FREQUENTLY ASKED QUESTIONS

1. **What is online harassment?**

Online harassment is generally described as any persistent act carried out via the internet or other forms of electronic or digital devices that causes someone to feel intimidated, threatened, tormented, humiliated, insulted, degraded or uncomfortable to a point where the action creates a hostile environment for that person.

2. **What are some examples of online harassment?**

Some examples of online harassment are stalking, hate speech, blackmailing, doxing, trolling, death threat, rape threat, revenge porn, being bombarded by a large volume of messages continuously, and sending sexually explicit content to someone who doesn't want it.

3. **So is sexting or sending dick pics a form of online harassment?**

It depends on who you are sexting and sending the pictures to. If it is to someone who welcomes it, it is not considered as harassment. Harassment is usually defined as an action that is unwelcomed or unwanted by the person on the receiving end.

However, bear in mind that whatever picture you send through the internet, it is now made available not just to the receiver but the "cloud". You are now faced with the risk of the picture being misused.

4. **Am I a victim of online harassment if someone disagrees with my comment on Facebook and calls me stupid?**

Expression of disagreement or criticism should not be regarded as harassment. Nobody should expect everybody to agree with them. However, the way you disagree or criticise someone can determine whether you are simply expressing disagreement or harassing someone. For instance, if someone deliberately finds every opportunity to disagree with you with the intention of humiliating you; persistently calling you names like stupid, imbecile, bodoh, etc. to a point where you feel degraded, you may become a victim of online harassment.

5. **How is online harassment different from offline/physical harassment?**

- *The harasser can be anonymous online. This makes it difficult, although not impossible, for the authority to identify who the harasser is.*
- *Anonymity means the harasser can get away with his/her action easily, without repercussion and accountability. Someone is less likely to be mean to you in person than when online.*
- *The harassing comments have the potential to spread wide, fast and last forever online. With physical harassment, a victim is able to detach him/herself from the harasser once he/she leaves the scene of the incident but online harassment goes beyond that physical space.*
- *Because online harassment can spread wide, fast and last forever, it means someone else (even a stranger from another country) can join in the harassment with no repercussion or accountability.*

6. **Is there a difference between online harassment and online bullying?**

Online bullying is a form of online harassment. Some international sources have defined online bullying as harassment conducted by children and targeted at children. So, there is generally no difference except the age of the perpetrator and victim.

7. **What is cybercrime then?**

Cybercrime is any criminal activity that takes place on the internet. For example, hacking, phishing, illegal gambling, online sale of illegal substance, child pornography, online sexual grooming, internet scamming, stalking, death threats, etc. So, online harassment is a type of cybercrime but not all cybercrime is online harassment.

8. **What are the laws that regulate online harassment in Malaysia?**

There are currently two major laws that specifically regulate online behaviour.

Section 3, 4 and 5 of the Computer Crimes Act (CCA) 1997 regulates illegal access to computer materials. So if someone tweet-jacks you to post all sorts of humiliating things about you, you can seek redress under this act.

Section 223 of the Communications and Multimedia Act (CMA) 1998 makes it illegal for anyone to post comment, request, suggestion or any other communication which sounds obscene, indecent, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass another person.

Other laws such as Section 506, 507 and 509 of the Penal Code address criminal intimidation and sexual harassment. They can potentially be used to regulate online harassment, particularly if someone has been threatened with violence or sexually harassed.

9. **What about international law on online harassment?**

Currently, the general consensus at the international level is that whatever regulates offline behaviour should apply to online behaviour as well.

10. **Is online harassment a concern in Malaysia?**

Online harassment is increasingly becoming a concern in Malaysia as various studies show. For example, in 2015, CyberSAFE (an initiative by the Ministry of Science, Technology and Innovation (MOSTI), Ministry of Education, Malaysian Commission on Multimedia and Communications (MCMC), and DiGI) reported that 83 percent of 18,000 students surveyed are susceptible to online danger.

A survey conducted by PeopleACT in 2016 reveals more than 50 percent of the 522 respondents said they have experienced some form of online harassment at least once in their life while 41 percent claimed they have felt fearful, threatened or uneasy because of the comments they received online.

There is also a rise in reported incidents of online harassment in the media.

11. How does online harassment affect me?

Anyone who is an internet user can be affected by online harassment. A study conducted by PeopleACT shows that the longer a respondent spends on the internet, the more exposed he/she is to online harassment. The study also indicates that those who express unconventional political or religious views, feminists and LGBTQIs are vulnerable to online harassment.

Online harassment can cause serious mental harm, sometimes resulting in suicidal attempts. It can affect one's self-esteem, personal relationship with loved ones and freedom of expression.

Online harassment such as hate speech can foster and reinforce intolerance of minority or marginalised groups, shutting down alternative or progressive voices which leads to discrimination, extremism and gender-based violence. Shutting down of alternative views will indirectly restrict one's access to information because the information derived from these views are being silenced.

12. What should I do if I am (or suspect) being harassed online?

- *If you know the harasser, make it clear that you do not want him/her to contact you again, preferably in writing so that you can record it.*
- *If you do not know the harasser, block or filter his/her messages. DO NOT reply to unsolicited, harassing or offensive e-mail if the harasser is not known to you. By responding, you confirm that your e-mail address is valid and active.*
- *DO NOT open attachments from unknown sources as they may contain viruses.*
- *Keep a log of any harassing activity.*
- *Save all offending communications for evidence, both electronically and in hard copy (print) and record the date when they are sent to you. DO NOT edit or alter them in any way.*
- *Report the harassment to someone you trust such as your parent, teacher, counsellor, supervisor and if appropriate, a NGO that deals with online harassment such as PeopleACT or the police. You do not have to face this on your own.*
- *Using your name as keywords, conduct a Web search to find out if there is any information about you that is made available on the Web without your consent. Save them both electronically and in hard copy with the date of publication. This way, you can be aware of what information about you is out there.*
- *If the harasser is known to you and harassment continues after you have asked the person to stop, contact the harasser's Internet Service Provider (ISP).*
    - *Most ISP's have clear policies prohibiting the use of their services to abuse another person.*
    - *Often, an ISP can stop the conduct by direct contact with the harasser or by closing his or her account.*
    - *The ISP domain name is identified by the information after the @ (e.g. name @ home.com). Most ISPs have an e-mail address such as postmaster @ domain name that can be used for complaints.*

13. How should I respond to harassing comments/emails?

- *DO NOT reply because that is usually what the harasser wants – to get your attention and to provoke you. But if you feel compelled to reply, DO NOT reply when you are*

angry or upset. Wait until you are composed; you do not want to be perceived as a harasser also.

- *DO NOT rush in to a confrontation. You can risk starting a "flame war" which can rapidly escalate.*
- *DO NOT engage in any question and answer scenarios that make you feel uncomfortable.*

14. What are some of the tips to prevent online harassment?

Every situation is different but in general, here are some DOs and DON'Ts you can adopt to prevent online harassment:

<u>DOs:</u>

- *Make your e-mail password at least seven (7) characters long and ensure that it is a combination of letters and numbers. The best passwords don't spell anything and don't follow a logical pattern.*
- *Change your password frequently.*
- *Review your e-mail signature (the block of text that gets added automatically to the end of an outgoing message). It should provide enough information about you so that you can be identified, but not so much that you are providing your e-mail recipients with personal information.*
- *Limit the information you share in your "out of office" message to the dates of your absence and who to contact. Don't broadcast that you are on vacation or on work-related travel.*
- *Ask before taking a photo of someone and check with them whether it is okay to share before sending it to anyone else or posting it on social media. Once a picture is shared, it is exposed to the risk of being circulated without your knowledge.*
- *Use encryption (e.g. PGP (Pretty Good Privacy)) for person-to-person e-mail to prevent someone from impersonating you or reading your e-mail.*
- *Watch for "red-flags", for example someone asking where you live or where you work.*
- *Be very cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend or business associate.*
- *Set up two e-mail accounts. One used for business correspondence and one that has another name for personal use, etc. Change or cancel your secondary account if you start receiving too much unwanted mail.*
- *Use an anonymous browser to browse the Web. Web sites collect all sorts of information about visitors (e.g., what Web browser you used, your Internet Service Provider and potentially your e-mail address).*
- *Discuss your safety and privacy with your Internet Service Provider. Seek their help and advice.*
- *Make your Internet Service Provider, discussion groups and chat networks have a Code of Conduct (no harassment permitted) and that the policy is enforced by the administrator of the site.*
- *Discuss Internet privacy and safety with your organisation's Internet technology specialist. Follow any policies or procedures your organisation has in place for Internet communication.*

DON'TS:

- *Tell anyone your password or make your password accessible (eg. writing it in your notebook, etc.)*
- *Leave your computer logged in and unattended.*
- *List your e-mail address on any Web pages or give your e-mail address when filling out forms on Web pages unless necessary, if you want to remain anonymous online.*
- *Share personal information in public spaces anywhere online, nor give it to strangers, including in chat rooms.*
- *Give someone else's number out without asking them first.*
- *Reply to texts or voice mails from people you do not know.*
- *Attack or insult anyone while participating in discussion groups. If you disagree with the person, state your position objectively and factually.*

15. What can I do to help combat online harassment?

- *Get educated. Create awareness about online harassment by sharing and discussing it with your peers.*
- *Secure your online identity and data by implementing privacy settings to your email and social media accounts. There are government agencies such as CyberSecurity under MOSTI and also NGOs such as EMPOWER that carry out digital security workshop.*
- *Report cases of harassment to the authorities; eg. parent, teacher, counsellor, employer, MCMC, police, etc.*
- *If possible, call out the harasser – do not let the harasser dominates or controls the narratives of our online space.*
- *Practise discretion when sharing or reposting a picture, video or information that could potentially humiliate or harm someone else. Do not be part of the harasser's agenda but instead foster an environment that is based on kindness and respect.*