Troll Angreb

Version for Undervisere

Sippo Rossi and 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.

Målgruppe og Undervisningsmål

Studerende på ungdomsuddannelserne og yngre voksne er de primære målgrupper for denne case, men essensen er relevant for alle brugere af sociale medier, uafhængigt af deres alder. Casebeskrivelsen er inddelt i tre sektioner, der analyserer forskellige former for cybermobning og cyberkriminalitet. Hver sektion indeholder specifik læringsindhold; anbefalinger for hvordan disse angreb kan forhindres og den essentielle respons.

Hensigten med casen er at illustrere vigtigheden af, at udvise forsigtighed på de sociale medier, samt overveje etiske problemstillinger, og indse omfanget af de skader cybermobning medfører, specielt i tilfælde hvor tusindevis af mennesker angriber et enkelt individ. Allervigtigst illustrerer casen vigtige cybersikkerhedsprocedurer, og adresserer de primære aspekter af onlinesikkerhed.

Tiltænkt Undervisningsform

Vi anbefaler følgende tilgangsvinkel til undervisningen: Først introduceres de studerende til temaet via den tilhørende videolektion og / eller underviser giver en forelæsning. Derefter læser de studerende casebeskrivelsen, og gennemgår indholdet med medstuderende og underviser. Det anbefales at stoppe op og gennemgå indholdet af hver enkelt af de tre sektioner, i stedet en samlet diskussion efter gennemlæsning af den samlede case. De studerende opfordres til aktiv deltagelse i diskussionerne og til at reflekterer over egne erfaringer.

Vi har inddelt materialet i tre sektioner. Hvor hver sektion beskriver et eskalerende handlingsforløb. Vi foreslår en særskilt klassebaseret diskussion, for hvert tema der præsenteres i en sektion.

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 udgøres langt overvejende af 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 Instragram med en frygtelig upassende joke relateret til et fodboldhold med nogle hashtags. Hun overvejer ikke budskabet yderligere, og har egentlig ikke nogle særlige tanker bag, men synes kun det var sjovt.

Nogle dage senere finder en meget populær Instragrammer, 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 Instragram 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 Instragramkonto.

Men det stopper ikke her. Der er stadig personer, der aktivt cirkulerer og videredeler 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.

Emner

- Indholdssynlighed
- Overdeling
- Online permanens
- Langsigtet effekt
- Online shaming

Læring

- Indhold kan tolkes forskelligt af andre mennesker
- Når mennesker har foretaget den første aktive handling, kan det være svært at stoppe dem igen
- Indhold forsvinder aldrig fra internettet. Dine posts bliver gemt i flere år
- Massens reaktioner og adfærd er svære at kontrollere

Forholdsregler

- Alt hvad du poster online er potentielt offentligt tilgængeligt
- Vil du acceptere at alle i din omgangskreds har kendskab til indholdet af dine posts?
- Aktivér privat status for profiler og indhold, tjek synlighed og delings indstillinger på sociale medier. Note! Det forhindre ikke dine venner i at dele dit indhold offentligt.

Respons

- Fjern online indhold og skjul konti
- Markér uacceptabelt indhold på sociale medier og forlang indholdet slettet
- Skjul proaktivt alt indhold, og skift navn på alle andre relaterede konti på sociale medier

Spørgsmål for Diskussion

1. Lav en liste med hændelser, der kan have forårsaget hadekampagnen.

Dette vil hjælpe med at starte en god samtale, og sikre at de studerende nemt kan deltage i diskussionen. Lav en liste over hvad Anna har gjort, samt hvad der er uden for hendes kontrol.

2. Er strømmen af beskeder berettiget?

De studerende kan i forbindelse med dette spørgsmål have modsatrettede meninger. Nogle studerende kan have den overbevisning at ”internettet er frit og offentligt tilgængeligt, derfor har andre mennesker ret til at give deres meninger tilkende”. Her er det undervisers rolle at tydeliggøre, at ytringsfrihed giver os ret til at udtrykke vores meninger, men der er en grænse hvor meningstilkendegivelse bliver til chikane. Yderligere er det en god ide at tydeliggøre eftervirkningernes proportioner, eksempelvis hvis baggrunden for cybermobningen kun er en plat vittighed, men den resulterende mobning kan føre til fyring fra job eller selvmord. Men også, at set fra den enkelte aggressors synsvinkel, kan det være svært at indse, at deres hæslige kommentarer og posts, kun er en lille del af de potentielt tusindevis ofret modtager.

3. Hvad kunne Anna have gjort anderledes for at undgå hændelsesforløbet?

Dette spørgsmål er et tillæg til spørgsmål 1. Her er hensigten at forstærke læringsmålene. De studerendes meninger og respons relateres til emnerne; indholdssynlighed, overdeling, online permanens og langsigtet effekt.

4. Hvad skal Anna gøre nu, hvor hun overstrømmes af beskeder og posts.

Her diskuteres copingstrategier. De studerendes svar kan her variere fra; rasende besvarelse af alle beskeder og posts (forkert), til politianmeldelse. Det er på nuværende tidspunkt vigtigt, at forstærke læringen fra videolektionen:

- Ignorer internet Trolls
- Fjern online indhold og skjul konti
- Markér uacceptable posts og forlang dem slettet

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 skifte telefonnumre og få slettet deres navne fra offentligt tilgængelige registre.

Emner

- Hvad er doxing
- Problematikker når flere tusinde mennesker har adgang til kontakt information

Læring

- Hvad er doxing
- Hvilken type privat information er offentlig tilgængelig online
- Hvor har aggressorerne opnået adgang til de personfølsomme oplysninger

Hvordan forhindres angreb

- Undgå at have kontakt og lokaliserings information eller private profil oplysninger offentligt tilgængelig online
- Minimer informationsmængden der er online tilgængelig

** Hvordan ageres hensigtsmæssigt**

- Politianmelde angrebet, hvis ikke allerede gjort tidligere
- Afhængig af trusselsniveauet, overvej midlertidig flytning til et hotel eller familiemedlem
- Nyt telefonnummer

Spørgsmål for Diskussion

1. Hvordan kan aggressorerne have fundet frem til privatadressen?

Indled en samtale hvor de studerende diskuterer hvor privat oplysninger kan forefindes. Pointen er: alt hvad vi foretager os online efterlader digitale spor, der kan lede tilbage til os. Tilsyneladende uskyldige posts kan bruges til at identificere privat oplysninger. Eksempelvis hvis en skole udgiver en offentliggørelse hvor vores navn er inkluderet, kan det afsløres på hvilken skole vi er elev. Et foto der bliver postet online kan have metadata tilknyttet, der kan lede uvedkommende frem til oplysninger om hvor fotoet er taget, eller et vejskilt eller andre lokaliserings oplysninger kan direkte genkendes. Når en hel hær af internet trolls er på krigsstien, finkæmmer de internettet og finder frem til oplysninger, vi aldrig troede kunne sammenkædes eller nogensinde ville blive gjort offentligt tilgængelige.

2. Sæt de studerende til at google sig selv i et nyt privat browser vindue.

Dette er en øvelse der demonstrerer hvad en simpel google søgning kan afsløre. Vi anbefaler brugen af et privat browser vindue, således eksisterende cookie informationer for de studerende ikke benyttes. Dette vis give dem samme synsvinkel som hvis en tilfældig person laver en google søgning på deres navne. Lad de studerende gennemgå den første side af søgeresultaterne, og spørg ind til hvilke oplysninger de har fundet frem til i løbet af bare nogle få minutter. Har de afsløret deres skole, fritidsaktiviteter, sociale medie sider, navne på deres venner eller familie?

3. Hvad kunne Anna have gjort for at begrænse doxing?

Her tilskyndes besvarelsen at være baseret på viden i Sektion 1, og indlæring af emnerne indholdssynlighed, overdeling, online permanens og langsigtet effekt styrkes.

4. Hvad skal Anna gøre nu, hvor fremmede mennesker fremsætter trusler mod både hende og hendes familie?

Her opfordres underviser til at diskuterer emner som at gå til myndighederne, politianmeldelse, låsning af onlinekonti, adresseskift osv.

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 fine både hendes e-mailadresse og adgangskode. Aggressorerne kunne nu finde og bruge den korrekte adgangskode og have adgang til Annas e-mail konto. Ved at gennemgå e-mailhistorikken kunne aggressorerne identificere hvilke websites Anna var registreret. Cybermobberne kunne nu tilgå Annas Snapchat konto, anmode om en ny adgangskode og modtage koden via hendes e-mail. Herefter havde aggressorerne ikke kun adgang til hendes konto, men kunne ændre alle identifikationsoplysninger.

Aggressorerne 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.

Emner

- Passwords; hvorfor brugen af sikre og unikke kodeord for hver onlinetjeneste er vigtigt
- Hvad sker der når dine onlinekonti falder i de forkerte hænder
- Hvorfor det at gemme beskeder eller fotos med personoplysninger indebærer risici

Læring

- Benyt aldrig det samme password til flere onlinetjenester
- Brug aldrig et password der nemt kan gættes, så som fødselsdagsdato, navn, bogstavkombinationer som ”asd” eller ”1234” og lignende
- Vær opmærksom på at materiale og oplysninger der gemmes online, uventet kan blive offentligt tilgængelige via lækager og stjålne kontooplysninger

Hvordan forhindres afsløring af passwords

- Tofaktorgodkendelse
- Password managers
- Vilkårlige og stærke adgangskoder
- Tjek om dine adgangskoder allerede er lækket. Eksempelvis: https://haveibeenpwned.com/

Hvordan ageres hensigtsmæssigt

- Skift alle adgangskoder
- Søg og anmeld websideindhold. Kan i nogle tilfælde afhjælpe problemet, med processen er normalt langsommelig og nogle websides handler ikke på anmeldelser om deling af følsomme oplysninger.
- Anmode Google om at slette relevante søgeresultater via: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=1

Spørgsmål for Diskussion

1. Hvilken fejl begik Anna, der resulterede i at hun mistede kontrollen over hendes onlinekonti?

Her er det meningen at de studerende inddrages i historien og grundtankerne bag cybersikkerhed. Brugen af identiske adgangskoder, ikke være klar over hendes adgangskode blev nulstillet sidste år, ingen benyttelse af multifaktor autentifikation, er nogle af de fejltagelser, der bør indgå i diskussionen.

2. Bed de studerende om at besøge webstedet: haveibeenpwned.com og lave en søgning på deres e-mailadresser. Spørg om de har været udsat for sikkerhedsbrud.

Desto længere og desto flere konti hvor samme e-mailadresse er tilknyttet, des større er sandsynligheden for et brud på datasikkerheden vil afsløre den. Bed de studerende om at kontrollere dem selv via linket og diskutér hvordan det føles.

Anbefal de studerende at tilmelder sig tjenester som Firefox Lockwise eller haveibeenpwned, for omgående at blive gjort opmærksom på sikkerhedsbrud.

3. Anvender du den samme adgangskode for flere onlinekonti? Hvorfor?

Uheldigvis er dette meget almindelig adfærd og skyldes oftest bekvemmelighed. Selvom et unikt og komplekst password for hver konto er væsentligt set fra et sikkerhedsperspektiv, vil de studerende sandsynligvis ikke være i stand til at huske dem. Bed de studerende gennemgå deres begrundelser for valg af adgangskoder, og pointér bedre alternativer som password managerne: LastPass, 1Password eller KeenPassXC.

Via de nævnte apps, kan de studerende gemme deres passwords decentralt og krypteret, let tilgængelige i deres browsere og telefoner.

4. Ved du hvad multifaktor validering, også ofte nævnt som tofaktorgodkendelse eller multifaktor autentifikation, er? Er der nogen der bruger det?

Ideen bag tofaktorvalidering er at indsætte et ekstra sikkerhedselement. Ud over det tilknyttede password, kræves en anden type validering, ofte vil det være indtastning af en unik engangskode sendt til enten en tilknyttet telefon eller e-mail, eller godkendelse i en separat sikkerhedsapp. Det betyder at selvom nogen har den korrekte adgangskode, vil personen ikke være i stand til at logge ind og få adgang til onlinekontoen, fordi der nu kræves adgang til den tilknyttede telefon eller e-mail konto, hvilket udgør det andet trin i valideringen. Derudover vil der modtages en notifikation via e-mail eller telefon, når nogen forsøger at logge ind på onlinekontoen, og derved advares der om at adgangskoden er blevet stjålet.