



# Human Rights in the Digital Age



 Pre-Assessment

 Introduction

 What are digital rights?

 How do I protect my digital rights?

 How do I protect myself from and respond to cyberbullying?

 Wrap up

 Post-Assessment

## QUESTION BANKS

 Human Rights in the Digital Age Pre/Post-Assessment\_EN

# Pre-Assessment

---

**Before you take this new module in Digital University, let's pause and reflect on what you know already about this topic through a short pre-test. The questions in this pretest will all be covered in the module, so it's OK if you don't know all the answers just yet!**

---

*Question*

**01/01**

---

7 questions drawn randomly from Human Rights in the Digital Age Pre/Post-Assessment\_EN

# Introduction

---

**Our lives and our advocacy work increasingly depend on the use of technology, including social media, and technology can be a valuable tool to enhance our advocacy work. But technology can also make us and others vulnerable to privacy breaches, discrimination, and bullying. In addition, the lack of equal access to digital technology prevents many people from realizing equal rights.**

“Digital” refers to the use of electronic devices that store and process data, such as mobile phones and computers, as well as software and applications (apps) used on these devices, such as email and social media. In the digital world, you are entitled to the same rights as you are in the offline or physical world, but few people know how to recognize and protect these rights.

This module will empower you to protect yourself and others and show you how to leverage your digital rights for greater impact.

**By the end of this module, you will be able to:**

1

Describe what digital rights are.

2

Understand how to protect your and others' digital rights.

3

Take actions to guard yourself against cyberbullying, and know how to respond when others are being cyberbullied.

**LET'S GET STARTED!**

# What are digital rights?

---

---

**Understanding your digital rights is the first step to taking control of your online presence. Even if your technology use is limited, in the age of the internet, digital rights are a critical component of human rights.**

## What are digital rights?

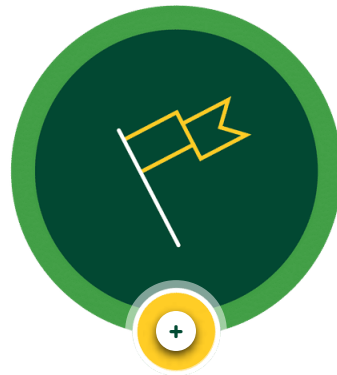
The [UN Human Rights Council](#) affirms that all human rights you have in the physical world (offline) apply to your digital self when you navigate the internet, engage on social media, and use technology such as your phone/smartphone. Digital rights include your right to privacy, freedom of expression, and the right to live free from violence and harassment.



**What does this look like on the international and national level? Select each one to learn more.**



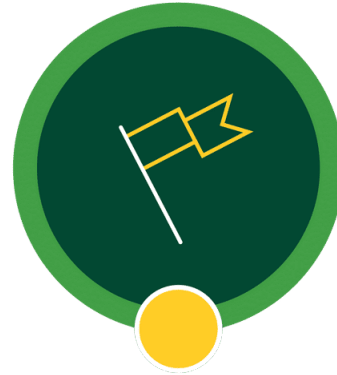
**International**



**National**



**International**



**National**

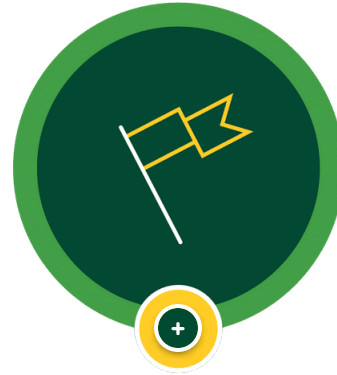
## **International**

Many of the international human rights frameworks that we as advocates rely on—such as the [Convention on the Rights of the Child \(CRC\)](#) or the [Convention on the Elimination of All Forms of Discrimination Against Women \(CEDAW\)](#)—were created before the invention of the internet and widespread digital technologies. While there have been some amendments to these conventions during the digital age, an international framework on digital rights is still lacking.





**International**



**National**

## **National**

At the national (country) level, laws that regulate the internet are mostly focused on transactional, financial, and e-commerce activities, rather than protecting and ensuring the digital rights of its citizens. A few countries do have laws that address online harassment, but these are quite limited and may not address all forms of harassment and cyberbullying that people, especially people of underrepresented populations, may face.

## **Why do digital rights matter?**

Even before the COVID-19 pandemic, much of our lives were conducted online. We communicate with friends and family, access information, and connect with important resources and services—all online. Now, as a result of the COVID-19 pandemic, we are even more dependent on digital technology.



**Let's take a look at these statistics. Select each one to learn more.**

**4.57 billion**

Active internet users as  
of April 2020.

**59%**

The percentage of the world's population with access to the internet. Nine out of 10 of the countries with the lowest internet access are in Africa.

**98%**

Women/girls surveyed in 22 countries who use social media, with the most used platforms being Instagram, Facebook, and WhatsApp.

**Source: Plan International**

Given how much of our lives are intertwined with these technologies, it's important to understand who is running the platforms and systems that dictate so much of our lives. Those in control of the online spaces we frequent are generally private sector companies that are motivated by profit, such

as Meta, Google, Alibaba, TenCent, or Apple. Regulations to ensure these companies protect our rights vary across the world and are usually not robust.



There are many ways our rights can be violated online, including cyberbullying, data mining, and surveillance. You have likely experienced some of these violations yourself. As with human rights, people around the world do not equally enjoy their digital rights. People who face discrimination in the physical world, such as Black, Indigenous, and People of Color (BIPOC); LGBTQIA+ people; and other traditionally excluded populations, also often experience further discrimination and marginalization in the digital space.

## **Who bears the responsibility to ensure and protect digital rights?**

States, businesses, individuals, and civil society organizations all bear the responsibility of protecting digital rights.



**Select each one below to learn more.**

---

## States —

As with your human rights, **states** (or governments) bear the responsibility to ensure and protect your digital rights—this is enshrined in the [International Covenant on Civil and Political Rights](#), a global treaty signed by 173 United Nations member states. States are obligated to both refrain from violating your digital rights (“negative” measures) AND to take action to protect and ensure your rights (“positive” measures). For example, states cannot conduct surveillance on you without following the legally defined process for doing so in their country—a “negative” measure. States also have an obligation to regulate technology companies to ensure they are not mining your data and selling it without your consent—a “positive” measure.

## Businesses —

Even though states are primarily responsible for protecting your rights, **businesses** have obligations to respect all human rights over and above compliance with any national laws in place. This is dictated by the [UN Guiding Principles on Business and Human Rights](#), which establishes global standards of expected conduct by businesses. Companies need to proactively examine the impact of their business models on human rights and avoid causing adverse impacts through their activities, directly or indirectly. Where there may be a negative impact on rights, they must take actions to mitigate that.

## Civil society organizations —

**Civil society organizations and advocates** like us play an important role in holding states and businesses to account for these commitments. Digital rights advocacy is a quickly growing movement at local, national, regional, and global levels. To get involved, review the suggested digital rights advocacy asks in the report [Free to Be Online](#), and check out these organizations conducting digital rights advocacy around the world:

- [Global Network Initiative](#)
- [Privacy International](#)
- [Ranking Digital Rights](#)

- [Digital Rights Nepal](#)
- [Fundación Karisma](#)
- [IPANDETEC](#)
- [Digital Grassroots](#)

International organizations, such as the United Nations, are also monitoring digital rights and introducing new institutions and mechanisms, such as a newly appointed [UN Special Rapporteur on the Right to Privacy](#).

## Individuals —

Lastly, as **individuals**, we have an obligation to respect the digital rights of our fellow human beings. That includes not harassing others online and protecting any personal information or data shared with you. Read on in this module to find out how to respect and protect the digital rights of your peers, fellow citizens, and technology users!



**Consider the following scenario. Use what you've learned about digital rights so far to**

## answer correctly.

You are organizing a social media campaign for an upcoming advocacy project you are working on. What steps can you take to ensure digital rights are kept in mind?

Select the best answers from the four choices below.

- 
- Consider who will have access to social media to participate in the campaign and what can be done to ensure the participation of those who don't have access.
  - Think about how to protect those who participate in your campaign from cyberbullying.
  - Ensure that any data collected is used as intended and stored safely.
  - Review security preferences for your social media accounts.

SUBMIT



UP NEXT: HOW DO I PROTECT MY DIGITAL RIGHTS?

# How do I protect my digital rights?

---

---

**Now that you know what digital rights are, it's important to be aware of possible violations of digital rights so you can take precautions to prevent them.**

## **What is the gender digital divide?**

Access to digital technology and the internet is a fundamental right, yet access may vary across communities and countries due to where you live, your income, your gender, your language, or your race or ethnicity. As gender equality advocates, it is important to know about the "gender digital divide," or the inequity in digital access for people based on their gender.



**Check out these stats on the gender digital divide.**

**If there were only 10 people in the world...**

...5 of them would not have internet access.

**If only 10 people were  
online...**

...only 1.5 of them would  
have affordable and  
accessible internet.

**If the world had 10  
people, 4.9 of them  
would be women...**

...and only 2 of them would  
have mobile access to the  
internet.

**Source: World Association of Girl Guides and Girl Scouts**

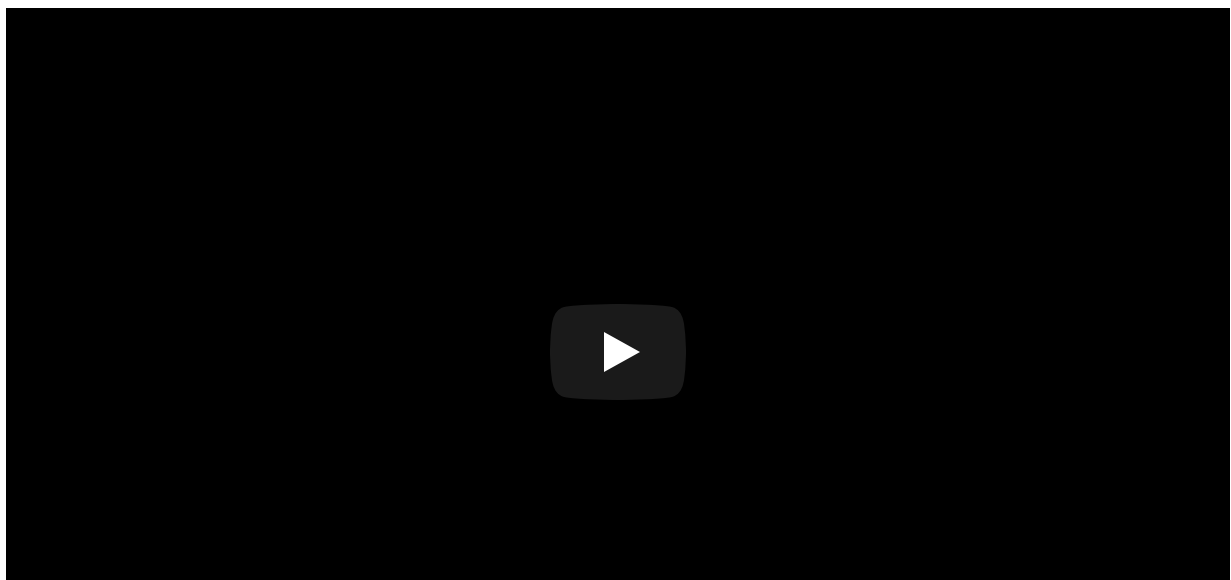
---

## **How can data be misused?**

“Data” is the raw facts or information about your identity (name, birthdate, address) and your behaviors online (what sites we visit, what search terms we use). This data actually reveals a lot

about who you are as a person and what is important to you. When compiled together, this data is called your “digital footprint.” Your digital footprint encompasses everything from which photos you like on Facebook to how long you view an ad on Instagram.

**Watch this video to learn more about when to share private and personal information (or when not to!).**





**Let's review three ways your data can be misused: use of algorithms and exploiting your information. Select each one to learn more.**



**Discrimination**



**Information control**



**Exploiting your data**



**Discrimination**



**Information control**

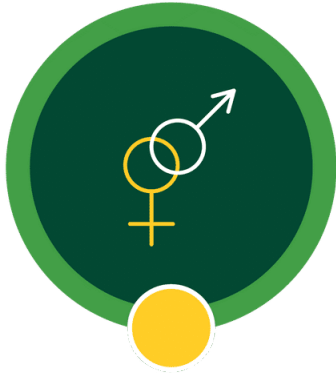


**Exploiting your data**

## **Discrimination**

Sometimes our digital footprints include data that may not accurately reflect our complex identities, such as when websites require users to choose a binary label such as “male” or “female.”

In such cases, this data can then be used to discriminate, as the targeting of information (discussed more below) often uses the personal characteristics embedded in a user’s data to control what kind of information a user sees. For example, information about contraception may only be shown to users coded as “female” and “over 18,” when in fact we know it’s important for everyone to have equal access to this information.



**Discrimination**



**Information control**

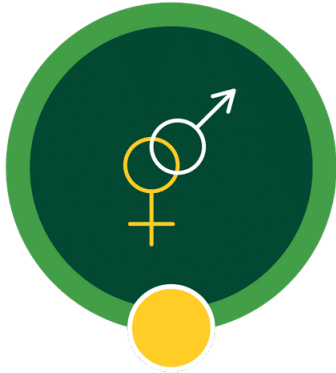


**Exploiting your data**

## **Information control**

You have a right to information and to freely express yourself online. However, algorithms and artificial intelligence used by many technology companies to enhance search capabilities disrupt the free and fair exchange of information and ideas online. For example, many algorithms elevate untrue or inaccurate content based on the number of views. This is why misinformation and sensational rumors, such as myths about COVID-19, can spread so quickly on the internet. Algorithms can be quite complex, and based on the factors an algorithm uses, the designer of that algorithm can actually control what kind of content a user sees when they use a social media site or a search platform. For example, based on the content you typically view online (for instance, from a specific news source or political party), an algorithm may be programmed to continue showing you similar content—this may prevent you from being exposed to different perspectives on an issue and lead to the spread of misinformation. This control of information places a lot of power in the hands of technology companies to decide which information to amplify. The information we consume greatly influences our opinions and ideas about our personal behaviors, beliefs, and our view of the world, thereby potentially impeding our ability to think clearly and pursue our own goals (freedom of thought). But being mindful and alert to their potential influence can help break their hold, and many advocates are pushing for greater oversight and regulation of these companies.





**Discrimination**



**Information control**



**Exploiting your data**

## Exploiting your data

Another way data can be misused is when technology companies that collect personal data share that information with other businesses who use it to target advertising, or to governments who use it to censor and control their citizens. Many technology companies operate according to a business model (how a business makes money) dependent on data extraction and/or surveillance. Sometimes, governments may even require a company to turn over data or have its own surveillance technology. Data can also be stolen by cybercriminals through hacking and cyber attacks, which have become more prevalent in recent years.

## Data protection regulations

Fortunately, there are some regulations to protect your data, such as the [General Data Protection Regulations \(GDPR\)](#). The GDPR went into effect in the European Union (EU) in 2018 and governs technology companies that operate in the EU, including Meta and Google. The GDPR requires companies that collect personal data to be clear about their intended use of the data and obtain the user's consent before it's collected. This information is usually communicated in the "Terms and Conditions" users are required to review and accept before using a platform. However, advocates argue that, given the predominance of several technology "giants"—like Meta, Apple, and Google—in our everyday lives, users do not have much choice but to agree to these terms. Therefore, the consent we give to have our data collected and used is not in fact freely given consent and could be seen as coerced consent.

# How do I protect myself online?

Now, let's discuss some actions you can take right now to better protect yourself and any organizations you are working with. Feel free to pause this course after each section and complete some of these action items.

**Select each strategy to learn more.**

## Use strong passwords

- Use a minimum of 8 characters in your password, including numbers, symbols, and uppercase and lowercase letters.
- Avoid commonly guessed passwords and personal information.
- Use different passwords for different accounts.
- Always log out when you've finished using a site, no matter what computer or mobile device you are on.
- Use a two-factor authentication login, which means that in addition to your password, you will enter a code that is texted to or accessed through an app on your mobile device.
- If you need to save your password, use paper or a secure, encrypted password management system. This is especially important if you work at an organization where multiple people need to share passwords and may access accounts on different devices. Only share passwords with your colleagues who need access to that site.

Still not sure if your password is strong? Use a tool such as [The Password Meter](#) to check it.



## Protect your digital footprint —

Keep your and others' personal information secure online by taking these actions:

- Don't share your full name or other identifying information, such as your age, specific location, phone number, or school name, on social media or in any public forums.
- Check your privacy settings on social media to ensure you know with whom you are sharing information, such as a picture, a status update, or your location.
- Remember that once something is posted online, it cannot be fully removed, so post thoughtfully! This includes your comments and reactions to other people, so remember to engage with your peers online the way you would want them to engage with you.
- Consider whether it is safe to tag your location, as this tells others where you are.
- Always ask before posting pictures, videos, or content about anyone. If you run an organization, this applies to your organization's internet activities, too—always ask for consent before sharing! If someone posts anything about you that you are uncomfortable with, ask them to take it down.
- If you are a minor or you are working with minors (under 18), speak with a trusted adult about the minor's social media presence.
- If you store any personal information or sensitive data about your staff, partners, constituents, or participants in your work, be sure this information is kept on a platform that is password-protected, encrypted, or otherwise secure.
- If you are working at an organization, consider asking for or offering cybersecurity training to your colleagues, if possible.



## Be aware of cookies

“Cookies” are not only a delicious dessert! They are also a way that your computer keeps track of your web activity, which can be helpful to record login information or to auto-fill your name and address when you are shopping online. But sometimes cookies can also hide security issues, so be sure to check what is stored in your web browser’s cookies often.

For more guidance, watch the video “[Cookies and Your Online Privacy](#).” You can also visit [How to delete Cookies?](#)



## Watch out for misinformation

There’s so much information online—how do you know what is true? Here are a few tips to sort myth from truth:

- Consider the original source of the information. What can you find out about this person, organization, or media outlet that can help you determine their credibility? Reliable news outlets employ experienced journalists that are independent from any other government, business, or organizational affiliation.

- Review other news sources that are reporting on the same story to understand how it is covered differently. This helps to correct for any bias that a given media outlet may have.
- Check your own bias. Is your own opinion clouding your judgment as to the truth of this information?
- When in doubt, turn to a known expert in that area. What are they saying about this issue?



## Responding to misinformation —

If you become aware of someone spreading false information, how should you react?

Start by speaking respectfully in a private setting with the person and don't accuse them of anything; that only serves to put people on the defensive. Using the tips you just learned, share with them why you don't think the information is accurate (for example, it is not from a trusted source; other news agencies are covering the story very differently; an expert is saying something contradictory).

You can share alternative information with them from trusted sources and ask them questions about the information they're sharing to help them see for themselves whether it is accurate or not. Sometimes, people are clouded by their own views and may not want to hear what you have to say. If a conversation becomes too heated or they are not willing to listen to you, end the conversation.

Learn more by reviewing the following two videos:

- [“Think before you share | UNICEF”](#)
- [“Helping Students Identify Fake News with the Five C’s of Critical Consuming”](#) to learn more ways to identify fake news.



**Using what you've learned so far, consider another scenario.**

You are conducting a survey online to inform a policy brief for decision-makers in your community. This survey contains personal information from those who responded. How can you best safeguard this information?

Select the best answers from the five choices below.

---

Make sure your devices and online accounts storing the private information have strong passwords.

Keep the spreadsheet with the data open on your computer. As long as no one else uses your phone or computer, the information can not be seen by others.

Check your privacy and security settings.

Use full names and identifying information in the report.

Only use this data as it was intended to be used for the purposes of this policy research.

SUBMIT

**UP NEXT: HOW DO I PROTECT MYSELF FROM AND RESPOND TO CYBERBULLYING?**

# How do I protect myself from and respond to cyberbullying?

---

---

**According to a 2020 survey by Plan International, 52% of girls have experienced online harassment and abuse. You, too, may have experienced or know others that have experienced cyberbullying. It is a serious issue that impacts the health and wellbeing of people everywhere. Luckily, there are ways to stop it and support others who might be facing it.**

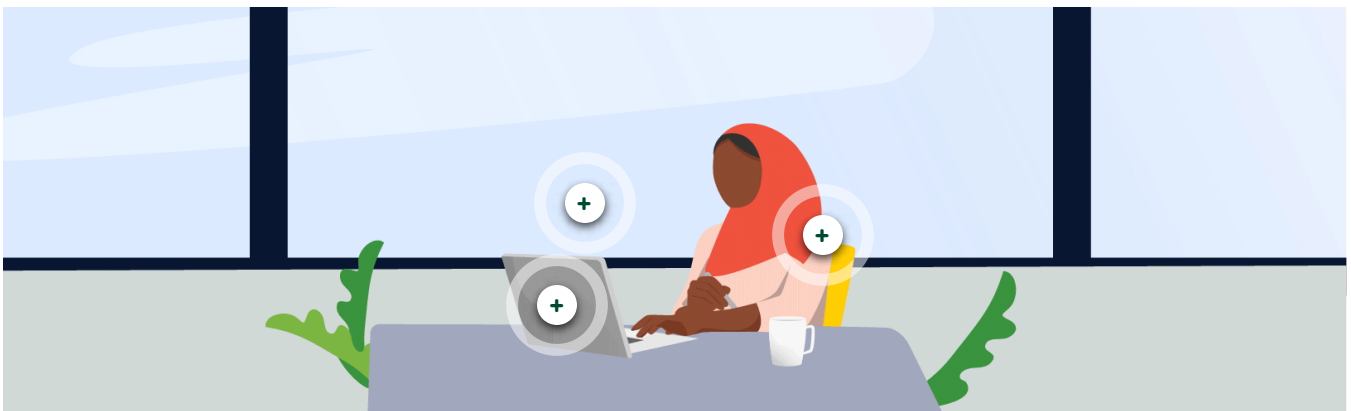
## **What is cyberbullying?**

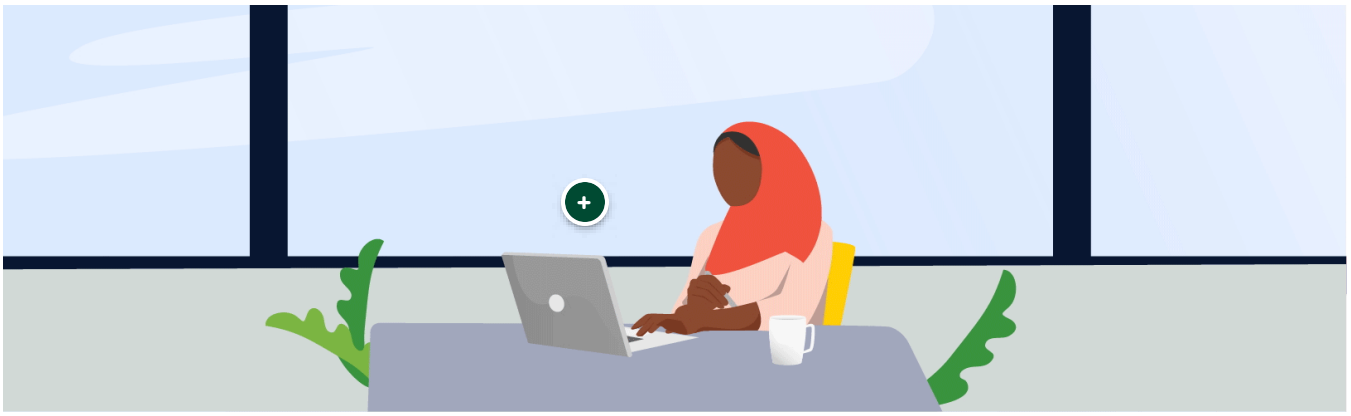
Cyberbullying is when someone is intentionally and deliberately mean or cruel to another by using technology, such as on social media, via text, email, or mobile apps.





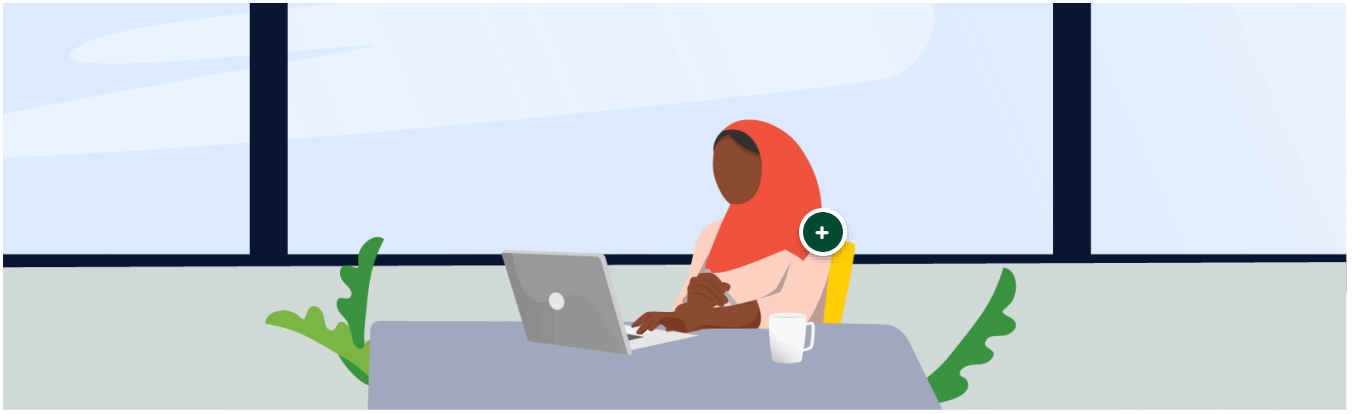
**To learn the what, where, and who aspects of cyberbullying, select each item to learn more.**





## What

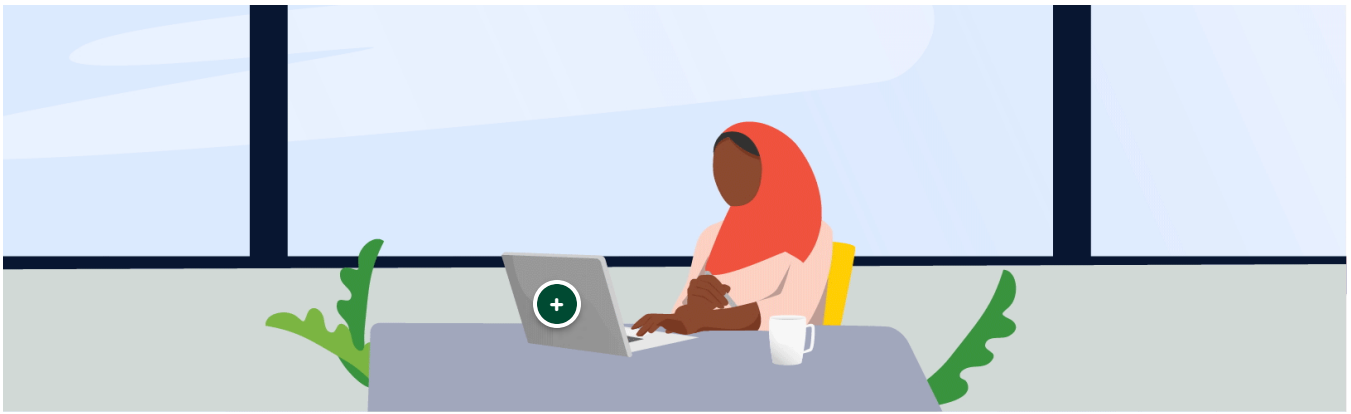
Cyberbullying can include posting, captioning, or tagging images inappropriately; excluding people from online groups or conversations; leaving disrespectful comments on someone's profile, photos, or updates; imitating or disrespecting people through one's status or online content; or sharing personal information from another without consent.



## Who

Anyone can be a victim of cyberbullying, however people who face additional discrimination or marginalization in the physical world based on their identities—such as girls and women; Black, Indigenous, and People of Color (BIPOC); LGBTQIA+ people; people at the intersections of these identities; and other traditionally excluded populations—often are more susceptible to cyberbullying.

For example, gender-based cyberbullying is when someone is bullied online because of their actual or perceived sexual orientation or gender identity.

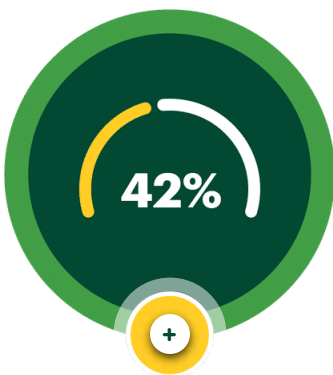


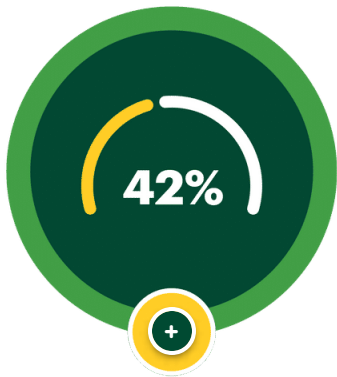
## Where

Because cyberbullying happens online, it can happen at any time or from any physical place, but it often takes place in a public digital space. Unlike in-person bullying, a cyberbully may feel more anonymous or safe because it is taking place online, making it harder to control and stop.

Sometimes cyberbullying can lead to in-person bullying or harassment, especially if someone's personal information, such as their name and location, are shared online. According to a Plan International report, one in four girls who experience cyberbullying say they feel physically unsafe as a result.

## Take a look at these findings from a **PLAN study**.





## 42%

The percent of girls in this study who say they were harassed for being LGBTQ+ (out of all girls who identify as LGBTQ+ and have experienced harassment).



## 14%

The percent of girls in this study who say they were harassed for having a disability (out of all girls who identify as having a disability and have experienced harassment).



**37%**

The percent of girls in this study who say they were harassed for being from an ethnic minority (out of all girls who identify as being from an ethnic minority and have experienced harassment).

**Source: [Plan International](#)**

With many social interactions confined to the online space during COVID-19, many young people report cyberbullying as having increased during the pandemic.

As advocates, we are often outspoken about our views and beliefs, which may be controversial or even radical in our communities. We may also be harassed online because of our beliefs, political affiliations, and personal opinions. In a Plan International study of gender equality youth advocates, 47% reported being attacked online for their opinions. The cyberbullying of advocates may be an attempt to silence those advancing social justice or gender equality issues.

**Let's review how to respond to cyberbullying. Select each one to learn more.**

## **How do I protect myself from cyberbullying?** —

People who engage in cyberbullying are not likely to respond to rational thinking or reason, so it is best not to respond or engage. This will likely make it worse. Instead, save copies or screenshots of the harassing behavior, change your privacy settings and block the person who is bullying you, if possible. Depending on the digital platform, there may be an option to “report abuse.” Remember that in many cases, someone has to be reported multiple times before they are blocked from a platform, so the harasser may attempt to harass you or others again through an alternate (unblocked) profile. If the person is someone you know personally through school or your workplace, talk to a teacher or manager about what happened. They may have ways to support you. In some cases, there may be local or national laws to protect from cyberbullying.

Additionally, cyberbullying, just like bullying or harassment in the physical world, can cause harm to our mental health. Talk with a trusted friend, advisor, parent, or mental health professional about your experience, find help in your community through [Child Helpline International](#), or search for online resources.

## **How should I respond to cyberbullying when it’s happening to others?** —

First and foremost, be aware of how you treat others online to ensure you are not contributing to cyberbullying. If you see someone being cyberbullied, talk to the person and offer any support you can, such as listening or helping them access resources. Do not engage directly with the harasser online, as that may put you at danger of being bullied, too.

Raising awareness about the impact of cyberbullying may help young people realize the serious damage it can cause, which can help prevent it before it starts. Additionally, social-emotional curricula that educate young people about healthy and respectful relationships can not only teach them how to interact with kindness and compassion but also build resilience so that they can better cope with any experiences of cyberbullying. On a large scale, public awareness campaigns can help send this message, and laws can hold harassers accountable. Some advocates are also holding social media companies accountable for the impact of their platform on users.



## **Case study: A young leader takes action to end cyberbullying**

**In addition to the ways we can all support each other if we see cyberbullying happening, many young people are taking action to prevent it from happening and to provide support to those who experience it. Women Deliver Class of 2020 Young Leader, Agita Pasaribu, is one such advocate! After no one took her own reports of workplace sexual harassment seriously, Agita, frustrated, founded Bullyid Indonesia. Bullyid provides free online mental health and legal support for victims of cyberbullying. As an advocacy organization, Bullyid aims to increase awareness about digital rights, specifically as it relates to cyberbullying, and increase the self-care and resilience of young people who may face cyberbullying. This multi-pronged approach addresses both the causes and impacts of cyberbullying.**



**One type of cyberbullying is revenge porn, which is known by the legal term, "image-based sexual abuse." Revenge porn is the act of sharing intimate images or videos of someone without their consent, either online or offline, with the intention of causing distress. Since the COVID-19 pandemic hit Indonesia, Bullyid has expanded its scope of services and advocacy to include the Revenge Porn Help Centre.**

**Between March to May 2020, the online abuse cases in Indonesia increased over 300% compared to 2019's statistics, according to the Ministry of Women Empowerment and Children Protection of Indonesia, and many of the cases that came to Bullyid fall under the category of online defamation and revenge porn. Seeing this, Bullyid sent a formal letter to several social media companies asking them to provide support for victims of revenge porn by taking down/removing this content quickly. Right now, Bullyid's Revenge Porn Help Centre works closely with the Public Policy Department of**

**Facebook/Instagram and Twitter Indonesia to remove any revenge porn content that is shared on their platform faster.**



**With the support of a Women Deliver Small Grant, Bullyid managed to add new features to the platform. Bullyid's SHARE Reporting Platform is the first secure and anonymous harassment reporting platform for institutions that allows their employees and/or students to report any harassment/cyberbullying or misconduct behaviors. It also comes with an incident case management platform that allows universities to respond, manage, and provide psychological support to victims. Since its launch in May 2021, SHARE Platform has been protecting 14 companies, four universities, and two organizations with 27,780 employees and students in Indonesia from cyberbullying. As a leading registered charity that works to prevent cyberbullying and harassment, as well as to provide help for victims, Bullyid has been featured in and partnered with 179 media outlets and organizations, including the World Health Organization, UNICEF, and One Young World. To date, Bullyid digitally benefits over 45,000 Indonesians and continues to seek more partnerships and advocate the cause to increase impact and save more lives.**



**It's time to consider how you would respond to these scenarios, using the information**

## you've learned so far.

Someone that you met at a recent school event begins sending you personal messages on Facebook. The messages start off complimentary, but soon devolve into pushy offers to take you out to dinner, asking for your phone number, and requests for personal photographs.

What actions can you take to protect yourself? Select all that apply from the six options.

- 
- Mute the conversation and block the user sending you the messages.
  - Save a copy of the messages.
  - Respond to the messages directly and tell them to leave you alone.
  - Report the conversation to Facebook and to your school.
  - Publicly post their name and what they've said to you on your status to shame them.

Ask a trusted family member, good friend, or mental health professional for help to process the experience.

SUBMIT

A young mother posts on Instagram a picture of herself on her first day going back to school after recently having her baby. You see a slew of negative responses, primarily from men, harassing her and saying she does not belong in school anymore now that she is a mother.

How can you best support this young woman? Select the best answer from the three options below.

---

Because you don't know this woman personally, you should not get involved.

Share the post on several social media pages to point out the injustice of what is occurring.

Reach out to her, listen, and refer her to services that can provide additional support, as needed.

SUBMIT

UP NEXT: WRAP UP

## Wrap up

---

With everything you have learned about your digital rights, how to protect them, and how to guard against cyberbullying, you are ready to put your knowledge to use in the real world.

We recommend implementing the best practices you learned in this course, particularly in the scenario sections. Be on the lookout for issues and situations that come up online with your partners and allies, and assist whenever you can. And don't forget to reach out to a trusted family member or friend when you need support.

[Next steps](#)



# Post-Assessment

---

**Now proceed to the post test to check your knowledge one more time.**

---

*Question*

**01/01**

---

7 questions drawn randomly from Human Rights in the Digital Age Pre/Post-  
Assessment\_EN

# Human Rights in the Digital Age Pre/Post-Assessment\_EN

---

Question

**01/07**

All human rights you have in the physical world (offline) apply to your digital self when you are online.

---

True

False

Question

02/07

Your digital rights include: (Select all that apply)

---

- The right to privacy
- Freedom of expression
- The right to live free of violence and harassment
- The freedom to do anything you want to do

Question

**03/07**

What are three ways your digital rights can be violated? (Select all that apply)

---

Cyberbullying

Data mining

Blogging

Surveillance

Question

04/07

Who bears the responsibility to ensure and protect digital rights? (Select all that apply)

---

States

Businesses

Individuals

Civil society organizations

Question

05/07

What should you do if you see someone else being bullied online?

---

- Confront the bully publically and call them out on their behavior so that others learn from the situation as well.
- Send a private message to the bully to tell them that their behavior is inappropriate and that you have alerted the proper authorities.
- Do nothing, as this could feed into an already negative situation.
- Offer support and a listening ear to the victim.



Question

**06/07**

35% of girls have reported that they have experienced online harassment and abuse.

---

True

False

Question

07/07

What are some ways you can protect yourself and your data online? (Select all that apply)

---

- There is no way to protect yourself unless you abstain from using the internet entirely.
- Use strong passwords.
- Check your privacy settings on all social media sites.
- Accept all "cookies" on websites you visit.
- Watch out for misinformation by checking sources and doing additional research.