Combatting cyberstalking and how it is evolving

Science, Computer Science



Cyberstalking can be defined: "

- 1. 1. to gather private information on the target to further; and
- 2. 2. to communicate (in real time or not) with the target to implicitly or explicitly threaten or to induce fear. " (Meloy, 1998a, p. 10)

Cyberstalking comes in many forms but usually the intent is to scare or threaten someone via online social media or communication systems. Cyberstalking can be very difficult to deal with due to the fact that many people don't realise that they are being cyber stalked. It is important to understand the different between social media stalking and Cyberstalking. Social media stalking is the act of looking at a friend's, or a friend of a friend's, page on Facebook, Instagram, Snapchat and any other social media service. Many of the younger generation feel obliged to create social media pages since everyone has one and they want to fit in with their friends, however these pages and accounts can be used by cyber stalkers as tools to gain knowledge on you. Many cyber-stalkers look for information online about people who may be vulnerable or easily persuaded target. Cyberstalkers will check your profile page and photos online if you give them access to. Many cyber-stalkers can pretend to be someone else, so that they get information on you. This is called Catfishing. Catfishing is where a person pretends to be someone else to trick someone into believing that you are that person. This can be done by accessing someone else's name, photos and information online, then stealing or copying it to a different account. They will usually appear to be friendly online but can have malicious intent. This is a new method of cyberstalking.

If you think someone may be Catfishing you, there are ways to combat it. Take a photo from their profile which includes them (usually a profile photo) and download it. Then take the downloaded photo then drag and drop it into the google search engine. Google can search multiple pages on the internet by using the photo to find other copies of the exact same photo online. If multiple pages appear, this could mean that the photo is fake. Different pages using the same photos online means that the photo is accessible to many people online to download. This means that anyone can create an account and put that photo onto their profile. A Catfisher will usually have a very low friend following. If someone adds you that you don't know, make sure to check their friends list to see if the account has many friends. If you see any mutual friends with this account, ask your mutual friends how they know this person. If they don't then its best off to ignore the friend request, and if they add again, its time to block that account. It's also important to look at the profile photos the user has set up. Many catfishers use different photos of different people. Check tags, comments, and compare the photos to each other to see if anything seems out of place. Checking tags is important because if there is someone tagged in a photo, check their account to see if they have a fake account too. A large group photo usually has a large amount of tags, if no one is tagged then assume that the photo is fake.

Catfishing accounts usually have strange links on their profiles. Its important to never click them. Links to different websites and pages can be dangerous and lead to giving valuable information away. If you see an account with a link to a different website, it is important to report the account. And lastly, a

catfisher will never show their face on a camera. Using apps such as FaceTime and any video calling service is a great idea to see who is behind the account. Snapchat may seem like a good idea to see who is behind the account, however it is very easy to download photos from online and post them, making it look like they were just taken. It is important to understand how much access of information online you are showing to your friends, friends of friends and the public. Friends get to see all activity on your page and any or all information you decide to show. This information can include: address, first name, middle name, last name, photos, phone number, links to other accounts, email address and your friends list. You must update your security settings so that your information is only shown to a small group of your friends, or your friends list. You must only ever add someone you know in person as a friend online and block users you don't know that add you. If a cyber stalker gets hold of this information, it is much easier for them to catfish your friends and trick them into thinking they are you. It is also easier for cyber stalkers to crack into your accounts with the information given on your pages. Cyber stalkers may impersonate an admin asking for your password online.

Remember, no one will ever ask for your password online, even if they are an admin on your social media platform. If someone asks for your password that you do or don't know, never give them it. Social media pages have been around for years but are a relatively new thing for many people of the older generation. Cyber stalkers are frequently searching for new emails, accounts and profiles made by older men and women because they understand that older men and women don't have as much IT knowledge as a person who

would frequently use the internet, and therefore could give out valuable information easier. If you are an older user of the internet, then it is important to understand that you are more of a target than any other type of user. To conclude, people back in 2003 could have been oblivious to cyberstalking because they didn't use the internet day to day like they do now. I personally believe that as every year goes on people become more relaxed with the internet and start to let their online presence show more and more, which makes cyberstalking more and more difficult to combat due to people putting up more content onto different social media types such as Instagram and Snapchat.