

DOMESTIC ABUSE RESOURCE

TECHNOLOGY-FACILITATED ABUSE

Do not focus only on “spyware.” Technology abuse often comes from ordinary features - shared accounts, location sharing, cloud access, family plans and password recovery - being used without genuine consent.

■ WHAT IT IS

Technology-facilitated abuse uses phones, accounts, location services, connected devices or online platforms to monitor, harass, impersonate, threaten or control another person.

LOOK FOR THE PATTERN

Ask four questions: Who has access? What can they see? How did they get access? What happens when you try to set a digital boundary? Repeated unexplained access may be part of a broader pattern even if no malicious software is found.

■ THREE SIGNALS WORTH NOTICING

REPEATS

It keeps happening.

ESCALATES

The impact or consequences grow.

RESTRICTS

Freedom, safety or choice gets smaller.

A single incident can be confusing. Repetition, escalation and reduced freedom are often what make the wider pattern easier to see.

THE BIGGER PICTURE

One incident can be confusing. The pattern shows what life is becoming.

CONTINUE → WHAT IT CAN LOOK LIKE

RECOGNIZE THE BEHAVIOR

WHAT IT CAN LOOK LIKE

These examples are not a checklist or a diagnosis. The context matters: frequency, fear, consequences, escalation and whether one person is losing ordinary freedom or choice.

- Demanding passwords, passcodes or access to messages and social media.
- Installing monitoring software or configuring devices so activity can be viewed remotely.
- Using location sharing, vehicle systems, trackers or connected devices to monitor movement.
- Impersonating someone online or posting in their name.
- Accessing email, cloud storage, photos or social accounts without permission.
- Threatening to share intimate images, private messages or personal information.
- Using account recovery methods to regain access after passwords are changed.
- Using smart-home cameras, doorbells, speakers, thermostats or security systems to watch or intimidate.

■ READ THE BEHAVIOR IN CONTEXT

ONE EVENT

Ask what happened in that moment and whether there was fear, force, pressure or intimidation.

THE PATTERN

Then ask what has been happening across weeks or months, especially when the other person resists or says no.

The useful question is not only “Did this happen?” It is “What does this behavior do to the other person over time?”

THE BIGGER PICTURE

Context matters. Notice what happens when a boundary is set.

CONTINUE → PATTERNS TO NOTICE

SEE THE WHOLE PICTURE

PATTERNS TO NOTICE

Patterns are often easier to recognize when you stop judging each incident separately. Look at what repeats, what escalates, what creates fear and what choices are gradually disappearing.



The person knows where you have been or who you contacted without an obvious explanation.



You feel required to keep location sharing on or hand over your phone for inspection.



You receive unfamiliar login alerts, password resets or device notifications.



Digital monitoring is combined with jealousy, accusations, isolation or stalking.



Privacy settings seem to change after you update them.



Attempts to regain privacy lead to anger, threats or escalation.

■ WHY IT MATTERS

Phones and accounts travel with us, which can make digital monitoring feel constant. Abruptly removing access or suspected trackers can sometimes alert the person, so safety planning may be more important than immediately changing every setting.

MYTH

“If you have nothing to hide, you should share your passwords and location.”

REALITY

Privacy and digital boundaries are normal parts of healthy relationships. Consent to share access can also be changed.

Healthy relationships can include conflict, mistakes and disagreement. The concern is a repeated pattern that creates fear, removes autonomy or changes behavior through pressure or control.

THE BIGGER PICTURE

Look at the pattern: what repeats, escalates or changes behavior?

CONTINUE → CASE STUDY & PRACTICAL STEPS

ANONYMOUS COMPOSITE EXAMPLE

CASE STUDY

This composite combines common patterns and is written to protect privacy. It is not presented as one identifiable person or investigation.

A person noticed that their partner seemed to know where they had been and who they had spoken to, even after a password change. They focused on the phone and assumed there must be spyware. Later, they realized their partner still had access to a shared cloud account, a family mobile plan, location services and an old recovery email. A tablet connected months earlier was also still receiving synchronized messages. Each incident had looked like a technical glitch. Together, they showed a much wider system of access and monitoring.

■ WHAT TO NOTICE



Technology-facilitated abuse often involves ordinary features and shared accounts, not sophisticated hacking.



Changing one password may not end access if other devices, recovery methods, cloud services or family plans remain connected.



The pattern is the repeated loss of privacy, autonomy or safety through technology.

■ IF THIS IS HAPPENING

- Use a safer device or account to seek help if you believe your regular technology may be monitored.
- Before removing trackers or changing major access, consider whether the change could alert the person or increase risk.
- When safe, review recovery emails, two-factor authentication, connected devices, location sharing and shared plans.
- Preserve screenshots, login notices and unusual account activity if they may be useful later.
- Consider specialist technology-safety or domestic violence support if the access is complex or connected to stalking.

FINAL TAKEAWAY

You do not need to explain away every incident before you are allowed to take a pattern seriously. Notice what repeats, what changes your behavior, and what happens when you set a boundary.