Troll Attack

Student Version

Sippo Rossi and Irfan Kanat

25/04/2021

Online Survival Guide: How to Fend Off a Troll Attack

Synopsis

This case goes through a story of a teenager who inadvertently becomes a target of cyber bullying after her post on Instagram goes viral. The case begins with the effects of the bullying being limited to happening on social media, but it gradually escalates to affecting the victim and her family also in the physical world. The situation gets even more out of hand as she becomes a target of a cyber crime as her accounts are accessed by the bullies.

The case at hand is a work of fiction, but it was created based on combining elements from multiple real-life cases from around the world.

Audience and Teaching Objectives

The target audience of this case is high school students and young adults, but the key points are relevant to all users of social media regardless of age. The story of the case is divided into three sections that explore different forms of cyberbullying and cyber crime. In each section is a separate set of key learnings as well as recommendations on how to prevent this from happening and how to respond if it has happened.

The case is meant to teach the audience about the importance of caution in social media, as well as to consider the ethics, and to realize the potential damage caused by cyberbullying especially in cases where thousands of people attack one individual. Most importantly, the case also gives an overview of good cyber security practices as well as information about different aspects of online privacy.

Suggested Teaching Format

We recommend the following approach to teaching this topic: First, the students are given an introduction to the topic with the included video lecture and/or a lecture by the teacher and then are given a chance to read the case and discuss it with peers as well as the teacher. We recommend stopping to discuss after each of the three sections rather than only after reading all three. The students should be encouraged to actively participate in discussions and reflect on their own experiences.

We divided the material into three sections. These sections describe increasingly sophisticated situations. We suggest a separate in-class discussion pertaining to the events presented in each section.

The Case

Background

Anna is a typical teenage high school student in Denmark. She has a good social life and is active on several social media sites. Her 500 Instagram followers are mostly her friends, people from the same school and some relatives. She doesn't have a private account but hardly anyone outside of her circle interacts with the content she posts.

Section 1: A post goes viral on social media and the bullying starts

One day Anna posts a photo on Instagram with an awful and inappropriate joke related to some football team with a couple of hashtags. She doesn't think of the content that much and really doesn't even have strong feelings about it but thought it was funny.

Several days later a much more popular Instagram influencer outside of Anna's social sphere is going through posts under the hashtag and sees the photo with the joke and is annoyed by it. The influencer shares a screenshot and Anna's Instagram profile name making the post now visible to over 100 000 people, which is 200 times larger than the original intended audience.

As a result, Anna wakes up to thousands of notifications on her phone. Her profile suddenly gets visited by thousands of people who comment on her current and older posts. Many also share the screenshot posted by the influencer with comments ranging from insults to death threats. After deleting the original photo the commenters don't stop and move on to her older posts. Anna has to make her profile private and changes the account's name in order to stop them.

But the rage doesn't stop there, as people are still circulating the posts, sharing screenshots of her posts with the comments and creating new hashtags about "canceling" him. By the time also her boyfriend and close friends identified from Anna's photos are also getting harassed by these people.

Topics

- Visibility of content
- Oversharing
- Permanence of online content
- Long term impacts
- Online shaming

Learnings

- Content can be interpreted differently by others
- Once people are activated it might be difficult to stop them

- Content never leaves the internet. What you post will be stored somewhere even years from now
- Reactions of masses are difficult to control

Prevention

- Consider everything as potentially public before you post
- Would you be willing to have anyone around you know the contents of the post?
- Make profiles and content private, check visibility and sharing settings on social media sites (Note! This doesn't stop your friends from sharing it publicly)

Response

- Remove content and hide accounts
- Flag on social media inappropriate content and ask for removal
- Proactively hide all other content and change names of other related social media accounts

Discussion Questions

1. List events that may have led to the online hate campaign.

This will get the conversation going and allow students to easily participate. Make a list of things Anna has done, and things that are outside of Anna's control.

2. Is the flood of messages justified?

This is a question where students may have opposing views. Some students may take a stance such as "Internet is a free environment, and the people have a right to respond to Anna." At this point the educator's role is to highlight that freedom of expression allows us to express our opinions, but there is a line between expression and harassment. Furthermore, it is good to discuss of the proportion of things, for example, if the reason behind the bullying is a bad joke but the bullying may result in lost jobs or even suicide. Also that one from the perspective of the bullies, they might not realize their nasty comment is just one of thousands which the target sees.

3. What Anna could have done differently to avoid this outcome.

This question builds upon the first question. At this point we are trying to reinforce the learning objectives. Take the student responses and relate them to visibility, oversharing, permanence, and unforeseen consequences.

4. What Anna should do now that there is a flood of messages coming in.

This is where we talk about strategies of coping. Student responses may range from, furiously responding to every message (wrong) to calling the police. It is important to reinforce the learnings from the video lecture at this stage:

- Don’t feed the trolls.
- Remove content, hide accounts.
- Flag posts as inappropriate and ask for removal.

Section 2: Doxing, things come to real life

Some unknown person from the internet managed to discover Anna’s full name, and with googling and searching different places eventually manages to discover not only Anna’s phone number and email address but also her home address. People share her contact information in an anonymous forum online and it starts to spread among the people enraged by her post.

This results in Anna getting constant prank calls making her have to switch her phone number. However, their house also gets pizza deliveries, death threats sent by mail and trash thrown onto the windows.

Things come to a boiling point when a prank caller posing as the police posts the angry profanity laden response of Anna’s father to 4chan. Trolls rejoice in the old man’s furry and Anna’s father becomes a topic of internet memes.

The family has to change phone numbers and remove their names from public directories.

Topics

- What is doxing
- Issues with tens of thousand of people seeing contact information

Learnings

- What is Doxing
- What private information is visible online
- Where do attackers obtain the private information from

How to prevent

- Avoid having contact information or locations visible to those who do not need it (private profile information)
- Minimize the amount of information available online

How to respond

- At this point informing the police if not done already earlier
- Depending on the seriousness of threats, consider staying at a hotel or a loved one
- Possibly change phone number

Discussion Questions

1. How could they have gotten the home address?

Have students talk about where the private information can be found. The lesson here is this: everything we do online leaves a trace of us. Innocent looking posts can be used to identify private information. The school making an announcement with our name in it may reveal the school we attend for example. A photo posted online may have metadata that may allow strangers to figure out where the photo was taken, or they may simply recognize a street sign… When an army of trolls are on rampage, they go through parts of the internet we thought would never see the light of day and dig that information up.

2. Ask students to open up a private browser window and google themselves.

This is an exercise to see what a simple google search can reveal. We recommend using a private window as the cookies stored for the student will not be used. This will give them the view of a stranger googling their name. Give the students some time to go through the first page of results and ask them what they could discover in a couple of minutes. See if they could discover the school, social clubs, social media pages, names of friends or relatives.

3. What could Anna have done to limit doxing?

This answer will build upon Chapter 1 learnings. The ideas of visibility, oversharing, permanence, and unforeseen consequences should be reinforced.

4. What Anna should do now that there are strangers threatening her and her family?

This is where the instructor should talk about going to the authorities, having accounts locked down, changing addresses and so on.

Section 3: Unauthorized access

Anna used the same very basic password for all her accounts. Unfortunately, Anna's credentials were revealed in an unrelated hacking of an online forum where she had an account. The hackers had shared in several forums the account names, emails and passwords of thousands of people and now suddenly her account information was of interest to people. Due to the hack and fact that she used the same password everywhere, anyone could find both her email address as well as the password with a lucky google search. Now the attackers could find and use the same password and access Anna's e-mail account. By looking at the email accounts history of emails, it allowed the attackers also to see which sites she had registered to. Anna had also a Snapchat account which the attacker could now request a new password to knowing her email and then after receiving it, made it possible for the attacker not only to access this account, but also change the credentials.

The attackers now could see all her private messages, photos and activity log and spread it online. What was even worse, is that she had stored some personal photos meant only for her and her boyfriend on these accounts, which were now circulated online.

Topics

- Passwords, why strong passwords and using a different one in each service matters
- What happens when your accounts fall to the wrong hands
- Why storing sensitive messages and photos on the internet has its risks

Learnings

- Never use the same password in multiple services
- Never have a guessable password (e.g. based on a birthday or name, or asd or 1234)
- Consider that materials stored online might become public due to leaks or stolen account information

How to prevent

- Two factor authentication
- Password management apps
- Randomized passwords
- Check if your passwords have been leaked (https://haveibeenpwned.com/)

How to respond

- Change all passwords
- Search and report content on websites (sometimes might help, but response is usually slow and some sites do not do anything about complaints of sensitive material being shared)
- Apply for google to remove search results (https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=1)

Discussion Questions

1. What was Anna's mistakes that led to the loss of control of her accounts?

Here we want the students to engage with the story and ideas of security. Using the same password, not being aware of release of her password last year, not using multi-factor authentication were some of her mistakes that should be mentioned.

2. Ask the students to go to haveibeenpwned.com and search for their email addresses. Ask them if they have been affected by a data breach.

The longer and the more accounts for the same email address has been used, the greater the probability it will be revealed as part of a data breach. Have the students look themselves up and discuss how that makes them feel.

Recommend that they sign up with services such as firefox lockwise or haveibeenpwned to be notified in case of a breach.

3. Are you using the same password for multiple accounts? Why?

This is unfortunately very common practice and reasons have to do with convenience. While complex passwords unique to each account is definitely better from a security perspective, the students likely won't be able to remember them. Have them go through their reasons, and offer a better alternative: Password managers like lastpass, 1password, and keepassxc.

These apps allow students to keep their passwords in an encrypted format elsewhere, easily accessible through their browsers and cellphones.

4. Do you know what is multi-factor authentication (also known as two step authentication)? Does anyone use it?

The idea of two step verification is that to log in to an account with it, you will be asked in addition to the password to be able to do a second verification that you are trying to log in, which is usually to type in a code that is sent to your phone into a separate application or alternatively to your email account. This means that if someone steals your password, they will not be able to enter the account still because they would also need to access your phone or email account which has the second step of the verification. Additionally, this will cause your phone or email to get a notification when someone tries to log in your account, so you will know if your password has been stolen.