILLIGA RESURSGRUPPEN

NOTERINGAR FÖR SOCIALA MEDIEANSVARIGA FÖR LOKALA FRG

I projektet för konton för FRG på sociala medier, när det gäller "officiella konton" är prioriteten främst för administratörer av dessa konton/sidor lösenordsskydd, säkerhetsrutiner och viss medvetenhet om källa när man delar information.

Överlag, se till att mer än en ansvarig har tillgång till lösenord till era konton på sociala medier, så att FRG kan ha omedelbar access till dessa vid behov om någon är på semester.

Håll regelbunden koll på era konton så att inget otillbörligt material läggs till i kommentarer av utomstående, etc. I sådana fall, ta skyndsamt bort detta från kontot. Ni kan på Facebook själva välja i inställningarna för kontot om ni vill tillåta kommentarer eller ej, och om dessa måste godkännas i förväg innan de publiceras (se hjälpfunktionen i Facebook för instruktioner).

Undvik/blockera ”följare” av tveksam natur som kan förekomma exempelvis på Instagram, dvs konton som uppenbart inte är riktiga personer utan skräpkonton med annat syfte, eller personer som har olämpligt innehåll på sina konton. Det förekommer ”spamkonton” på Internet och sociala medier och är förhållandevis vanligt. Bäst är att använda funktionen ”blockera” för dessa konton vid regelbundna kontroller så att de inte associeras med kontot.

En god idé är även att göra en viss bedömning när man från ett officiellt konto väljer att följa privatpersoner. Även om ett socialt mediekonto exempelvis självklart inte kan ansvara för innehållet som läggs upp på följares konton, kan en snabb kontroll av deras senaste inlägg åtminstone visa på att användaren verkar vara seriös, innan man väljer att ”följa tillbaka”. Ett uppenbart oseriöst konto är bättre att inte följa (och vid behov blockera).

Vid frågor eller behov av rådgivning kan ni kontakta webbred@civil.se.

Skapat av Patrik Vuorio, VolunteerPower Sweden (www.volunteerpower.se), december 2014.
Anpassade dokument har tillhandahållits till Civilförsvarsförbundet för användning i FRG-verksamheten i samband med projektet **Digital marknadsförings- och kommunikationsplattform för FRG**.