



Digital Safety Toolkit

Practical Tools to Prevent and Mitigate
Technology Facilitated Abuse



Page of Contents

1	Funding Acknowledgment
2	What is Digital Abuse?
3	Types of Digital Abuse
5	iPhone Safety
6	Android Safety
7	Stop NCII Image Removal Tool
9	PC & Laptop Safety
10	Resource Guide
11	References & More Information



Funding Acknowledgement

This publication was supported by Grant No. 15JOVW-22-GG-00914-MUMU awarded by the Office on Violence against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in the publication are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

What is Digital Abuse?



Digital Abuse, also known as Technology-facilitated Abuse, is any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools which results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms (NNEDV).

The impact of this abuse is significant and can be lifelong. Similar to other forms of abuse, victim-survivors experience higher rates of anxiety, depression, and suicidal ideation than their peers who have not faced digital abuse.

Anna Marie Chavez

CEO OF GIRL SCOUTS USA

“Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm.”

Types of Digital Abuse

Blackmail

Internet blackmail is a form of cybercrime where scammers and blackmailers manipulate individuals through emotional tactics to exploit their trust. They often threaten to expose explicit or embarrassing content unless their demands are met (Norton).

Coercive Control

Now known more formally as Technology-Facilitated Coercive Control, this type of abuse focuses on physical and digital control of devices by the perpetrator that are known to the victim-survivor.

Cyberstalking

Cyberstalking involves the use of technology (most often, the Internet) to make someone else afraid or concerned about their safety. Generally speaking, this conduct is threatening or otherwise fear-inducing, involves an invasion of a person's relative right to privacy, and manifests in repeated actions over time. Most of the time, those who cyberstalk use social media, Internet databases, search engines, and other online resources to intimidate, follow, and cause anxiety or terror to others (CRC).

Types of Digital Abuse

Cyberbullying

Cyberbullying occurs when someone uses technology to demean, inflict harm, or cause pain to another person. It is “willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices (APA).”

Hacking & Tampering

Hacking the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Device tampering takes the abuse one step further when the perpetrator uses their illicit access to a victim-survivor’s technology to do things such as change temperature settings, lock or unlock doors, set off security alarms, and even disable moving vehicles.

Image-Based Abuse

Nonconsensual intimate image abuse (or NCII) is any intimate content that was made public without consent of the person in the frame (Stop NCII).

iPhone Safety

1. Accessing Safety Features

From your iPhone home page, Select “Settings” > “Privacy & Security”. This page allows you to access all available security settings and features available on your device. For a step-by-step visual guide, click [here](#).

2. Location Services

From your iPhone home page, select “Settings” > Privacy & Security” > “Location Services”. This page allows you to view if you have Location Tracking on, what apps you are sharing your location with and when, and who you are sharing your location with. Apps are allowed to track your location based on permissions you set. These permissions are “Always”, “Never”, “While Using App”, and “When Shared”. You can change these permissions for each app by selecting the app’s icon under the “Location Services” Page. To view who you are sharing your location with, from the “Location Services” page select > “Share My Location”. Any contacts you are currently sharing your location with will appear here. While you can change location sharing for each person, please note that the person will be notified via text that you have stopped location sharing. To avoid these notifications being sent, simply toggle off the “Share My Location” button on the “Location Services” page. For step-by-step visual guides, click [here](#).

3. Tracking

From your iPhone home page, select “Settings” > “Privacy & Security” > “Tracking”. This page allows you to view what apps are tracking your activity across other websites and applications. At the top of this page you can toggle on or off “Allow Apps to Request To Track”. If this button is toggled on, you will receive notifications from apps asking if they can track your information across sites, which can either approve or deny. If this button is toggled off, these requests will automatically be denied. For a step-by-step visual guide, click [here](#).

4. Safety Check

From the iPhone home page, select “Settings” > “Privacy & Security” > “Safety Check” at the bottom of the page. This page allows you to review and manage access that individuals and applications have to your device in a quick, effective manner. Safety Check also allows you to “emergency reset” all sharing & access preferences at once in the event of an emergency. This page also features a quick exit button that closes the page window sends you back to your home page immediately when pressed. For a step-by-step visual guide, click [here](#).

5. Lockdown Mode

From the iPhone home page, select “Settings” > “Privacy & Security” > “Lockdown Mode” at the bottom of the page. This page allows you to completely lockdown your phone in the event of extreme cyber-based attacks. Once in Lockdown mode, apps and websites will function with extreme limitations for your safety and to limit the flow of information to or from your device. For a step-by-step visual guide, click [here](#).



1. Accessing Safety Features

From your Android home page, select “Settings” > “Privacy” for privacy or select “Settings” > “Security” for security settings. This page allows you to access all available security settings and features available on your device. For a step-by-step visual guide, click [here](#).

2. Location Services

From your iPhone home page, swipe down from the top of the screen. Select “Location” > “App Location Permissions”. This page allows you to see what apps you are sharing your location with and when. You can also change the access level each app has to your location from this page. To view and manage who has access your location, from the Location page, select “Location Services” < “Access to My Location”. This button can be toggled on or off. When it is on, everyone you have shared your location with can locate you in real time. When it is off, no one will be able to see your location. For a step-by-step visual guide, click [here](#).

3. Emergency SOS

From your Android home page, select “Settings” > “Safety & Emergency” > “SOS”. Select “Start Setup”. Set an emergency number for your phone to call by selecting “Start”. To allow an emergency contact to view your location when SOS is enabled select “Start Setup” > “Setup”. You will be asked what information you want to share with your emergency contact. Select “Next” > “While Using App”. This will allow your phone to access your location when SOS is enabled. To turn on emergency recording when SOS is enabled, return to “Start Setup” and select > “Turn On” > “While Using App”. To automatically send the emergency recording to your emergency contact, select “Share Automatically” > “Next”. To activate SOS, simply touch and hold the SOS icon on your home screen. For a step-by-step visual guide, click [here](#).





Stop NCII Intimate Image Search Removal Tool

Before an Image is Shared

1

Create A Case

Visit www.stopncii.org and select "Create a Case". You will be prompted to provide personal information about yourself, as well as information about the photos or videos you are concerned about.

2

Image Scanning

Once your case has been created, you will have access to the secure StopNCII platform. Utilizing the platform, select photo or videos in question to be scanned. Please note, these photos and videos will never leave your phone, nor will StopNCII staff see them or save them.

3

Hash Creation

Three scans of your photo or video creates a digital "hash" or barcode. Any duplicates of these images or videos now contain that digital hash.

4

StopNCII Hashbank

The digital "hash" or barcode is then uploaded to StopNCII's "hashbank" which is shared with participating websites and programs. These participating websites include Facebook Instagram, and Bumble.



Stop NCII Intimate Image Search Removal Tool

After an Image is Shared

1

Image Identification

If an image or video that has been “hashed” appears on a participating website or program, it is flagged and automatically submitted for removal.

2

Notification

Both the victim-survivor and StopNCII staff will be notified an image has appeared.

3

Image Removal

If the image meets criteria for removal, it will be removed from the website(s) in question. Both the victim-survivor and StopNCII staff will be notified that the image has been removed.

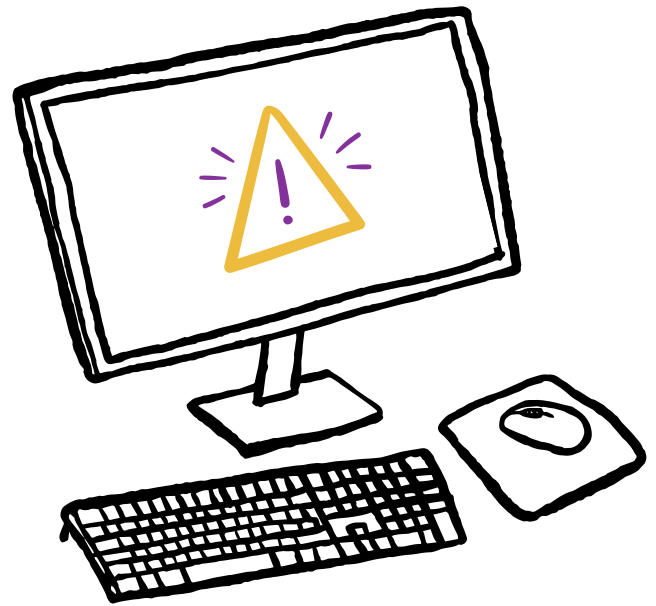
4

Continued Monitoring

The image removal tool will continue to monitor for “hashes” until a victim-survivor requests the hashes be removed.

PC & Laptop Safety

Virtual Private Networks, Antivirus Software, and Firewalls are all excellent methods to protect your PC or laptop. These cybersecurity tools are most effective when someone is the victim of hacking, device tampering, or identity theft. While these tools are similar, it is important to do research on which of them is best suited to your needs. NCEDSV does not endorse any particular brand of VPN, Antivirus, or Firewall. Rather, consumers should make an educated decision on what product to use through research and advice from IT professionals.



Installing VPN

From the home screen of your computer, select “Settings” > “Network & Internet” > “VPN” > “Add a VPN”. You will then be prompted to add information on the VPN product you are using. After completing this step select “Save” and exit settings.

Enabling Firewall

From your computer’s home screen, select “Settings” > “Control Panel” > “Firewall”. If the button for “Firewall” is toggled on, it is already enabled and functioning. If the button is toggled off, select “Enable Firewall”. After enabling Firewall, select “Save” and exit settings.

Installing Antivirus Software

Start by selecting the antivirus software you would like to use or purchase. Then, follow installation prompts to install the software. Next, activate the software. Usually this is done by entering an activation code or key given to you after purchase. After the software is installed, from your home screen select “Settings” < “Apps” > “Apps & Features” > the name of your antivirus software. Here, you can change settings such as notifications and automatic updates. After finishing changing settings, exit settings. The Antivirus software should now scan your computer on a regular basis.



Resource Guide

Name	Contact	Resource Type
Safety Net Project	www.techsafety.org	Training, technical assistance, and toolkits on the intersection of technology and IPV
National Network to End Domestic Violence	Youtube Playlist	Online privacy & safety instructional video series
Stop NCII	www.stopncii.org	Intimate image search removal tool
Cyberbullying Research Center	www.cyberbullying.org	Information and education on cyberbullying & cyberstalking
National Cybersafety Alliance	www.staysafeonline.org	Educational resources on all things cybersafety
iPhone User Guide	User guide here	Full user guide for iPhone & related devices
Android User Guide	User guide here	Full user guide for Android & related devices
Windows User Guide	User guide here	Full user guide for Windows operating system
Mac User Guide	User guide here	Full user guide for Mac operating system



References & More Information

- ✓ Cisco
- ✓ NNEDV
- ✓ Stop NCII
- ✓ Cloudflare
- ✓ Safety Net
- ✓ Norton Anti-Virus
- ✓ The New York Times
- ✓ Cyberbullying Research Center
- ✓ American Psychological Association

