Glossary of Digital & Technology-Facilitated Abuse Terms

calan dvs™

Providing sanctuary.
Inspiring change.

bright options

Digital and Technology Facilitated abuse glossary of terms

Term	Description
Account Takeover	When someone gains unauthorised access to another person's online account (email, social media, banking, etc.), often to monitor, impersonate, or control them.
Air Tag / Tracking Device Abuse	The misuse of Bluetooth trackers, GPS devices, or apps to secretly monitor a person's location without their knowledge or consent.
Coercive Control (Digital)	A pattern of behaviors using technology to dominate, monitor, isolate, or regulate another person's daily life.
Cyberstalking	Repeated, unwanted monitoring, harassment, or threats using digital tools such as social media, email, GPS tracking, or spyware.
Cyber harassment	Ongoing online behavior meant to intimidate, shame, threaten, or silence someone.
Doxxing	The public release of private or identifying information (such as address, phone number, workplace) without consent, often to intimidate or endanger someone.

Deepfake Abuse	The use of AI-generated images, videos, or audio to falsely depict someone in sexual, criminal, or compromising situations.
Electronic Surveillance	The monitoring of someone’s communications, location, or digital activity without their consent.
Extortion (Digital)	Threatening to release private, sexual, or harmful content to force someone to comply with demands (also called sextortion when sexual images are involved).
GPS Tracking Abuse	The non-consensual use of location services, apps, or devices to monitor someone’s movements.
Hacking	Gaining unauthorised access to someone’s device or online accounts.
Harassment by Proxy	Using other people (friends, followers, family) or online forums to harass or threaten someone.
Impersonation	Pretending to be someone else online to damage their reputation, access private information, or manipulate others.

Non-Consensual Distribution of Intimate Images (NCDII)	Sharing or threatening to share nude or sexual images or videos without consent. Often called image-based abuse or revenge porn.
Online Grooming	Building trust with someone online (often a minor) to exploit, manipulate, or sexually abuse them.
Password Abuse	Forcing someone to share passwords, guessing passwords, or using stolen login information to maintain control.
Photo/Video Surveillance Abuse	Using smart cameras, baby monitors, webcams, or hidden recording devices to spy on someone.
Sextortion	Blackmail using sexual images, videos, or threats of exposure to control or exploit someone.
Smart Home Abuse	Misuse of connected devices (thermostats, lights, locks, speakers) to frighten, punish, control, or surveil someone.

Social Media Monitoring	Excessive tracking of someone’s posts, likes, friends, messages, or activity to control or intimidate them.
Spoofing	Disguising communication so it appears to come from a trusted source (phone number, email, or account).
Spyware / Stalker ware	Hidden software installed on a device to secretly monitor calls, texts, locations, keystrokes, or camera use.
Technology-Facilitated Sexual Violence (TFSV)	Any form of sexual harm that involves digital tools, including image-based abuse, deepfake pornography, sextortion, and online sexual exploitation.
Two-Factor Authentication (2FA)	A security feature that requires two forms of identity verification to access an account (often used as a safety strategy).
Victim-Blaming in Digital Abuse	Holding the targeted person responsible for abuse because of their online behavior (e.g., “they shouldn’t have sent the photo”).
Youth digital exploitation	The use of technology to exploit minors through grooming, sexual content, coercion, threats, or trafficking.