PeopleACT

FIVE STEPS TOWARDS SURVIVING CYBER-HARASSMENT (S-K-I-P-S)

SPEAK UP OR STAY LOW
KEEP THE EVIDENCE
INFORM SOMEONE
PROTECT YOUR ONLINE PRESENCE
SELF-CARE

STEP #1: SPEAK UP or STAY LOW

Should I speak up or stay low?

You can choose to speak up against your harasser or stay low, depending on the situation and what your harasser's intention is. For instance, an Internet troll's main purpose is to provoke a reaction from you, which can easily turn into a flaming war once you start giving them attention.

Therefore, the best way to deal with trolls is to stay low and not react to their comments. They are likely to lose interest once they fail to get attention from you and move on to another target.

However, in a situation where someone you know or have just met starts sexting you on WhatsApp, and you don't want to receive such communication from the person again, you should probably speak up to let the person know that their action is unwanted or unwelcome.

Why is it important to speak up?

> "I will not stay silent, so that you can stay comfortable."

It is important to speak up:

i. i. To let the harasser know that their action is unacceptable

> **Scenario #1:**
> Someone sends you unwanted sexually explicit communications on WhatsApp.

By speaking up, you let the other person know their action is not wanted. On the other hand, not speaking up and staying silent may tell the person that you are comfortable with what has been sent or said to you.

Having a record of your disapproval makes a huge difference if you decide to file a formal complaint against the person because any proof that clearly shows you do not welcome the communications will give you an advantage. This is particularly useful when the other person claims that you felt comfortable with the communications or that you welcomed them.

ii. To take back your online space and not allow your voice to be dominated and controlled by the harasser

Scenario #2:
You upload a YouTube video that talks about the importance of having a sexual-harassment free work space to protect female employees.

Two people post these comments on your video:

"Typical of you bitches to be so emotional. If you can't take the heat at work, you're better off blowing your boyfriends at home."

"Would you shut the fuck up already, whore! I bet if I submerge you underwater, you'll still be talking."

The harasser's intention is often aimed at silencing you because of sexism. By not speaking up, you give exactly what the person wants; i.e. silencing feminist voices. When feminist voices are being silenced online, the space that offers a platform for people to discuss feminist ideology or issues is taken away. Therefore, it is important to speak up to reclaim that space and stop anti-feminist narratives to perpetuate, dominate and control our online space.

iii. To take back your power

Scenario #3:
You received this text message from your ex-boyfriend:
"If you don't answer my calls, I am going to send all the naked photos you sent me to porn websites."

When someone extorts you, they are essentially abusing the power they have from possessing compromising images of you. It is understandable for anyone to give in to the extortion to protect themselves. However, by surrendering to the person's demand, they will have further control over you, robbing you of your power. In other words, they get to "win" despite being the bad ones. Not only that, if someone is capable of doing something like this, what is stopping them from extorting more from you as long as they still have your photos? What guarantees do you have that they will not share the photos even after you have given in to them?

By speaking up, whether it is to tell the harasser "no" or to report it to the relevant authority, you are reclaiming your power by not giving the harasser any control over you. In the process of doing so, you are also shifting the blame and stigma often directed at victims (i.e. they are often blamed for sharing nude photos of themselves in the first place), to the harasser instead.

Note: Extortion or blackmailing are serious criminal offences and should be reported to the police.

iv. To educate those who are genuinely ignorant

There are instances where people are genuinely ignorant of their action; not knowing what they did is wrong and that they are causing harm to other people. Speaking up offers the person an insight to their behaviour and thus an opportunity to evaluate their action and learn not to do it again.

v. To prevent someone else from becoming the next victim

Speaking up, particularly when it contributes to educating the harasser, may stop them from harassing again.

Also, speaking up against the harasser in public will expose their misconduct to others and thus help to deter them from doing it again.

vi. To inspire others to speak up

When you speak up, you also inspire others to be brave enough to do the same. This explains why it often takes one person to start filing a complaint against an abusive employer before others who experienced the same to come forward as well.

Everyone needs a role model and by speaking up against your harasser, you can be that role model for others who are going through the same experience as you.

I want to speak up but I don’t know what to say?

Firstly, try not to respond to your harasser when you are still overcome by emotion. Responses that come across as being “too emotional” are often taken less seriously by the harasser who will use that to make you appear “irrational”, “emotional” or “sensitive”. This may also influence how observers see you.

Also, be aware that you do not end up being abusive as well.

When you speak up:

- focus on the facts;
- state the reason why you do not appreciate the harasser’s action from a factual rather than emotional point of view; eg. why their behaviour is not acceptable according to community standard;
- try to get the harasser to justify their behaviour. By doing so, you shift the focus on their conduct and force them to evaluate their action;
- state how you would like the harasser to behave instead; and
- keep your language firm but polite.

Scenario #2:
You upload a YouTube video that talks about the importance of having a sexual-harassment free work space to protect female employees.

Two people post these comments on your video:

"Typical of you bitches to be so emotional. If you can't take the heat at work, you're better off blowing your boyfriends at home."

"Would you shut the fuck up already, whore! I bet if I submerge you underwater, you'll still be talking."

Don't say this:

"Who the fuck do you think you are? What do you fucking know about being a woman in a male-dominated space? When you can give birth, then only you speak. Otherwise, please shut the fuck up and show some respect. What have I done to you to deserve this? Why do you have to be such a dick? Your mother didn't teach you, is it? Watch your back because I'll be watching yours."

Say this instead:

"Your comment has been noted. While you have the freedom to express your opinion, I would like to point out that calling me a whore and suggesting I am better off blowing my boyfriend just because I am pushing for a safer work environment for women is not only abusive but also sexist. Instead of calling me nasty names and throwing sexist ideas on how I can be of better service, why don't you try to convince me and the other people on this space why women do not deserve a safer work environment? Any constructive discussion on this space is welcomed but any further abusive behaviour from you will no longer be tolerated."

What do I do if my harasser becomes more abusive or violent after I speak up?

At this stage, the best thing to do is to block the person so that they can no longer contact you. You can also report the person to the relevant authorities (refer to **STEP 3** for details).

You are advised to document the abusive behaviour immediately to avoid the communications from being deleted. Refer to **STEP 2** on how to document online harassment.

Note: Once you block someone, you will no longer have access to the person's activity on that online platform. This means you won't know what the person could be saying about you.

Is it ok if I don't speak up? Would I be judged?

Yes, it is ok not to speak up. You may be judged for being a coward, but at the end of the day, it is your life, experience and consequences to bear. Nobody really knows what you are going through or how you feel and therefore is in no position to judge you. Other people can advise you to speak up but the decision to do so remain yours as you will be the person who is going to face the consequences of speaking up, not them.

You may consider getting others to speak up for you. Speak to your friends or allies and tell them you need their support to face the harasser. It is not a sign of weakness to ask for help.

STEP #2: KEEP THE EVIDENCE

It is an instinct to delete hateful, repulsive and abusive messages or comments targeted at you. Who wants to be reminded of them, right? However, documenting or keeping a record of the harassment is important for two key reasons:

- Collect the evidence needed to support your complaint especially when you want to pursue any formal or legal action against the harasser; and
- Help you monitor whether the harassment is getting worse and thus determine whether you will need to take any appropriate action.

What information should I keep?

- The date, time and location for each harassment. The location should be where you are when you first read the message or comment, etc. For eg. "I was at the living room at Yanti (my friend)'s house when I read the message."
- The type of communication tool used to send the message or comment. For eg. WhatsApp, Facebook, phone call, SMS, etc.
- Detail of the harasser (if available); name, age, gender, relationship with you (if any), occupation, when and how did you first know each other. The more information you have about the harasser, the better.
- Description of what the harasser did. Record what is relevant only.
- Description of how you felt when you read the harassing message or comment.
- Description of how the harassment has affected you; eg. loss of sleep, emotional trauma resulting in long term psychiatric treatment, changing phone number, deactivated Facebook account, etc.
- Detail of any witness; their name, contact and relationship to you.
- If you suspect that your private information has been shared online without your consent, conduct a Web search using your name as keywords to find out. Save them both electronically and in hard copy with the date of publication.
- If you are a victim of non-consensual pornography (revenge porn), keep the original photo (if it is a selfie) that was shared without your consent. This will prove you own the photo for copyright reason.
- Screenshot or take a photo of the harassing messages or comments with the corresponding Internet Protocol (IP) address (for emails)/ phone number (for WhatsApp/text message)/ social media user ID (for Facebook, Twitter, Instagram, YouTube, etc.). Click here to learn how to do this. https://www.netsafe.org.nz/gathering-electronic-evidence/
- Call log containing the date, time and phone number of each harassment if it happens via phone calls. Take a photo of the caller ID with the corresponding time and date of the harassing call.

Click here for the template on documenting cyber-harassment.
https://cdn.lb.my/sites/9/20171227120624/TEMPLATE-Documentation.docx

ADDITIONAL RESOURCES:

Documentation Tips for Survivors of Technology Abuse and Stalking by the National Network to End Domestic Violence, Safety Net Project
https://cdn.lb.my/sites/9/20171227121054/DocumentationTipsforSurvivor_2014.pdf

How to Gather Electronic Evidence by Netsafe
https://www.netsafe.org.nz/gathering-electronic-evidence/

Evidence Preservation
http://withoutmyconsent.org/resources/evidence-preservation

Where should I keep the information?

There are several options where you can keep your evidence safely:

- Your desktop or laptop;
- An external hard drive or a USB stick;
- Email: create a new email account to be used as storage and then send the documents as attachment to that new email address. You can also send it to someone else you trust for safekeeping; and
- Cloud file hosting service such as Dropbox, Google Drive, One Drive, etc. which offers free usage for a limited memory size.

For safe measure, back up your documents by saving them in at least two different places; eg. one in your desktop and the other in an external hard drive in case one of the files is damaged or lost. It is also recommended for you to print out all the documents so you have a hard copy ready to be used at any time.

STEP #3: INFORM SOMEONE

Experiencing cyber-harassment can be traumatic and it is something you don't have to go through alone. You may think that it is not a big deal or are afraid that other people will judge you for making a big deal out of it. However, if it is affecting you in a negative way, it is a big deal. Help you monitor whether the harassment is getting worse and thus determine whether you will need to take any appropriate action.

Who can I inform?

i. Someone you trust

It may help to speak to someone you trust such as a friend, colleague, parent, teacher, counsellor, etc. whom you feel comfortable with. An empathetic ear or shoulder to lean on can provide you with some relief and comfort, even if only temporarily.

ii. Social media and Internet service providers

All popular social media service providers such as Facebook, Twitter, Instagram as well as search engines like Google, Microsoft Bing and Yahoo! have a reporting mechanism against abusive behaviour online. You can contact them to block the harasser or remove the abusive content targeted at you.

Click on the relevant social media and Internet service provider below to take you to the page where you can lodge a report against online abuse.

WhatsApp (Android)Whatsapp (IPhone)
https://faq.whatsapp.com/en/iphone/21197244/?category=5245250

Facebook
https://en-gb.facebook.com/help/contact/274459462613911

Twitter
https://support.twitter.com/articles/20169998

Instagram
https://help.instagram.com/372161259539444

Microsoft Search Engine – Removal of information
https://www.microsoft.com/en-my/concern/bing/

Google Search Engine – Removal of information
https://support.google.com/websearch/troubleshooter/3111061

Google+
https://support.google.com/plus/answer/6320425?hl=en

YouTube
https://www.youtube.com/intl/en-GB/yt/about/policies/#reporting-and-enforcement
Yahoo!https://help.yahoo.com/kb/SLN26401.html

iii. Non-governmental organisation (NGOs)

There are a handful of NGOs that are documenting cases of cyber-harassment in Malaysia. This exercise is important not only for statistical purpose, which is crucial towards understanding the severity of cyber-harassment in Malaysia, but also to obtain relevant real-life data needed to support any effort to address and lobby for this issue.

EMPOWER – documentation of online gender-based violence
http://empowermalaysia.org/contact-us/

Pusat KOMAS – documentation of online incidents of racism and racial discrimination.
http://reportracism.komas.org/

PeopleACT – documentation of cyber-harassment.
https://peopleact.mcchr.org/screenshot/

iv. Law enforcers

If the harassment becomes worse; i.e. you feel unsafe or in danger, you may want to consider reporting it to the relevant law enforcers such as the police, the Malaysian Commission on Multimedia and Communication (MCMC) or Cyber999 as soon as you can.

– Police
The police is responsible for taking complaints from the public on crime-related matters. If the harassment you face could potentially risk your security such as hacking, identity theft, blackmailing, sextortion, death threat, rape threat or stalking, you can lodge a police report at any police station closest to you.

You can also submit your complaint via your smartphone using the Volunteer Smartphone Patrol (VSP) application created by the police to enable the public to work with the police to combat crime.

Download this app here:
Android – Playstore
https://play.google.com/store/apps/details?id=my.gov.onegovappstore.rv2&hl=en

Apple/ IPhone – Appstore
https://itunes.apple.com/ao/app/volunteer-smartphone-patrol-vsp/id1118234031?mt=8

Note: Once you lodged a police report, the incident will be treated as a criminal matter. What this means is, the police is obliged to investigate the matter and when sufficient evidence is obtained to support that a crime has been committed by the alleged harasser, a criminal charge will be filed against them through the Public Prosecutor (PP)'s office.

A police report cannot be withdrawn. However, you may make a written application so that no action is taken against the report lodged, but the final decision is still left to the PP.

– MCMC
MCMC is a regulatory body created to look into all aspects of multimedia and communications in Malaysia. It has the power to receive and investigate complaints related to cyber-harassment. Click here for information on how to lodge a complaint. https://www.skmm.gov.my/make-a-complaint/make-a-complaint

– Cyber999
The Ministry of Science, Technology and Innovation (MOSTI) has created a help center called Cyber999 for the public to lodge complaint on incidents related to computer security. Click here for information on how to lodge a complaint.
https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/443/index.html

ADDITIONAL RESOURCES:
Removing online content
https://www.cybercivilrights.org/online-removal/

What should I tell the police?

When reporting to the police, you need to bring all the evidence you have documented in hard copy with you. It will make the process a lot easier if you are able to provide supporting document, particularly screenshots of the harassment containing any information that can help the police to identify the alleged harasser; eg. email address, username, IP address and phone number of the alleged harasser.

Below is a list of standard questions you are expected to tell the police. They may ask you more but you should be prepared to answer the questions below before going to the police station to ensure the reporting process goes as smoothly as possible.

- When did the harassment happen?
- Where did it happen?
- What happened?
- Do you know the harasser? If yes, who is it?
- What action have you taken so far?
- Do you have any witness? If yes, who are they?
- How has the harassment affected you?
- What action would you like the police to take?

You will be assisted by the police to write your report and then asked to verify the accuracy of the report. At this stage, make sure you read through the report thoroughly to ensure the information is correct. Seek for clarification if you are unsure of anything written on the report. If there is any mistake, you should inform the police to rectify the mistake. It is important to do this even if you feel nervous or uncomfortable as this can affect the investigation or the credibility of your report if you found out later that there were things on the report which you did not say to the police.

The police also have a responsibility to update you on the progress of their investigation. You have the right to ask them for an update regularly. Take down the name of the officer attending to you so you can speak to the officer directly to ease the follow-up process.

How do I get the police to cooperate?

There could be instances when a survivor turns up at the police station hoping that the police will take immediate action only to find that their complaint is not being taken seriously. There could be multiple reasons why some police may not take complaints of cyber-harassment seriously, but the three most common reasons that have been reported by real survivors are:

i. Some police may not know how to process the complaint as there is currently no specific law that deals with cyber-harassment, unless it involves a rape or death threat. Therefore, the police have no precedent or guidance on what law to use when handling the case;

ii. There is still a perception that the online space is unreal; i.e. users are not interacting with each other physically and therefore whatever harassment or threat that takes place online does not translate to physical harm; and

iii. Victim blaming – this happens when some police believe that the survivor is responsible for the harassment; e.g. posting politically inflammatory opinions or photos of the survivor dressed in sexy clothing on social media is expected to provoke hostile reactions from the public. Therefore, the survivor should have known better.

Here are five tips which may help you to get the police to cooperate. Remember, police are human beings and they too are subjected to everyday stress caused by work and their personal life. So the last thing they need is an aggressive and obnoxious person to turn up at the station to lodge a complaint without any evidence.

Tip #1: Start establishing rapport with the police by addressing the police officer attending to you respectfully; eg. refer to them as Tuan or Puan followed by their name which can be found on their name tag. Addressing them by their title and name can help to personalise the interaction and communicate to the police that you acknowledge them as an individual and not just part of a police force who is solely there to serve you.

Tip #2: Be very clear about the facts of your complaint. Being able to present your complaint coherently will save the police time and reduce their stress of trying to get information out of you.

Tip #3: Organise and prepare all documentation in hard copy to support your complaint. All evidence must be in its original language and form. For eg. if the harassing message is in Tamil and sent through Facebook, take a screenshot/photo/print screen of that message and print it out as it is. Do not translate or retype the message on a word document.

Bring them along with you to the station. Remember to keep a copy for yourself.

Tip #4: When speaking to the police, be polite and humble. Don't enter the station with the attitude that the police owe you and therefore they must entertain you at any cost.

Tip #5: Stay calm and try not to get angry and abusive when things do not go the way you expected it to. By being abusive, the police will not hesitate to retaliate by being hostile to you.

What do I do if the police say:

"You gave the photo to him. It's his property to do anything he wants with the photo."

Politely explain to the police that this may be incorrect especially if the photo is a selfie which means you have ownership of that photo. Besides that, let the police know that your modesty and reputation are at stake even if the photo does not belong to you. Try to get them to understand that just because you share a photo with someone privately does not give that person the permission to publicise it. Ask whether they would appreciate if an embarrassing picture of them is being shared on social media without their permission.

"This is not a crime. There is no law against this."

Politely explain to the police that this may be incorrect as there are existing laws such as the Penal Code, Communications and Multimedia Act 1998 and Computer Crimes Act 1997 that are applicable to offences such as criminal intimidation, illegal access to computer materials, outrage of modesty and posting of abusive content.

Also explain to the officer that the Royal Malaysia Police's position is that whatever laws that apply to offline misconduct will also apply to the same misconduct happening online. The Internet is only a medium or tool. The crime remains the same and will be dealt with by the appropriate laws. If they are unsure about this, they should check with their headquarters in Bukit Aman.

"He says it wasn't him."

With the documentation (websites, IPs, email service providers, etc.) you have done, inform the police that it should help them to investigate and prove the identity of the harasser.

"This online stuff is not real. You are not in actual physical danger."

Explain politely that it is possible for online harassment (especially threats and stalking) to transition from online to offline space when private information such as home or work address, car plate number, etc. has been shared publicly.

Also, the fact that the Internet has allowed people to stay anonymous can potentially magnify the danger you are facing. The anonymous person could be someone closer to you than you know.

"You shouldn't have expressed your opinion/dressed like that. Surely you know that it would cause you trouble. Why are you complaining about it when you know this is expected to happen?"

Politely explained to the police that while what you said or how you dressed may not appeal to everyone, it is not a crime. However, what the harasser did is a crime. Therefore, regardless of what you have done, it does not give an excuse to anyone to abuse you.

Note: If you encounter a police who still refuse to help you to report the harassment despite using the tips above, you should take down their name and badge number and submit a complaint to the police headquarters. https://www.rmp.gov.my/direktori/direktori-pdrm/bukit-aman

---

STEP #4: PROTECT YOUR ONLINE PRESENCE

Now that you have gone through STEP 1, 2 and 3, is there anything else you can do to secure your online presence? ABSOLUTELY. In fact, you should increase the security of your online presence if you have not already done so. Just by applying some basic security measures can help to prevent you from being harassed online.

There are many online safety guidelines that are easily available to you on the Internet. We have listed some below. We highly recommend you to click on the links found under additional resources to find out more.

Here are some basic do's and don'ts you should always practise to minimise the risk of cyber-harassment:

DO'S

- Make your e-mail password at least 15 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.
- Use encryption (e.g. Proton Mail) for person-to-person e-mail to prevent someone from impersonating you or reading your e-mail.
- 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.
- Set your privacy setting to allow only people you know to have access to your social media accounts.
- Watch for “red-flags“, for example someone you just met online 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.
- Websites collect all sorts of information about visitors (e.g. what Web browser you use, your IP address and potentially your e-mail address). Browse smartly and use tools that increase your browsing security, i.e. use VPN and install **Privacy Badger** in your browser.
- Think very carefully before sending intimate photos of yourself to someone else. You are still at risk even if you trust that person as your photo can still be accessed by someone else if the person’s phone or laptop is stolen or hacked.
- Install and update anti-virus, firewall and anti-spyware programmes on your computer to prevent virus attack, hacking and spying.
- Make sure 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 IT 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 or anywhere online, nor give it to strangers, including in chat rooms.
- Leave the geotagging function on your phone as this will give away your precise location when you snap a photo and post it online.
- 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.

ADDITIONAL RESOURCES:

Security in a Box – Digital Security Tools and Tactics
https://securityinabox.org/en/

The Staying Safe Online Guide
https://cdn.lb.my/sites/9/20171227144346/The_Staying_Safe_Online_Guide.01.01.pdf
Klik Dengan Bijak
http://www.klikdenganbijak.my/Utama.aspx

WhatsApp
https://faq.whatsapp.com/en/android/21197244/?category=5245250

Who's Spying on Your Computer: Spyware, Surveillance and Safety for Survivors
https://cdn.lb.my/sites/9/20171227144347/Who-is-spying-on-your-computer.pdf

What to Do When You've Been Threatened Online
https://www.lifewire.com/what-to-do-if-youve-been-threatened-online-2487763

STEP #5: SELF-CARE

After going through STEP 1 to 4, you may still find yourself feeling vulnerable and in need of further support. Some survivors reported that they continued to live in fear because of the online threats they received and as a result suffered from deep depression and emotional trauma. During this time, it is important that you care for yourself. Caring for yourself means taking care of your physical, mental and emotional health to start your healing process. This healing process is critical to get you back to the life you once enjoyed.

One of the ways of self-care is to take some time to disconnect from social media or other online platform that has caused you harm. Opting out from that space can help you to step away from a toxic environment to help you breathe again.

There are various methods of self-care you can find online. Please click on the link under additional resource for more information.

Sometimes when it becomes too difficult to bear, it is advisable for you to seek counselling, either from someone you trust or organisations such as the Befrienders or AWAM.

The Befrienders, KL
Address: Befrienders Center,
No.95 Jalan Templer,46000 Petaling Jaya.
Face to face: Call the phone number below to make
an appointment. Phone Calls (open 24 hours/day):
03-79568144 or 03-79568145
E-mail: **sam@befrienders.org.my**

All Women's Action Society (AWAM)
Address: 85, Jalan 21/1, Sea Park,
46300 Petaling Jaya, Selangor, Malaysia
Opening hours: 10am to 4:30pm,
Monday to Friday. Saturday is by appointment only.
Phone (office): +60 3-7877 4221
TELENITA Helpline: +60 3-7877 0221

ADDITIONAL RESOURCES:

Self-care: Coping and Healing
https://www.takebackthetech.net/be-safe/self-care-coping-and-healing

END NOTE TO SURVIVORS

This kit serves only as a guideline to assist you on what to do and where to seek help. It does not promise you a solution. There is a wealth of other resources on how to cope with cyber-harassment that can be accessed on the Internet easily.

PeopleACT tries its best to identify the most suitable resources to be used for this kit and then localised it to serve Malaysians, or those living in Malaysia.

PeopleACT also tries to ensure that all information provided here is as accurate as possible. Some information may be subjected to change and when this happens, PeopleACT will try its best to update the information in a timely a manner.

You are still strongly encouraged to explore other information which may provide you with better support, although we truly hope that this kit will provide the basic information you need to help you survive cyber-harassment.

Finally, you do not have to follow the steps in the recommended sequence; i.e. Step 1, 2, 3, 4 and 5. Always trust your own instinct and act according to how you feel. For example, if you think Step 4 is the most urgent, then do it. Every individual is unique and it is you who can decide what is best for you.

Stay strong and know that you are not alone.

CONTACT

Address:
The Malaysian Centre for Constitutionalism and Human Rights
A-3A-8, Pantai Business Park, Jalan Pantai Baharu, 59200 Kuala Lumpur, Malaysia
(Office opening hours: Monday – Friday, 9:30am – 5:30pm)
Telephone: +60 3-2201 1454
Email: **peopleact@mcchr.org**

GLOSSARY

Flaming war

When two or more people attack each other by hurling insults, name-calling or using other forms of verbal abuse. This is usually a result of a heated difference of opinion on a hot topic like politics, religion, feminism, etc.

Sexism

1. Prejudice or discrimination based on sex; especially against women.
2. Behaviour, conditions, or attitudes that foster stereotypes of social roles based on sex.

Feminist voices

Expressions of thoughts or opinions that advocate women's rights on the ground of the equality of the sexes.

Extortion

The practice of obtaining something, especially money, through force or threats.
(Source: Oxford dictionary)

Community standard

Acceptable norms or conduct enforced by a just and open community.

Non-consensual pornography

Popularly known as "revenge porn" whereby a sexually explicit photo of a person is being shared without that person's consent as a revenge. Since revenge is not always the motive for sharing such photo, the right term to use is non-consensual pornography.

Internet Protocol (IP) address

An IP address provides an identity to a networked device. Similar to a home or business address supplying that specific physical location with an identifiable address, devices on a network are differentiated from one another through IP addresses.

Most IP addresses look like this: 151.101.65.121
(Source: www.lifewire.com)

Online gender-based violence

Any act of online violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women. Examples of online violence are sexual harassment, stalking, rape and death threat, sextortion, non-consensual pornography, hateful or abusive comments, and other forms of threat or intimidation that impede on a woman's freedom. Such violence is usually the result of power inequalities that are based on gender roles.

Around the world, gender-based violence almost always has a greater negative impact on women and girls. For this reason, it is often used interchangeably with violence against women.
(Source: UN Declaration on the Elimination of Violence against Women)

Sextortion

The practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them.
(Source: Cambridge dictionary)

Public Prosecutor (PP)

The principle legal advisor of the government of Malaysia.

Victim blaming

When a victim of a crime or other wrongful act is held fully or partially responsible for the harm they are suffering from. For example, a rape victim is told that they would not have been raped if they had not allowed the rapist to enter their hotel room.

Red-flags

A warning signal.
(Source: Merriam-Webster dictionary)

VPN

stands for Virtual Private Network. It is essentially, a private network that uses a public network to connect remote sites or users, while encrypting all of a device's internet traffic in the process, routing it through a middle-man server in a remote location, granting access to otherwise inaccessible network resources.
(Source: www.wired.co.uk)

Geotagging

The act of "tagging" a geographical location to something like a status update, a tweet, a photo or something else you post online. It's particularly useful because a lot of people now share content on their favourite social networks via their smartphones or tablet computers while on the go, so they're not always in one specific location all the time like we used to be back in the day when we could only access the web from a desktop computer.
(Source: www.lifewire.com)