

CYBER ABUSE PROJECT TOOLKIT

TABLE OF CONTENTS:



- Introduction
- Supporting Youth Survivors
- Digital Evidence Collection Guide
- Non-Consensual Sharing Guide
- Cyber Safety Plan
- Case Studies

Produced by:



The Cyber Abuse Project was supported by Grant No. 2016-TA-AX-K070 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Introduction to the Toolkit

The Cyber Abuse Project (CAP) is an initiative of Break the Cycle and the California Coalition Against Sexual Assault. CAP aims to provide training and technical assistance to criminal justice professionals and other adult first-responders on the use and misuse of technology in sexual assault, domestic violence, dating violence and stalking (including cyber-stalking) cases involving young people ages 12-24.

The tools available in this toolkit were identified as a result of researching related issues, resources, and response processes available to young people impacted by cyber abuse, including a series of listening sessions with youth and adult first-responders.

Each tool helps to inform young people, and the caring adults in their lives, about their options after experiencing different forms of cyber abuse. These tools also help to promote the autonomy of young survivors as they determine how to proceed, particularly when pursuing criminal justice remedies.

The Tools

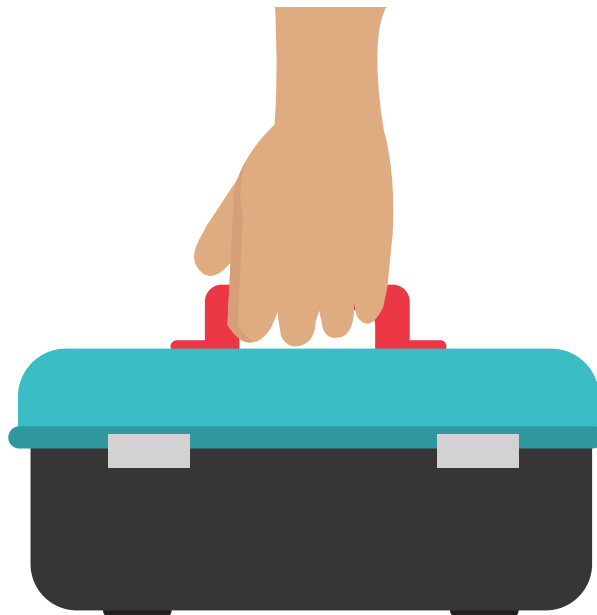
Supporting Youth Survivors: This one-pager shares important tips for adults to keep in mind when supporting a young person who is experiencing or at-risk of cyber abuse.

Digital Evidence Collection & Safekeeping Guide: This guide shares tips for gathering digital evidence that can be later used in civil and criminal court cases.

Non-Consensual Sharing of Intimate Images Guide: This guide shares legal and non-legal options for young people who have experienced the non-consensual sharing of their intimate images.

Cyber Safety Plan: This guide helps young people, and their supportive adults, identify personalized strategies to promote their safety online and in person.

CAP Case Studies: These sample stories help identify the ways CAP tools can be used to support young people when they have experienced different forms of cyber abuse.



Supporting Youth Survivors of Cyber Abuse

What can we do as adult responders?

It's our responsibility to make sure young survivors and their support systems are aware of all the available options when they've experienced cyber abuse, so they can make informed decisions. It's important to understand the spectrum of options for survivors and to share that information.

If a young person has experienced cyber abuse, including the non-consensual sharing of their intimate images, and reaches out to you for support, here's how you can help:

Interact with survivors in a victim-centered and trauma-informed way.⁷

- **Recognize** that not all survivors experience victimization similarly, even when they are victims of the same crimes. How a survivor reacts to abuse may be largely shaped by their age, gender, sexual identity, race, ethnicity, and previous experiences.
- **Acknowledge** that victims of cyber abuse and the non-consensual sharing of intimate images have experienced trauma like other victims of sexual abuse. While physical trauma is often visible, emotional trauma can be difficult to identify and comes⁸ in many forms.
- **Respect** survivors' agency. Some survivors may decide pursuing a protection order is the safest course of action. Some may want civil remedies or restitution for the harm they experienced. Others may want to press criminal charges. Still, some may not want to take legal action at all. Whichever course of action survivors choose, it is essential for advocates, criminal justice professionals, and judges to respect victim autonomy throughout this process.
- **Respond** to victims in a supportive and transparent manner that recognizes their individual trauma and does not cause further harm. When victims feel they are not supported, they may experience secondary trauma and begin to distrust criminal justice professionals or other adult responders.

Engage in safety-planning efforts.

A **safety plan** is a personalized plan that promotes victim safety in the wake of ongoing abuse or the threat of future violence.⁹ Safety plans are tailored to fit the unique needs and lifestyle of the victim, as well as the extent and severity of the abuse. Plans may include how to cope with emotions, report abuse to friends and family, and take legal action.

Share the options & help youth prepare

Explain to survivors all of the options available to them and provide them the resources to make an informed decision. Once the survivor chooses the option that is best for them, prepare them for what the process might be like, including the possibility of losing their electronic device to evidence collection.

7 Kristiansson, V. & Whitman-Barr, C. (2015, February). Integrating A Trauma-Informed Response Violence Against Women and Human Trafficking Prosecutions. *Strategies: The Prosecutors' Newsletter on Violence Against Women* (13), 2.

8 National Center for Victims of Crime. (2008). How Crime Victims React to Trauma. Get Help Bulletins for Crime Victims. Retrieved from <http://victimsofcrime.org/help-for-crime-victims/get-help-bulletins-for-crime-victims/how-crime-victims-react-to-trauma>

9 The National Domestic Violence Hotline. (2013, April 10). What is Safety Planning. Blog. Retrieved from <http://www.thehotline.org/2013/04/10/what-is-safety-planning/>

DIGITAL EVIDENCE COLLECTION GUIDE

TABLE OF CONTENTS:

- THE 4 C'S
- PHONE CALLS AND VOICEMAILS
- TEXTS AND EMAILS
- SOCIAL MEDIA
- ONLINE GAMING AND FORUMS

Produced by:

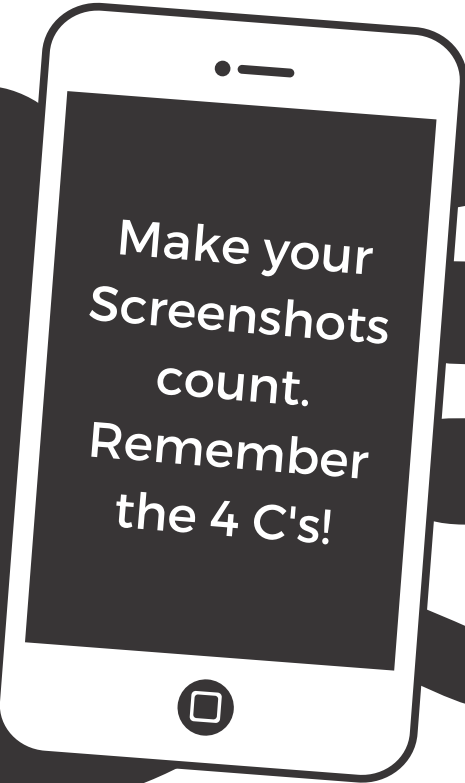


The Cyber Abuse Project was supported by Grant No. 2016-TA-AX-K070 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Digital Evidence Gathering & Safekeeping

If you've experienced cyber abuse -- whether a partner is sending threatening or controlling messages, constantly calling, or if someone has shared your intimate images without consent -- the digital evidence left behind can be used in civil and criminal court cases, including protection orders. Even if you aren't ready to pursue legal action, documenting and storing digital evidence gives you options if you change your mind later.

You can use screenshots of text messages, social media posts, emails, phone call logs, voicemails, and so much more.



Make your
Screenshots
count.
Remember
the 4 C's!

CONTACT INFO & DATE

COMplete CONTEXT

CONTROL POSTS

CONFIDENTIAL STORAGE

C ONTACT INFO & DATE

Screenshots should include details that identify the person who is abusing you, such as their name, user/profile name, profile picture, and phone number as they appear on your device. Also include the date & timestamp of the communication. Judges won't know who was contacting you or when without these identifying details.



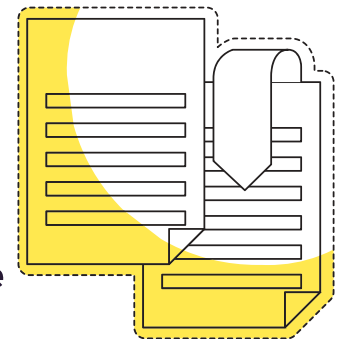
C COMPLETE CONTEXT

Screenshots of texts, emails, chats, or direct messages should include all original messages exchanged by both people - even if you think it looks bad or embarrassing. Remember, Judges can compare your screenshots with the other person's copies. Also capture past messages in an email chain or prior communications that help add context. Make sure to overlap text message screenshots (see how on the next page).



C ONTROL POSTS

Screenshot abusive posts on social media as soon as you see them to capture evidence of posts you don't control. Remember, people can delete content from their page or block others at any time. Some apps also delete content automatically. Friends can also help get screenshots of posts if you do not have access to the original post/page.



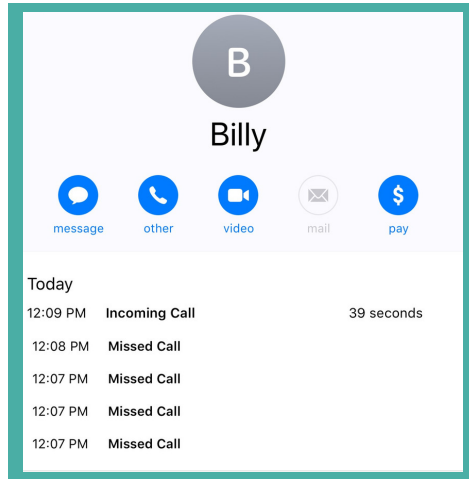
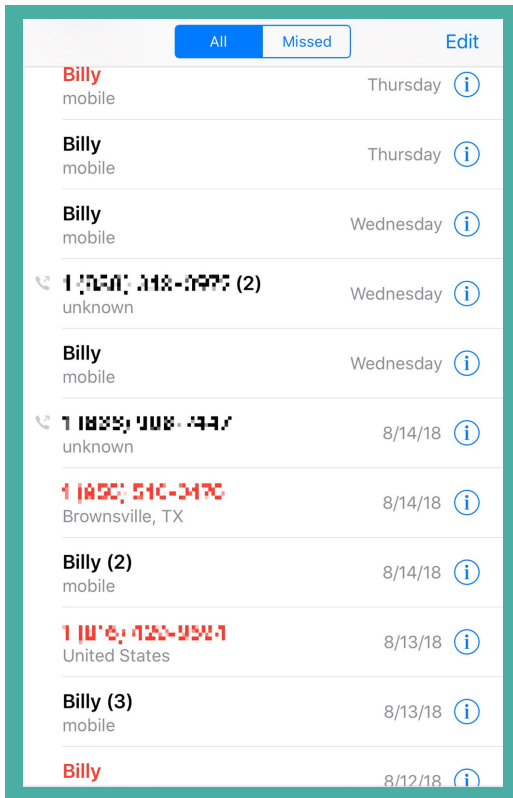
C ONFIDENTIAL STORAGE

Devices get broken, lost, stolen, monitored, and hacked, so they are not a good place to store your evidence. Once you've taken screenshots, immediately send them to a secure email account or cloud that only you have access to. You can also send them to a friend, advocate, or attorney who can keep a copy for you. Print and keep a copy if it is safe to do so. Some state's laws may require consent before sharing intimate images. If your screenshots include intimate images, consult a lawyer for more information about issues of consent in your state.



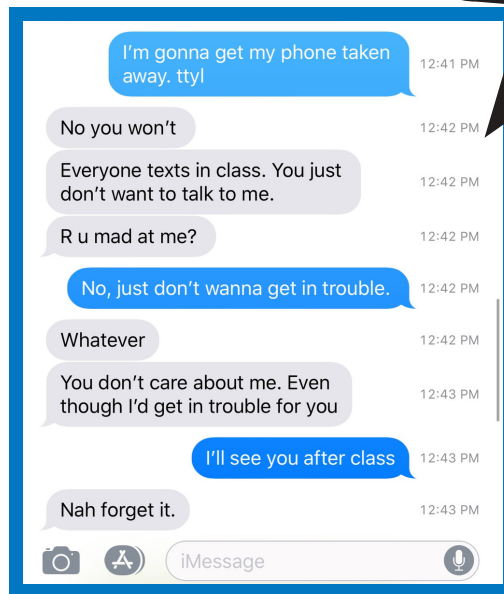
The practices above are helpful but are no substitute for the judgment of a survivor and their attorney. Consult an attorney or legal advocate for more information about evidence and its uses in court cases. Visit breakthecycle.org to find a cyber safety plan and information about our legal services.

PHONE CALLS & VOICEMAILS



Screenshot voicemail & call logs showing # of calls, caller's information, & dates (some devices show the day instead of date). Keep notes detailing what happened on answered calls, especially if you're able to identify an unknown/restricted number.

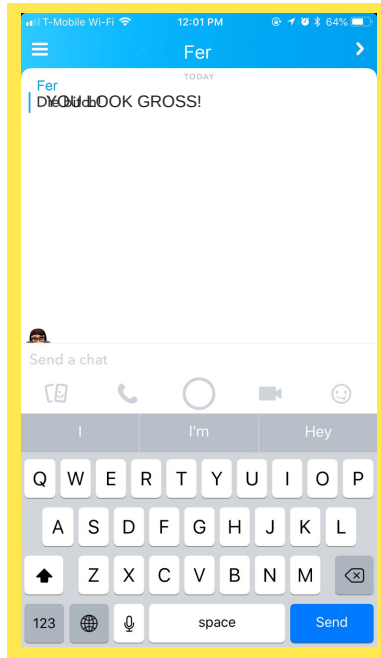
TEXT & EMAILS



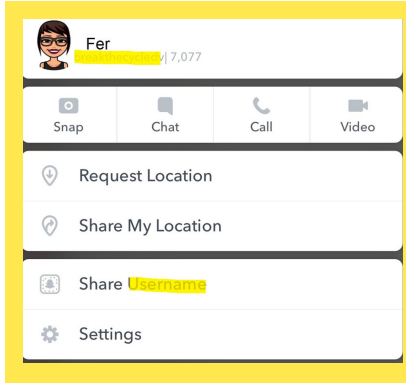
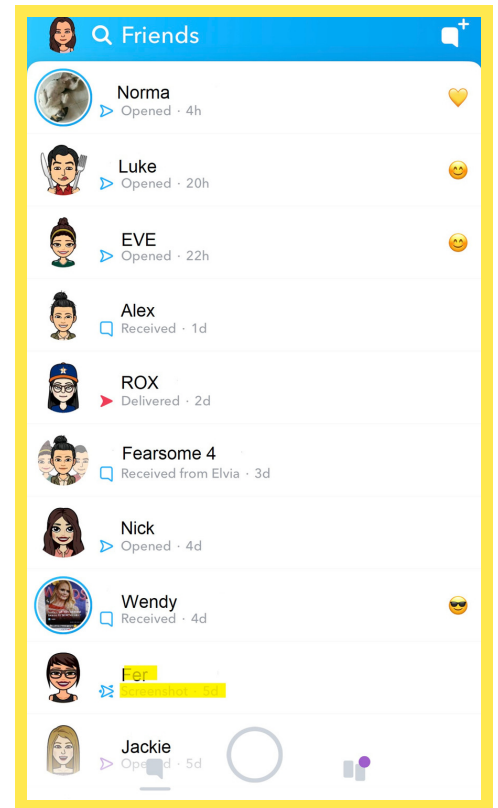
Capture identifying information such as name, phone number/email address, the dates of messages, & the subject line from emails. Keep screenshots of previous & on-going messages in the conversation in order to show the flow of the conversation.

SOCIAL MEDIA

Screenshot identifying information & all related messages. Because Snapchat & Instagram notify users when screenshots are taken, consider taking a photo of the content on your phone from another phone. You can also report online misconduct to the social media platform.

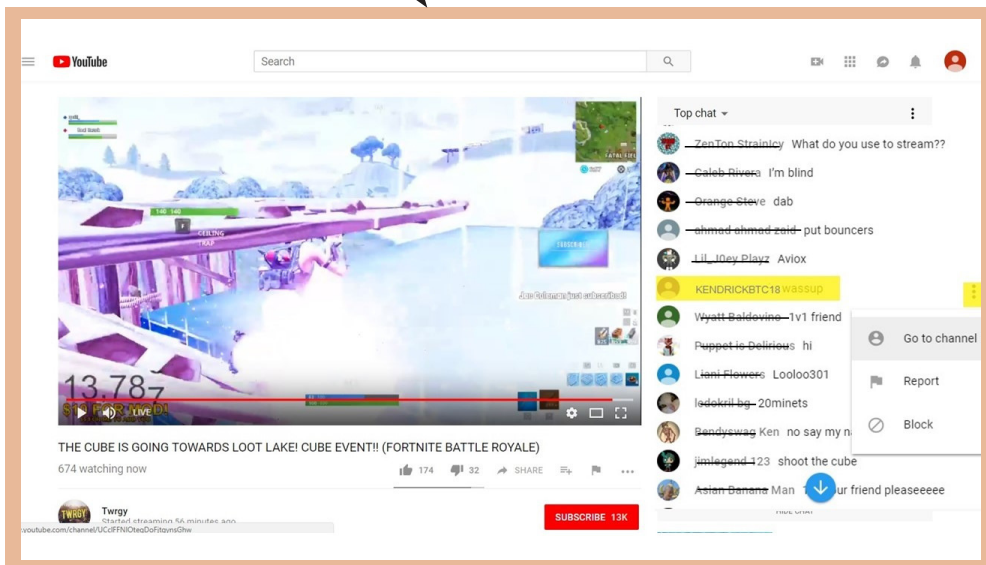
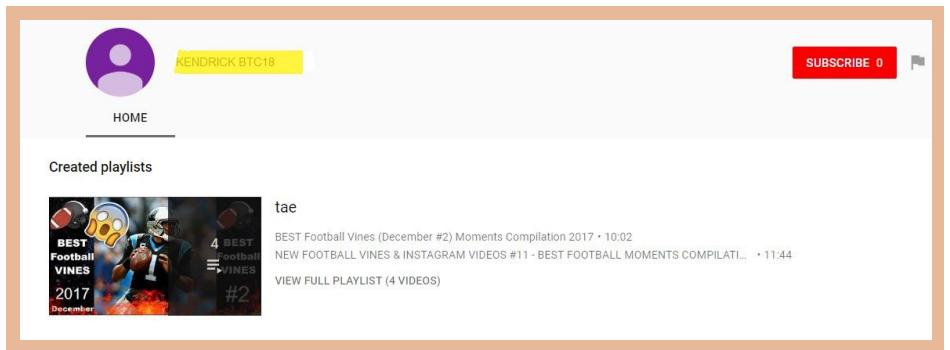


CLICK the menu tab to get full details of the snap.



ONLINE GAMING & FORUMS

Capture the user's name, picture, & identifying information listed in the user's channel, and screenshot the on-going conversation & messages. Consider reporting online misconduct if safe to do so.



CLICK the "Go to channel" tab to get the platform user's full details.

NON-CONSENSUAL SHARING OF INTIMATE IMAGES GUIDE

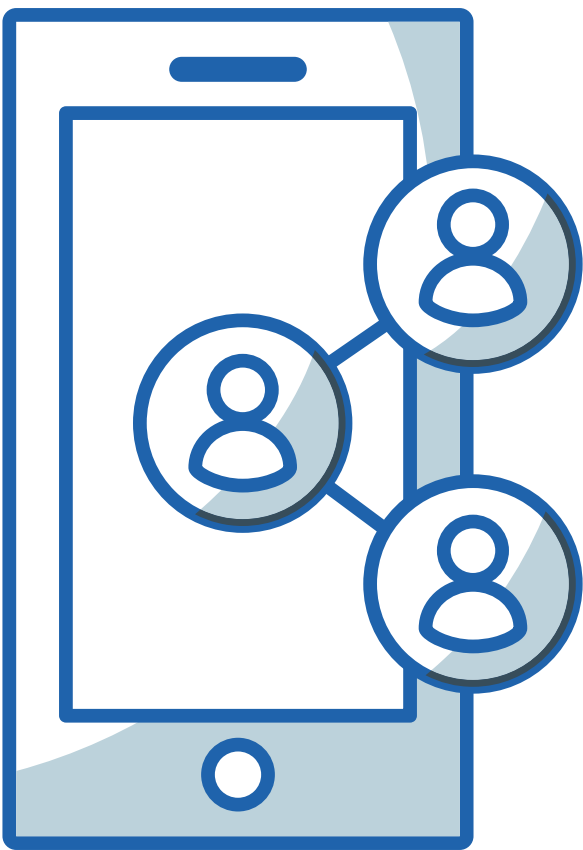


TABLE OF CONTENTS:

- What is Non-Consensual Sharing of Intimate Images
- Legal Options & Non-Legal Options
- DMCA Takedown Notice

Produced by:

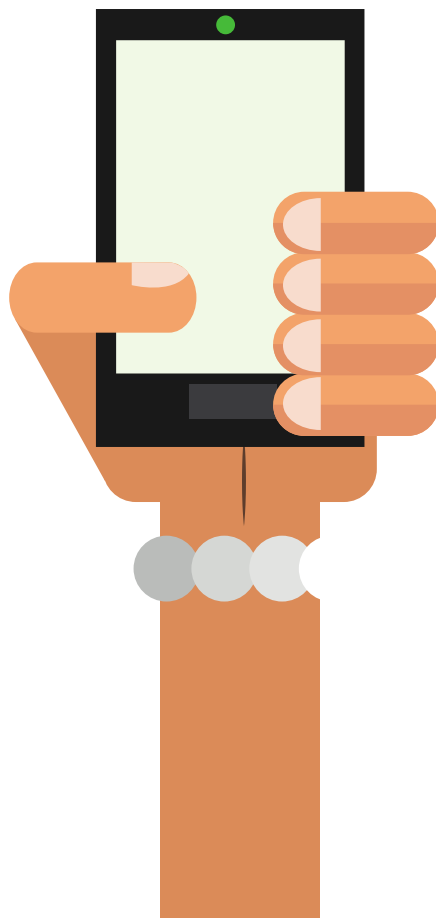


The Cyber Abuse Project was supported by Grant No. 2016-TA-AX-K070 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

What is Non-Consensual Sharing of Intimate Images?

Non-Consensual Sharing of Intimate Images is when someone shares nude or semi-nude pictures or videos of a person online or through text messaging without their permission. The images are often obtained from two different scenarios: pictures and videos are shared consensually by the person who appears in the image, or the images are taken nonconsensually by other means (e.g., a cell phone, computer hacking, friend of a friend, etc.). These images are often used to blackmail, harass, or even ruin an individual's reputation.

If someone shares nude or semi-nude content of you without your consent, you can take action. Here are some legal and non-legal options available to you:



Non-Consensual Sharing of Intimate Images

This Happened, Now What?

Legal Options: (Note: laws vary by jurisdiction)¹

1. **Criminal Charges**-- You can report the abuse to the police and they can work with you to file a criminal charge against the person who shared your photos.
2. **Civil Remedies**-- If going to the police isn't for you, you can also apply for a civil remedy and request that the offender take responsibility for sharing your private images. Under civil remedies, there are a few options:
 - a. **Suit for Damages**-- you can request "damages" or a remedy for the harm you felt as a result of the sharing of your images.
 - i. **Copyright Action**:² If you are the person who took the original photo (i.e. it was a selfie) then you own the copyright to the photo, even if someone else shares it. Under copyright actions, you can request that the image be removed from any websites, hold the offender legally accountable for sharing your image, and maybe even get money to help pay for any harm you have felt due to the sharing of your images.
 - ii. **Privacy Torts Claim**: You can also seek remedy if you believe the posting of your image has invaded your personal privacy or portrays you in a false light. Click here to learn more about privacy torts.³
 - b. **Apply for a Protection Order**:⁴ A protection order can help protect you from the abusive person in your life. A protection order is a legal order signed by a judge that requires your abuser to do certain things, like stay away from you.
3. **Takedown Procedures**⁵ Contact the platform where your image is posted and ask that the platform remove the image from their site, also called a DMCA Takedown notice. In addition, you could ask the platform to suspend the abuser's account because the image was illegally posted.
4. **Administrative Remedies**-- **Your school and/or employer have policies and procedures in place to protect you from cyber abuse.**
 - a. **Title IX**⁶-- Title IX is a federal law that allows students to hold their schools legally accountable if a student experiences cyber harassment or other sex-based discrimination and the school fails to respond appropriately.

¹ <https://www.cybercivilrights.org/venge-porn-laws/>

² <http://www.withoutmyconsent.org/resources/copyright-registration#what-are-benefits-registering-copyright>

³ <https://torts.uslegal.com/intentional-torts/invasion-of-privacy/>

⁴ <https://www.breakthecycle.org/sites/default/files/Protection%20Orders%20101.pdf>

⁵ <http://www.withoutmyconsent.org/resources/take-down>

⁶ <https://www.knowyourix.org/>

Non-Consensual Sharing of Intimate Images

This Happened, Now What?

Non-Legal Options:

Going the legal route is not for everyone. It can be time-consuming and without guarantees. But you can regain your power and recover from the trauma of technology-facilitated cyber abuse. If you do not wish to take legal action, here is a list of other non-legal options that are available:

Seek Healing

Non-consensual sharing of intimate images can have a traumatic effect on victims of this crime. Survivors frequently describe the same powerlessness, shame, humiliation, paranoia, and anger experienced by survivors of physical assaults, and typically do not make a distinction between the pictures and their physical person – violation is violation. There are many options available to survivors with no timetable for recovery. Healing looks different for everyone, and everyone moves at their own pace – don't feel rushed to do anything that doesn't work for you and your process. Below are some options:

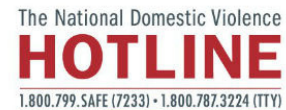
Hotlines: survivors can receive free, confidential crisis support over the phone. Contact the resources below to find a local program that fits your needs.



844-878-2274.



1-800-656-4673



1-800-656-4673

Group Counseling: survivors can meet with a licensed mental health professional in a group setting and work with others who have experienced similar traumas. If you are a student check with your campus for support group resources, or online resources such as a therapy finder can assist in locating confidential counselors near you.

Individual Counseling: survivors can meet individually with trained professionals to help recover from various forms of abuse. If you are a student check with your campus for support group resources or online resources such as a therapy finder can assist in locating confidential counselors near you.

Safety Planning- A safety plan is a personalized set of actions, strategies, and resources that address physical & emotional safety from ongoing abuse or threats of abuse. This can include staying safe from cyber abuse. Check out our Cyber Safety Plan Guide at breakthecycle.org to create your own.

Non-Legal Options Continued:

Confronting Those Who Do Harm- sometimes survivors are in, and have to remain in close proximity to those that do harm (e.g., classmates, co-workers, or family members, etc.). With the support of advocates and careful facilitation, survivors of NCS can find a face-to-face process beneficial. All parties involved must volunteer to participate freely, and it is imperative that you feel safe and free from imminent and/or future harm. Below are the most common practices:

Restorative justice- with trauma-informed skilled facilitators, survivors are able to voice the impact of the harm done, ask questions, and seek acknowledgment of responsibility from the perpetrator in a conference-like setting. In some instances, this approach can be used to make amends to the victim, family, and community. As an additional step, harm-doers can create an action plan to prevent the reoccurrence of harm. In the case of cyber abuse, this could include attending prevention education classes or counseling.

Mediation- in cases where you just want pictures removed, this process can be used to convince the perpetrator to do so. Like restorative justice approaches, participation in mediation must be voluntary and safe for survivors.

YOU DO NOT HAVE TO GO THROUGH THIS PROCESS ALONE

Whatever you choose know that you are a survivor, that this is not your fault, and that you can recover from the abuse with help. If you are a student, here are some people that can assist you:

Middle & High Schools

- School Resource Officer
- Counselor/Social Worker
- School Administrators
- Local Domestic Violence/Sexual Assault Program
- Attorney/Lawyer
- School Nurse

College Campuses

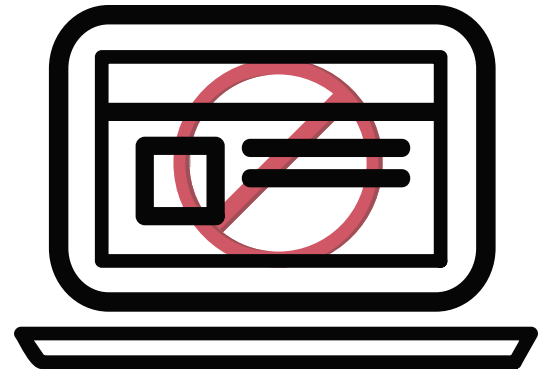
- Campus Law Enforcement
- Campus Women's Resource Center
- Local Domestic Violence/Sexual Assault Program
- Attorney/Lawyer
- Title IX Coordinator

While law enforcement and legal professionals want to support you, you can help these professionals by knowing how to collect and preserve evidence relevant to your case. Visit Without My Consent's "**Something Can Be Done! Guide**" to learn more about evidence preservation.

DMCA Takedown Notices

What is a DMCA takedown notice?

DMCA stands for the Digital Millennium Copyright Act, a federal law that protects copyright owners (authors, artists, musicians, and regular people) from copyright infringement. When you take a photograph or video of yourself (or of anything), YOU automatically own the copyright to that content and have the right under federal law to have the content removed from a website where it appears without your consent.



This includes your intimate images or content shared without your consent.

A Takedown Notice is a letter sent to a company, web host, search engine, or internet service provider notifying them that they are violating your copyright. The Notice requests that they remove the content from their website because you own the copyright, and it was uploaded without your consent.

Does my photo/video have to be registered with the U.S. Copyright Office before I can send a DMCA Takedown Notice?

No, you don't have to register a copyright before sending a notice to a company to remove the content. Registering is helpful if you get into a legal battle over the content later. However, most companies will take the content down immediately once they receive notice to prevent being sued for damages. Learn how to register a copyright here: <https://www.copyright.gov/help/faq/faq-register.html>

Is there a form I can use for this?

Some companies, web hosts, and search engines offer DMCA forms you can use on their websites. There is also a sample letter at the end of this guide.

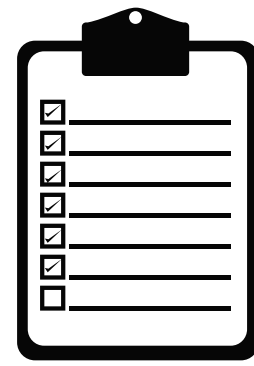
Where do I send the Takedown Notice?

Many companies have a web page, sometimes referred to as the "abuse department," with the contact information for their "DMCA Agent." Send your notice to the specified person in the format requested by the website, whether it be e-mail, fax, or mail.

How long will it take them to take down the content?

It can take anywhere from one to ten days on average to remove the content.

What steps should I take in order to file a DMCA Takedown Notice?



Step 1:

If you can do so safely, try to contact the person who posted the content and ask them to remove it. They may not have known the content was originally yours or posted illegally. It could also help lead you to the user who first posted the content illegally.

Step 2:

Locate the URL of the content you want removed **and** the URL of where you originally posted the content. For example, if someone shared your Instagram photo, you'll need the URL for your original Instagram post and the URL where the content was shared without consent. Include this information in your notice.

Step 3:

Use the sample letter in this guide or one from the company's website to draft your notice. You must include:

- both URL links
- statement of good faith
- perjury declaration statement
- confirmation of correct information
- your contact information & signature

Important note:

If you are under 18, copyright law states you have the right to make claims. However, it's recommended to seek help from a caring adult, campus resource officer, or legal aid to walk you through these steps or make your claim stronger.

Step 5:

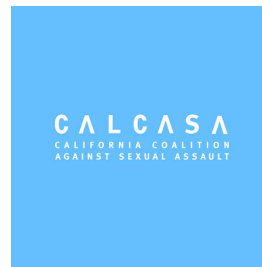
Check the company's website to find the name of the "DMCA Agent" who accepts Takedown Notices, sometimes listed within the "abuse department." Address your notice to this person.

Step 6:

If possible, send the notice via the company's website using their DMCA Form. Otherwise, send the notice in the format requested by the company's website and save a copy for yourself. This may be via fax, registered mail, electronic mail, or regular mail.

Step 7:

Follow up if you do not hear back within 10 days.



SAMPLE DMCA TAKEDOWN NOTICE:

Dear Sir/Madam [*include name of company's DMCA agent if known*]:

Please consider this formal service of a DMCA Takedown Notice on your company as a service provider. I have a good faith belief that the content listed below has been published on your website without my authorization or consent and that I am the copyright owner of this material.

As required under 17 U.S.C. 512 (c)(3), I hereby submit:

My Original Content: [*Here you would post the URL link to the original content. Include any other important information here that would be important to identifying the material, such as a title.*]

Infringing Page: [*Here you would include the URL link to the reposted or infringing page on the company's website.*]

I declare, under the penalty of perjury, that the information in this Notice is correct, that I am the copyright owner of the content in question, and that I have the exclusive right to act on this infringement. Please remove the content listed above and tell me when you have done so.

My Contact Information is:
(Your First and Last Name)
(Street Address)
(City, State, Zip Code)
(Phone)
(Email)

Signed,
(your signature)

CYBER SAFETY PLAN

TABLE OF CONTENTS:



What is a safety plan?

Things I can do to keep myself safe

My personal resources

Reporting abuse online

Produced by:



What is a Safety Plan?

A safety plan is a practical guide that helps lower your risk of being harmed by someone who has abused you in the past. It is designed specifically for you and your lifestyle so you can stay safe. A safety plan can help you navigate harmful situations you may encounter online and when you are using your phone or other device.

Why do I need a Safety Plan?

Everyone deserves to be part of a fun and supportive online community. If you are experiencing harmful interactions online or on social media, it is important to know that cyber abuse is never your fault. It is also important to start thinking about ways to keep yourself safe from cyber abuse. While you can't control everything that happens to you online, you can take action to keep yourself as safe as possible.

How do I make a Safety Plan?

Take some time for yourself and go through this safety plan guide. You can complete it on your own or with someone you trust.

Keep in Mind:

- For a safety plan to work, you must fill in personalized answers so that you can use the information when you need it most.
- Once you complete the safety plan, keep it in a secure place where you can always access it. You may want to give a copy to a friend, take a picture of it on your phone, or keep a copy in your email.
- Getting support from someone who has experience working with students in abusive relationships can be very useful. Keep in mind that Break The Cycle is always here to help you.
- It may be unsafe to abruptly change your digital routine so use your best judgement.

Things I can do to keep myself safe from Cyber Abuse:

- I can control what I post knowing that anything I post can be reposted or screenshot.
- I can make my profile private so that I can screen who follows me and control who has access to my page.
- I can be mindful of any suspicious accounts and report them as necessary.
- I can choose not to engage with any harmful accounts or posts.
- I can ask my friends not to tag me in any social media posts or pictures.
- I can read the terms and agreements of websites so that I understand their privacy conditions.
- I can chose not to use my real name or any other important biographical information while interacting with people online.
- I can use this resource to learn how to turn off my GPS location/geolocation services while using apps.
- I can choose to keep my password information to myself and myself only.
- I can stop engaging or communicating with an abuser across all platforms.
- I can block him/her on all social media and messaging apps.
- I can have friends report their page.
- I can save and keep track of any abusive, threatening, or harassing comments, posts, or texts.
- I can change my passwords, usernames, email addresses or phone number if I need to.
- I can access a computer with a different IP address when necessary to avoid being tracked.
- I can take time away from social media if it becomes too triggering.
- I can look into getting a protection order against them.

Staying Safe Emotionally:

My abuser often makes me feel bad by doing this online:

When my abuser does this, I will stay safe by:

I will do things I enjoy like:



During an emergency or if I feel confused, scared, or depressed, I can call the following friends or family members:

Name: _____

Phone: _____

Name: _____

Phone: _____

Name: _____

Phone: _____

Name: _____

Phone: _____

I Can Also Contact These Organizations For Help:

For Emergencies



www.loveisrespect.org
Text: LOVEIS to 22522



Because Everyone Deserves a
Healthy Relationship

<https://www.breakthecycle.org/>

Police Station:

Phone: _____

Location: _____

Health Center:

Phone: _____

Location: _____

Women's or LGBTQ Center:

Phone: _____

Location: _____

Local Free Legal Assistance:

Phone: _____

Location: _____

I Can Report Abuse Online!



- You may encounter abusive content on Facebook in your timeline, or in ads, events, groups, messages, pages, photos, videos, or other posts.
- The best way to report abusive content on Facebook is by using the “Report” button that appears next to the content itself.
- You can also block¹ the abusive user.
- Click here² for more information on how to report different types of abusive content on Facebook or fill out this form.³

- Abuse can happen over Instagram too. The app has a guide⁴ for what to do if you are experiencing abuse.
- Click here⁵ to learn how to report abuse over Instagram or fill out this form.⁶
- To block another user that is abusing you, follow this link.⁷



- If you see inappropriate conduct on Snapchat, you can click here⁸ to report it.
- There are also ways you can report on Snapchat harassment, spam,⁹ a hacked account,¹⁰ or other safety concerns you may have.¹¹

¹ <https://www.facebook.com/help/168009843260943>

² <https://www.facebook.com/help/reportlinks>

³ <https://www.facebook.com/help/contact/274459462613911>

⁴ <https://help.instagram.com/527320407282978>

⁵ <https://help.instagram.com/165828726894770>

⁶ <https://help.instagram.com/>

⁷ <https://help.instagram.com/426700567389543>

⁸⁻¹² <https://support.snapchat.com/en-US/i-need-help>

I Can Report Abuse Online!



- To report someone engaging in abusive behavior on Twitter, click [here](#).¹³ To block that person, click [here](#).¹⁴
- To report account impersonation, click [here](#).¹⁵

- If you experience abusive behavior on Tumblr, you can report it by clicking [here](#).¹⁶
- If you're being harassed on Tumblr, click [here](#).¹⁷
- To block another user, click [here](#).¹⁸



- Youtube has a form you can fill out if you experience abuse or feel content is unsafe.¹⁹
- For more information on how to report abuse on Youtube, click [here](#).²⁰

¹³ <https://help.twitter.com/forms/abusiveuser> ¹⁴ <https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts> ¹⁵ <https://help.twitter.com/forms/impersonation> ¹⁶ <https://www.tumblr.com/abuse>
¹⁷ <https://www.tumblr.com/abuse/harassment> ¹⁸ <https://tumblr.zendesk.com/hc/en-us/articles/231877648-Blocking-users> ¹⁹ <https://www.youtube.com/reportabuse>
²⁰ <https://support.google.com/youtube/answer/2802027?hl=en>

CASE STUDIES



TABLE OF CONTENTS:

- Elena and Taylor
- Jess and Ash
- Cameron and Tiana

Produced by:



The Cyber Abuse Project was supported by Grant No. 2016-TA-AX-K070 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Elena and Taylor

Elena and Taylor are both 15 years old. They dated for almost a year. Early on in their relationship, Taylor pressured Elena to let him take nude photos of her. Later, Taylor pressured Elena to send more nude photos. Taylor also abused Elena physically during the relationship. Elena ended the relationship, but Taylor did not accept that. Taylor shared a nude picture of Elena with other teenagers over direct message on Instagram. Elena heard Taylor has done this before and bragged that he can do it without getting in trouble.

Q: What kind of cyber abuse has occurred here?

A: This is an example of revenge porn, a subcategory of nonconsensual sharing of intimate images. Taylor posted the nude image of Elena without her consent when Elena ended the relationship, which is one common scenario under which the nonconsensual sharing of intimate images occurs.

Q: What recourse is available to Elena?

A: 40 states and the District of Columbia have enacted laws specifically criminalizing nonconsensual sharing of intimate images, and 9 states have civil nonconsensual sharing of intimate images laws, so depending on Elena's state, Taylor's behavior may be a criminal act on its own. Depending on the state in which Elena and Taylor live, criminal harassment, stalking, or child pornography laws also may apply to Taylor's conduct. If Elena took the photos herself, she likely owns the copyright to the image Taylor posted and could potentially send a takedown notice to the social media platform requesting that the image be removed under the Digital Millennium Copyright Act (DMCA). The DMCA provides a mechanism through which copyright holders can request that social media platforms and other websites remove content that belongs to the copyright holder. Elena could also likely file a petition for a domestic violence restraining order. Most state laws regarding dating and domestic violence would apply, given both Taylor's physical abuse of Elena and the more recent harm done by his distribution of the photo.

Q: What kinds of evidence could you help Elena collect?

A: You can help Elena collect any screenshots that she has of the photo that Taylor shared. If possible, ensure that the screenshots include information that can be used to identify Taylor as the sender. For example, a screenshot of a social media message with Taylor's name and profile picture included would likely be sufficient to positively identify Taylor as the sender. Help Elena think through ways to store this evidence securely and privately, whether that is by giving printouts to a friend or by saving screenshots to a cloud service.

Q: What are some other ways to support this young person?

A: The best way to support Elena is to take her situation seriously and help her create a safety plan. Additionally, think through possible outcomes with Elena before pursuing a course of action as there may be unintended consequences of some courses of action. In this Break the Cycle case, Elena ended up dismissing her petition for a civil protection order out of fear that Taylor would distribute the image more widely if she pursued the order. Break the Cycle carefully explained to Elena that a protection order or future criminal penalties unfortunately could not remove her image from the internet or prevent further sharing from downloads that had already occurred. In other words, in some cases the damage has already been done when a young person reaches out for help. It is important to discuss the pros and cons thoroughly with your client and of course let them decide how to proceed. Elena may also benefit from connections with other services, such as counseling, to help her deal with both the physical and cyber abuse she experienced.

RESOURCES

Sample DMCA Take Down Notice
Cyber Abuse Safety Plan
Digital Evidence Collection Guide
Protection Orders 101
Protection Orders: Special Considerations for Minors

Jess and Ash

Jess is 16 years old and dated Ash off and on for a couple years. During that time, Ash physically abused Jess. Jess is afraid that Ash is cyber-stalking her. Once, Ash clicked around on Jess's computer, and showed Jess how easy it is to figure out Jess's password based on metadata. Jess believes Ash has figured out all of her passwords. (Recently, Jess tried to end the relationship with Ash, and then Jess's gmail account was deleted.) Jess also believes Ash has been monitoring her phone or computer. The other day Jess said something on the phone to a friend about a specific topic. A short while later, Ash texted Jess about the same topic using Jess's words. Also, Ash has been showing up when Jess is out. Jess suspects Ash is tracking her with GPS. Jess has let her phone battery die and is afraid to charge it, thinking Ash could find Jess's location or learn other information about Jess. Jess has also changed all passwords and created a new email account.

Q: What kind of cyber abuse has occurred here?

A: This is an example of cyber-stalking. As is true in many cases, the cyber-stalking Ash is perpetrating against Jess (monitoring her devices and hacking int

Q: What recourse is available to Jess?

A: Jess could obtain a domestic violence restraining order in most states because most states define cyber-stalking as a crime. (Additionally, Ash physically abused Jess during the relationship.) A civil protection order could require Ash to cease all communication with Jess, including via the internet. State criminal stalking statutes normally define stalking as repeated behavior intended to cause harm or fear. Most states have expanded definitions to include online stalking or communication via the internet, e.g., stating that the repeated behavior can be in person "or by any means." Some states have separate cyber-stalking statutes that criminalize this behavior. Turning to federal law, the Violence Against Women Act includes the Interstate Stalking Punishment and Prevention Act, 18 USC 2261(A)(2), which prohibits harassment and intimidation in interstate commerce and does not require direct communication with the victim (but would require the stalking to occur across state lines). If Jess and Ash resided in different states, this would be applicable.

Q: What kinds of evidence could you help Jess collect?

A: You could help Jess collect screenshots of any contacts she has with Ash, especially the text message Ash sent her that suggests Ash is monitoring Jess's phones. Jess could also start keeping a log of stalking incidents that records the date, time, location, and what happened during each incident. A log like this makes it easier for Jess to present a clear narrative about her situation, and can also be helpful for remembering incidents that happened some time ago. Clear narrative reporting can be challenging for clients who have experienced trauma. You also could suggest that Jess give evidence, especially electronic evidence, to a trusted person for safekeeping since it is likely that her devices are not secure.

Q: What are some other ways to support this young person?

A: You could help Jess obtain a new phone so she has access to a device that Ash does not know about or have access to. Free phones are available through the Federal Communications Commission's Lifeline program if Jess is income eligible. Some domestic violence programs offer phones free to victims as well. You could also help Jess safety plan so that she has a system for letting people know where she's going or bringing someone with her when she goes out. Another element of Jess's safety plan could include asking her friends not to tag her on any social media posts or pictures to make it more difficult for Ash to find Jess's location online.

RESOURCES

Cyber Abuse Safety Plan
Digital Evidence Collection Guide
Protection Orders 101
Protection Orders: Special Considerations for Minors

Cameron and Tiana

Tiana is 21 years old. Her ex-boyfriend, Cameron, is 23. They met in college and dated for about 3 years. After Tiana ended the relationship, Cameron refused to stop contacting her by email, text message, and Snapchat. Sometimes Cameron would insult or threaten Tiana. At other times, he sent her long romantic messages. Snapchat does not keep a record of conversations, but Tiana took screenshots of the messages before they disappeared. Tiana told Cameron to stop contacting her, and she blocked Cameron. Unfortunately, Cameron found other ways to contact Tiana. For example, Cameron sent Tiana money through Square Cash on several occasions. The app allowed Cameron to write messages to Tiana in the memo field. On her birthday, April 18th, Cameron sent Tiana \$4.18. All Cameron needed was Tiana's phone number to make these payments. Tiana had to delete her app, even though she used it to exchange money with friends and family.

Q: What kind of cyber abuse has occurred here?

A: This is an example of cyber harassment or cyber-stalking. Cameron is repeatedly engaging in threatening behavior towards Tiana using technology.

Q: What recourse is available to Tiana?

A: A domestic violence protection order is probably Tiana's best option. Because some state criminal harassment statutes require physical proximity, whether they apply to cyber harassment like this will be highly state-dependent. If Tiana and Cameron live in different states, the Interstate Communications Act and/or the Telephone Harassment Act might apply depending on the severity of the behavior. The Interstate Communications Act prohibits people from communicating threats to others across state lines. The Telephone Harassment Act prohibits abusive, harassing, or threatening communication through a telecommunications device across state lines.

Q: What kinds of evidence could you help Tiana collect?

A: Since Tiana has already taken screenshots of the Snapchat messages Cameron was sending her, you can help her organize them to make it easier for a judge to understand what occurred. You can also encourage her to take screenshots of the other ways Cameron contacted her, such as email and the Square Cash app, if she has not done so already. You can offer to store the evidence for her if she does not feel she can keep it safe and private on her own, or suggest that she ask a trusted friend or family member to do so.

Q: What are some other ways to support this young person?

A: You can help Tiana create a safety plan that addresses this specific type of cyber-stalking. Additionally, helping Tiana access a new phone (see above case study) that the abuser has no knowledge of could also provide support. If she cannot obtain a new phone, help Tiana change her phone number so that she can use the Square Cash app safely. Tiana may also benefit from connections to other forms of support, such as mental health counseling that can help her deal with the cyber abuse she experienced.

RESOURCES

Cyber Abuse Safety Plan
Digital Evidence Collection Guide
Protection Orders 101
Protection Orders: Special Considerations for Minors