
Troll Angreb

Version for Studierende

Sippo Rossi & Irfan Kanat

25/04/2021



Online Guide: Hvordan Forsvares Mod et Troll Angreb

Synopsis

Denne case beskriver et scenarie, hvor en teenager utilsigtet bliver offer for cybermobning efter hendes post på Instagram går viral. I starten af scenariet er konsekvenserne af mobningen begrænset til de sociale medier, men eskalerer gradvist til også at påvirke offeret og hendes familie i den virkelige verden. Situationen kommer endnu mere ud af kontrol, da hun bliver et direkte mål for cyberkriminalitet og hendes personlige konti bliver kompromitteret af personerne bag cybermobningen.

Casen er ren fiktion, men er baseret på en kombination af flere autentiske begivenhedsforløb rundt om i verden.

Casen

Baggrundsinformation

Anna er en typisk dansk gymnasieelev. Hun har et normalt socialt liv og er aktiv på flere social medier. Hendes 500 Instagram følgere er langt overvejende hendes familie, venner og personer fra samme gymnasie. Hun har en offentlig tilgængelig profil, men stort set ingen uden for hendes omgangskreds interagerer med hendes oplæg og posts.

Sektion 1: En post går viral på sociale medier og begyndende mobning

Anna poster en dag et foto på Instagram med en frygtelig upassende joke relateret til et fodboldhold med nogle hashtag. Hun overvejer ikke budskabet yderligere, og har egentlig ikke nogle særlige tanker bag, men synes kun det var for sjov.

Nogle dage senere finder en meget populær Instagrammer, uden for Annas sociale omgangskreds, fotoet med joken via de hashtags der var tilføjet, og bliver meget irriteret. Influenceren deler et screenshot og navnet på Annas Instagram profil, derved bliver posten nu eksponeret til over 100.000 personer, hvilket er over 200 gange mere omfangsrigt end postens oprindelige tiltænkte publikum.

Med det resultat, at Anna vågner op til flere tusinde notifikationer på hendes telefon. Hendes profil bliver pludseligt besøgt af tusindevis af personer, der kommenterer både hendes nuværende og tidligere posts. Desuden videredeler mange screenshottet postet af Influenceren med kommentarer, der spænder fra fornærmelser til deciderede dødstrusler. Sletning af det oprindelige foto stopper ikke den løbende strøm af grove og truende kommentarer, der nu blot flyttes til Annas tidligere posts. For at sætte en stopper for mobningen, er Anna nødt til at ændre profilstatus til privat samt skifte navn på hendes Instagramkonto.

Den det stopper ikke her. Der er stadig personer, der aktivt cirkulerer og videregiver screenshots af hendes posts med kommentarer, samt opretter nye hashtags om "canceling" af hende. På dette tidspunkt, spredes effekten yderligere, således Annas kæreste og tætte venner, der er identificeret via hendes tidligere postede fotos, nu bliver ramt af chikanen.

Sektion 2: Doxing, eskalering til virkeligheden

En ukendt person på internettet finder frem til Annas fulde navn, og via en kombination Google og andre målrettede søgninger, klarlægges både hendes fulde hjemmeadresse, telefonnummer samt e-mail. Nu begynder forskellige personer at dele hendes kontaktinformationer på et anonymt online forum, der herved formidles til de personer der er rasende over den oprindelige post.

Hvilket resulterer i at Anna konstant modtager chikanerende telefonopkald, der tvinger hende til at skifte telefonnummer. Desuden bliver der uopfordret leveret pizzaer til døren, afleveret breve med dødstrusler og kastet skrald på vinduerne.

Tingene kulminerer, da en person udgiver sig som politiet under en opringning til Annas far og poster den rødglødende samtale til 4chan. Trolle kaster sig over den ældre mans vrede, og Annas far bliver et yndet mål for internetmemes.

Familien er nu tvunget til at få nye telefonnumre og få slettet deres navne fra offentligt tilgængelige registre.

Sektion 3: Uautoriseret adgang

Anna brugte den samme simple adgangskode til alle hendes konti. Uheldigvis blev Annas identifikationsoplysninger lækket i forbindelse med et urelateret hacking angreb af et online forum, hvor hun havde en konto. Hackerne havde delt tusindevis af kontonavne, e-mails og adgangskoder i adskillige internetfora, og nu var hendes kontooplysninger pludselig blevet interessante. Kombinationen af den succesfulde hacking, og det faktum at hun havde brugt samme adgangskode overalt, resulterede i at alle via en heldig søgning på google kunne finde både hendes e-mailadresse og adgangskode. Cybermobberne kunne nu finde og bruge den korrekte adgangskode og have adgang til Annas e-mail konto. Ved at gennemgå e-mailhistorikken kunne mobberne identificere hvilke websites Anna var registreret. Mobberne kunne nu tilgå Annas Snapchat konto, anmode om en ny adgangskode og modtage koden via hendes e-mail. Herefter havde mobberne ikke kun adgang til hendes konto, men kunne ændre alle identifikationsoplysninger.

Mobberne havde nu adgang til alle hendes private beskeder, foto og hendes aktivitetslog, og de udbredte informationerne over internettet. Hvad der var endnu værre, var at hun havde gemt flere

intime fotos, kun tiltænkt hende selv og hendes kæreste, på de involverede konti. Disse billeder blev nu cirkuleret og spredt online.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).