



Funded by the Government of Ontario



# Addressing Cyber Crime- Building Safer & Inclusive Online Communities Project

## Malton Women Council

Email: [info@mwc.community](mailto:info@mwc.community)

Website: [www.mwc.community](http://www.mwc.community)

Phone: +1 647-391-9668

# Table Of Content

<b>CYBER/ONLINE FRAUD AWARENESS AND PREVENTION</b>	<b>Page 3</b>
<b>CYBER/ONLINE HATE CRIME AWARENESS AND PREVENTION</b>	<b>Page 12</b>
<b>CYBERBULLYING AWARENESS AND PREVENTION</b>	<b>Page 18</b>
<b>UNDERSTANDING AND ADDRESSING ISLAMOPHOBIA</b>	<b>Page 24</b>
<b>WHAT IS COUNTER-SPEECH?</b>	<b>Page 30</b>

**TIP SHEET –  
CYBER/ONLINE FRAUD  
AWARENESS AND  
PREVENTION**

# WHAT IS CYBER/ONLINE FRAUD?

Cyber/online fraud is a blanket term to describe crimes committed by cyber attackers via the internet. These crimes are committed with the intent to illegally acquire and leverage an individual's or business's sensitive information for monetary gain.



# TYPES OF CYBER/ONLINE FRAUDS

## Identity fraud:

Identity fraud happens when criminals use stolen personal information. It is often used to commit another crime. Criminals can use your stolen or reproduced information to:

- access your computer/email.
- access your bank accounts.
- open new bank accounts.
- transfer bank balances.
- apply for loans and credit cards.
- buy goods and services.
- hide their criminal activities.
- get passports or receive government benefits.



## Actions you can take to protect yourself from identity fraud:

- be aware of unsolicited e-mails, text messages, telephone calls, or mails asking you for personal or financial information.
- check your credit reports, and bank and credit card statements and report any irregularities.
- shred personal and financial documents before putting them in the garbage.
- retrieve your mail regularly to limit possible mail theft.
- when you move, notify the post office and your relevant financial institutions and service providers.

## Foreign money offers or inheritance scams or fake business proposals:

- Scam medium: email and text, mail, phone, and fax
- A scammer contacts you asking for help to transfer a large sum of money from one country to another. The requests often appear to come from a lawyer or legal entity.
- These requests can include fake inheritance letters, fake business proposals, or requests for help with illegal activity (e.g., smuggling gold out of Iraq).
- They advise you that you need to pay one or more fees before the money can be released. However, money doesn't exist, and you never receive anything.

These scams are sometimes referred to as Nigerian, 419, or West African.



## Air duct cleaning fraud:

A scammer offers services that include air duct cleaning or furnace/boiler repairs at very low rates. If the company completes the services, they are of low quality; the warranties are invalid; or the repairs can cause potential risks.

#smallbusinesschallenge 🏆

Duct cleaning is sooooo necessary. What are you breathing? 🤔🌬️❄️

Please contact me for more information  
515-448-7759

Air Duct Cleaning March first week 50% Off Special Promotion.  
We are charging a flat price for the whole house Duct Cleaning  
I guarantee all my work  
First 5 COMMENTERS will get special DISCOUNT

Our service package includes the following:

- ✓ Unlimited Vents Cleaning
- ✓ Before after pictures.
- ✓ Camera inspection.
- ✓ Ac unit checkup.

You must consider duct cleaning if you have

- Residents with allergies and asthma
- Smoker in the household
- Hair and dander from pet
- Done duct cleaning more than a year ago

NOTE 1 : Do not worry about moving your furniture as we are using latest modified equipment like whip snap which can go inside each and every vent easily

NOTE 2 : No kind of upfront charges before the service all you have to pay after you are fully satisfied

## Cellphone service provider fraud:

- A fraudster calls and claims to be from a cellphone service provider. They offer a deal that's too good to be true. The fraudsters proceed to ask for the victim's personal information including their Social Insurance Number (SIN) and Driver's License number. They will then use your personal information for identity fraud or order a cellphone using your identity or order a cellphone and have it shipped to the victim but then tell you it was the wrong cellphone, and you need to ship it back to the criminal's address.
- If you get a call from your service provider, tell them that you will call them back and end the call. Look up the legitimate phone number for the company and communicate with them directly by always making the outgoing call.

## Low-interest rate offers fraud:

A scammer offers reduced interest rates on credit cards or lines of credit. They request personal information from you, such as your Social Insurance Number (SIN), mother's maiden name, date of birth, or credit card information. In most instances, scammers request a one-time fee for the service. The scammers do not have the ability to lower interest rates. They're stealing your personal information and/or your money.

## AVOID FAKE LOAN WEBSITES/APP FRAUDS





### ***Immigration website fraud:***

Scammers create fake websites and online ads that offer "cheap" immigration services or even may "guarantee" high-paying jobs. Many of the websites will look like official government sites. Beware if they are asking you to pay for application access fees or deposits before the application is even started.

## IMMIGRATION FRAUD



## HOW TO REPORT CYBER/ONLINE FRAUD?

- If you have been a victim of a scam, fraud, or cybercrime, please contact your local police as soon as possible.
- It is also recommended that you report the instance of a scam, fraud, or cybercrime, whether you are a victim or not, to the Canadian Anti-Fraud Centre (CAFC).
  - 1-888-495-8501
  - <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>

## TIPS TO PREVENT CYBER/ONLINE FRAUD:

- Keep software and devices updated to ensure your systems have the most up-to-date security enhancements.
- Make sure all your devices are equipped with antivirus and malware protection software.
- Use different and unique passwords for all your accounts.
- Don't make them the same and avoid using predictable passwords such as birthdates or names.
- Enable two-factor authentication to your passwords to add an extra layer of protection.
- Back up your data on the cloud or external drive.

## RESOURCES AND REFERENCES:

- Canadian Anti-Fraud Centre: <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>
- Get Cyber Safe: <https://www.getcybersafe.gc.ca/en>
- Peel Regional Police Cyber Safety Tips and Resources: <https://www.peelpolice.ca/en/safety-tips/cyber-crime-computer-and-internet-safety.aspx>
- RCMP seniors guidebook for safety and security: <https://www.peelpolice.ca/en/safety-tips/cyber-crime-computer-and-internet-safety.aspx>



**TIP SHEET –  
CYBER/ONLINE HATE  
CRIME AWARENESS  
AND PREVENTION**

# HOW IS HATE CRIME DEFINED IN CANADA?

Hate crimes refer to criminal incidents that are found to have been motivated by hatred toward an identifiable group. According to s318(4) of the *Criminal Code of Canada*, such groups are distinguishable by race, national or ethnic origin, language, color, religion, sex, age, mental or physical disability, sexual orientation, gender identity or expression, or on any other similar factor. In other words, *any criminal activity* has the potential to be a hate crime if the hate motivation can be proven.



# WHAT IS CYBER/ONLINE HATE?

- Cyber/Online Hate is posting and sharing hateful and prejudiced content against an individual, group, or community. It can take the form of derogatory, demonizing, and dehumanizing statements, threats, identity-based insults, pejorative terms, and slurs.
- If a post is hostile towards a person's race, religion, disability, sexual orientation, or gender identity, it could be viewed as Hate Speech. If it is serious enough, it may break the law, whether it is online or offline.
- Cyber/Online Hate can be expressed through many types of media, including text, images, videos, and audio. These different types of media content are sometimes combined.
- Cyber/Online Hate can include malicious communications (sending letters, emails, and messages that cause distress and anxiety), cyberbullying, cyberstalking, harassment, stirring up hatred through content (text, image, video, audio), and incitement to commit violence.



# HOW TO REPORT AN ONLINE HATE INCIDENT?

- It is vitally important that we don't let online hate speech go unanswered.
- Because online content is fluid, it is always good to be as specific as possible.
- When reporting an incident, include as much of the following as you can:
  - When did this happen? Noting the time and date is important because some online content, such as discussion threads in chatrooms, can quickly disappear.
  - How was the content delivered?
  - Were you sent something directly through email, SMS, text message, instant message, or private messaging?
  - Did you come across something while browsing the Web?
- If the message was sent directly to you: - keep the original email or save your chat/text log, should you need to give them to law enforcement officials. - if possible, save the username or email address of the person sending you the hateful message.
- If you encountered the content on a website: - copy and paste the address of the site by clicking your Web browser's address bar, highlighting the full Web address, and copying and then pasting it into a word processor. - take a screenshot of the content in question to give to the police. (On Windows computers, hit the "Print Screen" key, then go to a graphic or word processing program and select "Paste" from the "Edit" menu; on a Mac, hitting Command-Shift-3 will save the current screen image as a graphic file on your desktop.)

The following are places you can report online hate to:

- **Site Administrators:** Sites and services which allow people to post content, such as Facebook, YouTube, and Xbox Live, have policies about what is acceptable. You can generally complain about content on these sites through a "Contact Us" link somewhere on the home page. Some sites also have tools that have been designed specifically for this purpose:
  - Facebook allows people to report different types of offensive content. For more information see <https://www.facebook.com/help/?page=247013378662696>

- YouTube allows visitors to “flag” offensive videos (you need to have a YouTube account to do this). For more information see <http://support.google.com/youtube/bin/answer.py?hl=en&answer=95403>
  - Xbox Live users can file complaints about all forms of harassment. For more information see [http://forums.xbox.com/xbox\\_forums/xbox\\_support/f/26/t/19139.aspx](http://forums.xbox.com/xbox_forums/xbox_support/f/26/t/19139.aspx).
  - World of Warcraft has a policy that forbids harassment based on race, ethnicity, national origin, or sexual orientation. It can be seen at <http://us.battle.net/support/en/article/previous/20455>. To complain about harassment, you must contact a Game Master and “Open a Ticket.” For more information see <http://us.battle.net/support/en/article/previous/19775>.
- **Internet Service Providers (ISPs):** Many ISPs will remove hate content that is hosted on their servers once they are made aware of it. To find out the host of a particular site, visit [www.uwhois.com](http://www.uwhois.com) or [www.easywhois.com](http://www.easywhois.com).
  - **Canadian Human Rights Tribunal:** You can bring a complaint about online hate to the Canadian Human Rights Tribunal by contacting the Canadian Human Rights Commission. Canadian Human Rights Commission 344 Slater Street, 8th Floor, Ottawa, Ontario K1A 1E1, Canada Telephone: (613) 995-1151 Toll-Free: 1-888-214-1090 TTY: 1-888-643-3304 Fax: (613) 996-9661 The Commission can also be contacted online at the following address:  
[www.chrc-ccdp.ca/contact/default-eng.aspx](http://www.chrc-ccdp.ca/contact/default-eng.aspx)
  - **Non-Governmental Organizations:** There are also non-governmental organizations that collect reports of both offline and online hate. They include:
    - B’nai Brith Canada ([www.bnaibrith.ca/contactus.html](http://www.bnaibrith.ca/contactus.html))
    - Friends of the Simon Wiesenthal Center ([www.wiesenthal.com/site/pp.asp?c=lsKWLbPJLnF&b=4441269](http://www.wiesenthal.com/site/pp.asp?c=lsKWLbPJLnF&b=4441269))
    - Canadian Anti-racism Education and Research Society ([www.stopracism.ca/reportfrm.php](http://www.stopracism.ca/reportfrm.php))



- **Law Enforcement:** Many police forces have special hate crime units to deal with hate incidents. If you live in Ontario or British Columbia, you also have access to a provincial hate crimes unit:
    - Ontario Hate Crime Extremism Investigative Team ([www.hceit.ca](http://www.hceit.ca))
- B.C. Hate Crime Team (604-543-4903 or 604-598-4243)

## RESOURCES AND REFERENCES:

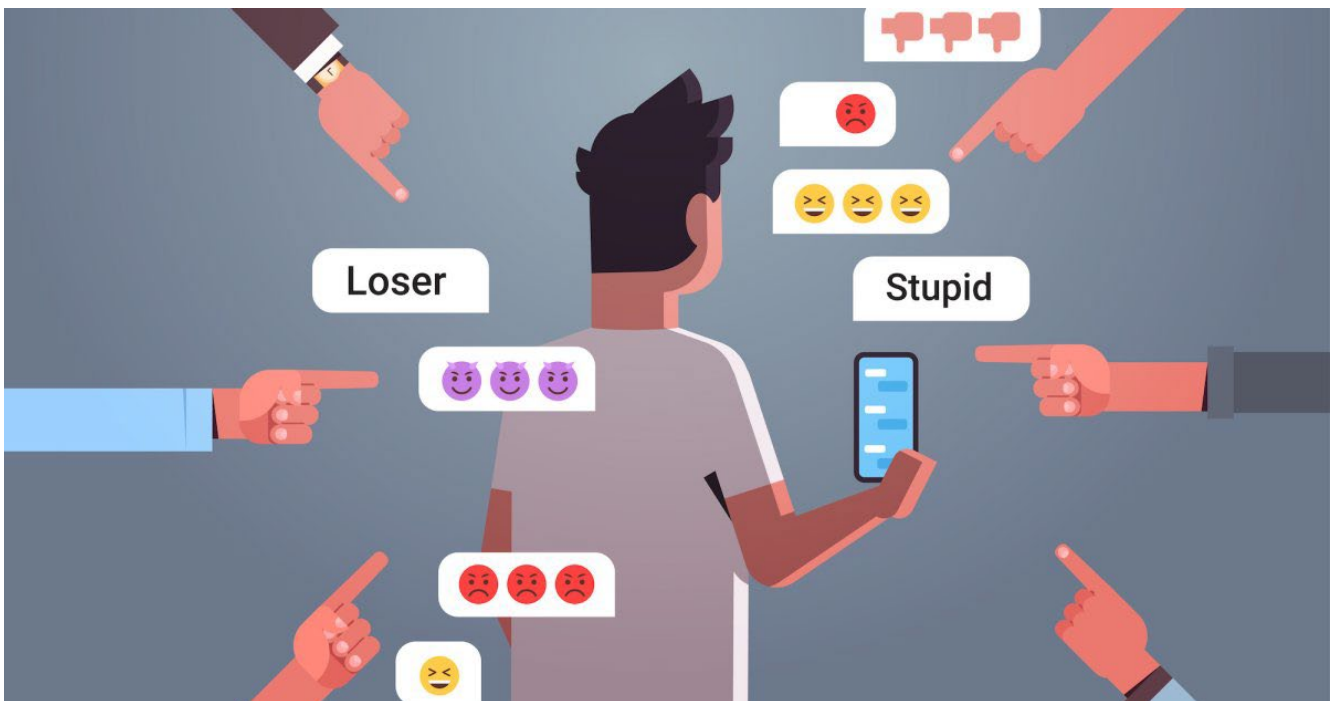
- Canadian Race Relations Foundation: <https://www.crrf-fcrr.ca/en/news-a-events/articles/item/26823-hate-crime-in-canada>
- Stop Hate UK: <https://www.stophateuk.org/about-hate-crime/what-is-online-hate-crime/>
- Media Smarts: <https://mediasmarts.ca/teacher-resources/responding-online-hate-guide>
- Ontario Hate Crime Extremism Investigative Team: [www.hceit.ca](http://www.hceit.ca)
- Canadian Human Rights Tribunal: [www.chrc-ccdp.ca/contact/default-eng.aspx](http://www.chrc-ccdp.ca/contact/default-eng.aspx)
- Canadian Centre for Cyber Security: <https://cyber.gc.ca/en>



**TIP SHEET –  
CYBERBULLYING  
AWARENESS AND  
PREVENTION**

# WHAT IS CYBERBULLYING?

- The activity of sending messages through social media, emails, and text messages to frighten or upset somebody.
- Sending, posting, or sharing negative, harmful, false, or mean content about someone else.
- It can include sharing personal or private information and causing embarrassment or humiliation.



## WHERE CAN IT HAPPEN?

- Social Media Apps: TikTok, Twitter, Snapchat, Instagram, Reddit, Facebook, etc.
- Messaging Apps: WhatsApp, iMessage, etc.



## TYPES OF CYBERBULLYING:

- **Harassment:** repeatedly sending messages with an offensive meaning.
- **Flaming:** insulting someone in an online discussion using foul language.
- **Outing:** revealing someone's private thoughts, secrets, or personal information.
- **Degradation:** spreading lies and rumors using digital tools.
- **Impersonation:** pretending to be someone for entertainment or to commit fraud.
- **Cyber Stalking:** using digital tools to harass and monitor someone's movements online.

## Effects of Cyberbullying:

Emotional Effects	Mental Effects	Behavioral Effects	Physical effects
<ul style="list-style-type: none"> <li>• Humiliation</li> <li>• Isolation</li> <li>• Powerlessness</li> <li>• Anger</li> </ul>	<ul style="list-style-type: none"> <li>• Depression and Anxiety</li> <li>• Low self-esteem</li> <li>• Academic Issues</li> <li>• Suicidal thoughts and self-harm</li> </ul>	<ul style="list-style-type: none"> <li>• Using alcohol or drugs</li> <li>• Skipping school</li> <li>• Poor relationships</li> </ul>	<ul style="list-style-type: none"> <li>• Gastrointestinal issues</li> <li>• Eating disorders</li> <li>• Sleep disturbances</li> </ul>



## STEPS TO TAKE IF YOU ARE CYBERBULLIED:

- **STOP:** Do not respond to the behavior.
- **SAVE:** Don't delete the message. It's important to keep a record of what's happening.
- **BLOCK:** Block the sender's phone number or email address. If you don't know how to contact your cellphone company and/or Internet service provider.
- **TELL:** It's important you tell someone you trust about what's happening. You should:
  - Report to your local police station.
  - Report to social media sites or apps.
  - Notify school administrators or teachers.
  - Tell a trusted adult.

## TIPS TO PROTECT YOURSELF FROM CYBERBULLYING:

- Keep your passwords private, even from your friends.
- Don't share personal information with strangers including your name, the names of friends or family, your address, phone number, and your school.
- Be careful about whom you share your photos with online.
- Remove tags on photos that make you feel uncomfortable.
- Secure your profile information by making sure only friends can see it.
- Think before you post anything online. It may become public.
- Be very careful whom you trust online because once you share information online, you cannot control who sees them or how they are used.
- Trust your gut. Don't answer requests or open messages from strangers.
- Search your name in search engines frequently, including in an image search. If any personal information, images, or videos come up that might be used by cyberbullies, visit [NeedHelpNow.ca](http://NeedHelpNow.ca) to get help having it removed.

## RESOURCES AND REFERENCES:

- <https://kidshelpphone.ca/>: Free, 24/7 confidential counseling, information and referrals, and support service for young people. Text: 686868; Call: 1-800-668-6868
- <https://www.cybertip.ca/en/>: Canada's tip line for reporting the online sexual exploitation of children.
- <https://needhelpnow.ca/app/en/>: Helps teens stop the spread of sexual pictures or videos and provides support to youth.
- <https://www.prevnet.ca/bullying/cyber-bullying/>: Provides online resources for youth and parents to prevent and or deal with cyberbullying.
- <https://getcybersafe.gc.ca/en/>: A national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.
- <https://cssn.me/about/>: The Canadian Safe School Network is a national, not-for-profit, registered charitable organization with a mandate to reduce youth violence and make our schools and communities safer.
- <https://www.ccohs.ca/oshanswers/psychosocial/cyberbullying.html>: Internet harassment tip sheet from Canadian Centre for Occupational Health and Safety
- <https://www.peelpolice.ca/en/safety-tips/child-and-teen-safety.aspx#Bullying-Resources>: Cyberbullying tip sheet from Peel Regional Police.



**TIP SHEET –  
UNDERSTANDING AND  
ADDRESSING  
ISLAMOPHOBIA**



## ISLAMOPHOBIA:

- Islamophobia is an extreme fear of and hostility toward Islam and Muslims which often leads to hate speech, hate crimes, as well as social and political discrimination.
- The Ontario Human Rights Commission defines Islamophobia as “stereotypes, bias or acts of hostility towards individual Muslims or followers of Islam in general.”
- Some of the sources of Islamophobia include fear of the influence of Islam on Canadian society as the result of immigration, the perception of a regression in women’s rights, and the perception of religious values that incite violence.



## GENDERED ISLAMOPHOBIA:

- Prejudice against Muslim women which comes from specific stereotypes that were historically contextualized—that veiled Muslim women are oppressed.
- According to data from Statistics Canada, from 2010 to 2019, in 47 percent of the violent hate crimes committed against Muslims and reported to the authorities, the targets were women.



## SYSTEMIC ISLAMOPHOBIA:

A system of Islamophobia created through the existence of laws, policies, practices, and actions that may appear neutral but have an adverse effect on Muslims or those who are perceived to be Muslim. An example of this in the Canadian context is Bill 21 in Quebec, a law that prohibits the wearing of religious symbols such as the hijab in public sector jobs, including teaching. In the education system, this can exist through policies prohibiting headwear, limited options for athletic uniforms, and the absence of halal food options.

## Understanding Intersectional Identities:

Ways in which systems of inequality based on gender, race, ethnicity, sexual orientation, gender identity, disability, class, and other forms of discrimination “intersect” to create unique dynamics and effects. For example, when a Muslim woman wearing the Hijab is being discriminated against, it would be impossible to dissociate her female from her Muslim identity and to isolate the dimension(s) causing her discrimination.

## ISLAMOPHOBIA IN CANADA:

Islamophobia has been at the root of increased targeted hate attacks killing Muslims in Canada compared to any other G-7 country. Statistics Canada’s most recent report on hate crimes notes that in 2021, there was a 71 percent increase in police-related hate crimes being perpetrated against Muslims in Canada.

## HOW TO COLLECTIVELY ACT AGAINST ISLAMOPHOBIA?

- Learn about structural Islamophobia, such as Islamophobic legislation, unfair treatment in the legal system, media bias, anti-Muslim political rhetoric, and resistance to refugee resettlement and private Islamophobia including hate group activities, mosque opposition, mosque vandalism, harassment, and violence.
- Educate yourself and others about Islam and Muslims using authentic sources and learn about the anti-shariah movement, ideologically motivated violence, facts about immigration and crime, media double standards, the Islamophobia industry, and challenges to mosques.
- Speak up against injustice, biased media coverage, unfair legislation, hate speech, mosque vandalism, harassment, and in favor of minorities, immigrants, refugees, and civil and human rights.

- Organize by mobilizing neighbors and communities, collaborating across civic groups, cultivating interfaith allies, and holding public displays of solidarity.
- Center the voices of Muslims – men and women – and give them space to speak for themselves.
- Do your research and do not ask marginalized communities to shoulder the burden of educating others.
- Avoid common mistakes made by interfaith allies.
- Study success stories of collaborative efforts to fight Islamophobia.



## RESOURCES AND REFERENCES:

- Islamophobia Is: <https://islamophobia-is.com/>
- International Civil Liberties Monitoring Group: <https://iclmg.ca/resources-against-islamophobia>
- National Council of Canadian Muslims: <https://www.nccm.ca/community-resources>
- The Digital Anti-Racism Education Project: <https://www.daretobeaware.ca/about>
- Council of Agencies Serving South Asians: <http://cassa.on.ca/eradicatehate/>
- NSCC Libraries: <https://subjectguides.nsc.ca/anti-racism/anti-islamophobia>
- Muslim Educators Ontario: <https://www.muslimeducatorsontario.org/resources>
- Peel District School Board's Anti-Islamophobia Strategy:  
[https://www.peelschools.org/documents/4d852330-cc5d-41ef-bcd4-1787e4231b24/14.1d\\_Directive%2014%20Affirming%20Muslim%20Identities%20and%20Dismantling%20Islamophobia%20StrategyReport.v3.pdf](https://www.peelschools.org/documents/4d852330-cc5d-41ef-bcd4-1787e4231b24/14.1d_Directive%2014%20Affirming%20Muslim%20Identities%20and%20Dismantling%20Islamophobia%20StrategyReport.v3.pdf)



# **TIP SHEET – WHAT IS COUNTER-SPEECH?**

# COUNTER-SPEECH:

## WHAT IS COUNTER-SPEECH?

- Counter-speech is any direct response to hateful or harmful speech that seeks to undermine it.
- Counterspeech has been proposed as a more effective approach to challenging online hate. Instead of blocking or removing content, counter-speech directly presents an alternative, polite, and non-aggressive response to whatever has been posted.
- Counterspeech can take the form of text, graphics, or video, and it offers several benefits over content moderation, such as protecting free speech, supporting victims, and signalling to other social media users that hate is unacceptable.



# WHY IS COUNTER-SPEECH IMPORTANT?

- Counter-speech is a humane, empathetic expression. The purpose of counter-speech is to show that every person is valuable.
- Counter-speech tries to appeal to the larger audience and to reclaim the discussion space with positive speech. It demonstrates that there is strength in numbers.
- Counter-speech does not try to create more opposition, but to find solutions and to show that a bigger group is standing behind the target of hate speech.
- Counter-speech tries to avoid providing a direct answer to hate speech.

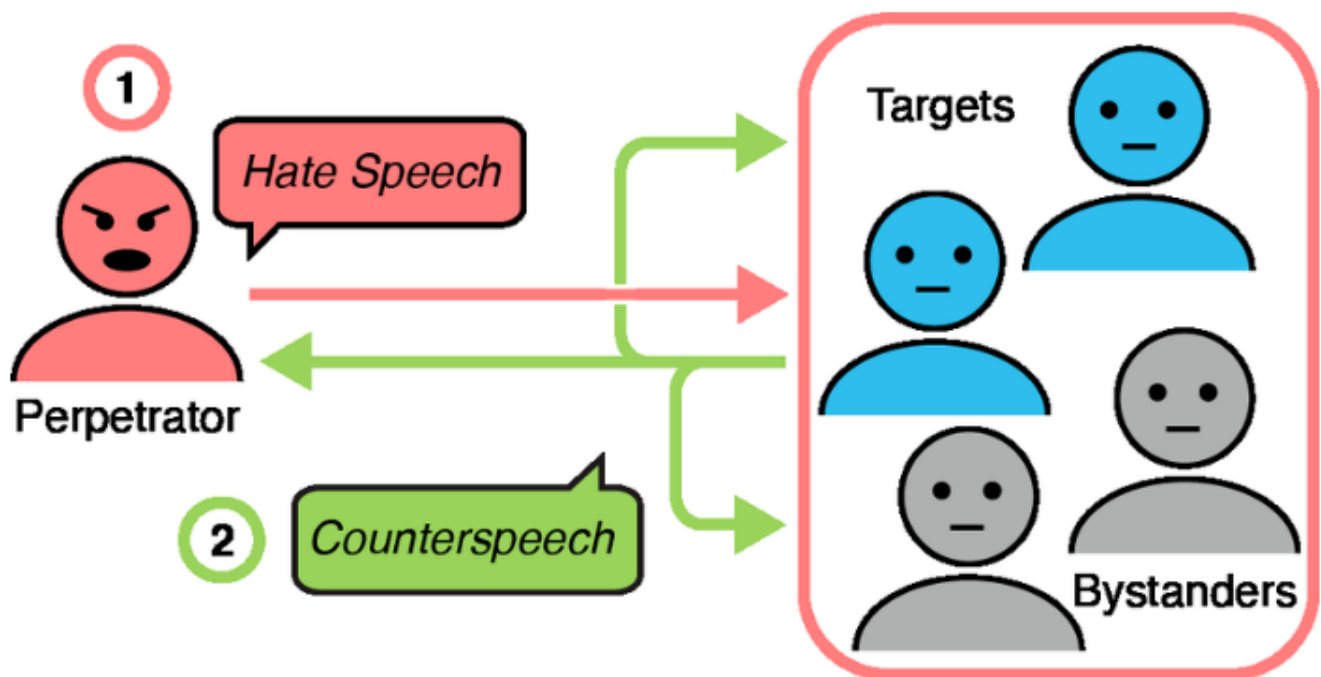


# HOW TO USE COUNTER-SPEECH?

- Be brave. Engage. Say out your thoughts. Make the audience interested!
- Try to be empowering and inspiring. Not condescending or critical of the topic.
- Come up with a message that could effect change. Simple words instead of complex vocabulary.
- Leave room for the viewer's or listener's own interpretation and thinking.
- Summarize your message in a few sentences, this makes for a powerful message.
- Do not produce hate speech yourself - counter-speech is about finding a solution.



- Do not victimize others or portray yourself as a victim. Remember to empower the target group and to demonstrate a better solution!
- Do not preach or provide a final answer to the problem. Remember: Change happens one step at a time.
- Understand what online hate is.
- Use Human rights to educate yourself and others about online hate.
- Know the difference between online hate and cyberbullying.
- Recognize conflict in conversations.
- Engage in empathic and peace-building conversations online.
- Be clear on what we are calling hate speech.
- Be transparent.
- Consider approaches beyond fining the companies.
- Take a go-slow approach.
- Avoid policies that can be twisted to censor free speech.



## RESOURCES AND REFERENCES:

<https://www.mll.fi/en/about-mll/media-education/safely-in-digital-environments/hate-speech-and-counter-speech/>

<https://mediasmarts.ca/online-hate/resources-teachers-online-hate>

<https://dangerousspeech.org/counterspeech/>



*MALTON WOMEN COUNCIL*

# CONTACT INFORMATION



+1 647-391-9668



[www.mwc.community](http://www.mwc.community)



[info@mwc.community](mailto:info@mwc.community)