

# Parental controls

## Securing devices and accounts

- Change passwords
- 2-Factor and multi-factor authentication
- Checking for access/connected devices such as Google, iCloud, and Apple ID accounts
- Consider separate tech devices for each household

## WiFi Router

- Use WiFi router or ISP setting to control access to WiFi
- Some ISP also have parental control features
- Turning off WiFi router after hours

## Device

- Use built-in parental control features on devices
- Turn off location services on both the device and the apps
- Regularly check apps on the device if it travels between households to make sure additional tracking apps aren't added
- Require devices to be on charge after hours
- Restrict access to technology

## Parental control apps

- Install parental control software to monitor or restrict access

## Other options

- If the harassment or threats from the perpetrator are coming through the child's devices, consider blocking them
- Consider replacing devices if the device has been compromised
- Consider making new email and online accounts that can't be accessed by the abusive parent

# Who to report to?

## Police

Report and provide the digital evidence of tech abuse and/or breaches of protection orders via tech

## Child Protection

Report abuse or threats of abuse towards the child by the abusive parent

## eSafety Commissioner

Report incidents of serious online abuse or illegal and restricted online content including cyber bullying, image-based abuse, material showing or encouraging child sexual abuse, or other material showing or encouraging other violent crimes

Reports can be made online

## Before reporting

Consider the safety of yourself and your children

Send copies of screenshots and photos to a secure device or email in case something happens to your device

## Contact us

Macarthur Women's Domestic Violence Court  
Advocacy Service  
Ph: (02) 4640 7333

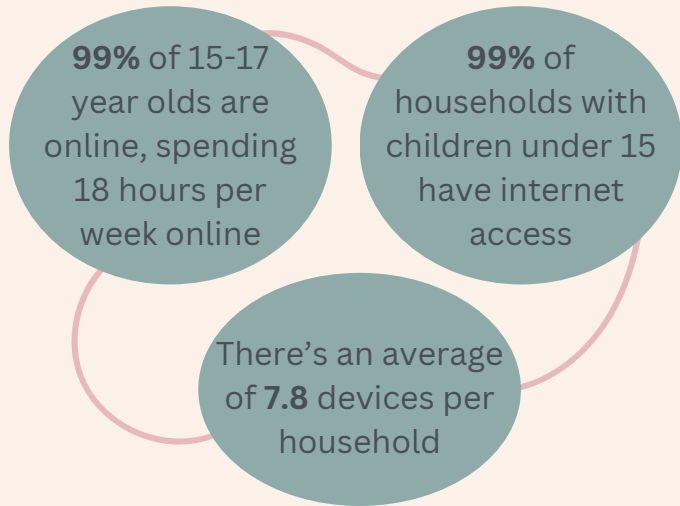
Information originally compiled from WESNET's 6th  
Technology Safety Summit  
For more information, visit: [techsafety.org.au](http://techsafety.org.au)

# Tech Abuse

## Safety for Children and Adolescents Online

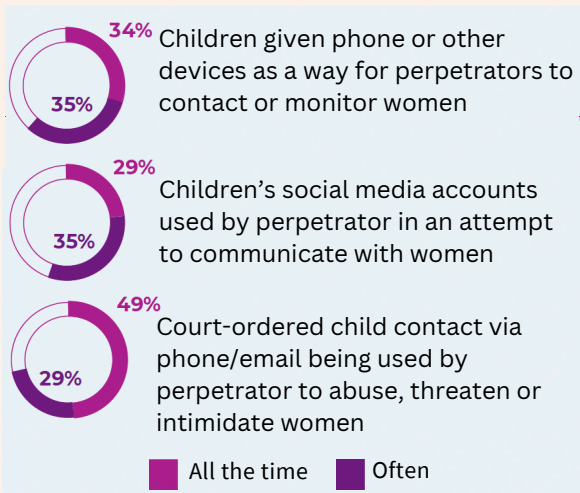


## The Stats



## The Tactics

### Impersonation and the use of children



Source: Wesnet's 2nd National Survey on Technological Abuse and Domestic Violence

# Tech abuse affecting children

### MONITORING AND STALKING

- Using tech to find new home location
- Using tech to ask child about non-abusive parent's activities or location
- Asking child for non-abusive parent's new phone number
- Using child social media to track their activities

### IMPERSONATION

- Using tech to pretend to be a friend of the child
- Using tech to pretend to be a child victim (to implicate non-abusive parent)

### SEXUAL ABUSE

- Failing to prevent child accessing sexual images
- Other types of sexual exploitation of children
- Purposely exposing child to sexual images
- Sharing child sexual abuse material of child using tech

### OTHER TYPES OF TECH ABUSE

- Using emotional blackmail to manipulate children
- Making false claims to overseas family members

### BLOCKING CHILDREN'S COMMUNICATIONS

- Blocking comms between non-abusive parent and child
- Prohibiting child from using tech
- Destroying child's tech
- Changing passwords on child's accounts to prevent access

### THREATS AND INTIMIDATION

- Insulting parent where child can see
- Using tech to send child messages that insult non-abusive parent
- Demanding child answer calls and texts immediately
- Threatening to take child away

### BYPASSING CYBERSECURITY

- Installing stalkerware to monitor child's tech
- Forcing child to log in to device
- Coercing child to share passwords

### CO-OCCURRING ABUSE

- Financial abuse
- Blocking parental communications
- Co-occurring impersonation
- Co-occurring threats