# **What *must* we do to get victims to report cybercrime to law-enforcement?**

The main reasons people do not report cybercrime to the police are:

* Victims are unsure if what they experienced was actually a crime;
* Victims don’t know what their options are for reporting;
* Victims are disappointed or feel let-down by law enforcement.

**We can prevent the above by doing the following:**

* **Provide a clear definition of what a cybercrime is.**

… Or what types of cybercrimes will be accepted and processed within the system.

Reassure people that they are in the right place to report a scam, an online fraud, online harassment, etc.

Provide examples of what kinds of cybercrimes can be reported.

* **Provide a clear definition of what evidence is.**

People do not know what police need in order to solve a crime or launch an investigation. They do not know what to share or how to acquire this information. Use non-technical explanations to describe evidence.

Provide examples of evidence. Provide directions on how to find evidence.

Make it easy to share evidence.

* **Ask specific questions.**

When people are upset or confused, they are not able to provide details of a crime unless the question is specific and comprehensible.

* **Set clear expectations for what will happen after victims submit a report.**

People expect the police to immediately investigate them, identify a suspect, or interview them. People expect the police to solve the problem and get their money back.

If follow-up is not likely then this must be made clear to users. The service must be clear about who will be receiving the reports, and for what purpose.

* **Give victims next steps to protect themselves and seek help.**

Victims call police stations, or visit in-person to follow-up on reports. They seek advice and clarity on what has happened to them.

Provide guidance on what victims can do to a) protect themselves b) seek support outside of police and law-enforcement agencies.

* **Set clear expectations throughout the flow (ie. from page to page, section to section, etc.)**

Prep people on what they will need to prepare and provide. Make it clear how many steps they will need to complete in order to submit a report.

* **Use language that provides emotional reassurance.**

If language makes people feel like they did something wrong, victims will not share crucial details about their experience with police.

If language or the tone of the language makes people feel isolated or ashamed, they will not complete the entire form because they will be overwhelmed or upset.

* **Use plain language that provides clarity.**

Do not use legal, policy-driven definitions of cybercrime, online harassment, evidence, and fraud because they are vague, unclear, or simply unknown to the people who experience these crimes on a daily basis.

If language is not people-friendly, victims will not be able to understand why they are reporting, or how to report.

* **Reassure victims that this is not a scam.**

People are likely to suspect an online tool as a scam or trap. Do not use casual language. Balance clarity with officiality.

* **Make this service accessible where people already report cybercrimes and seek help.**

Victims of cybercrime tell us that they call 911 or visit police stations in-person after experiencing a cybercrime.

The design of this service must be universally accessible at all points of the reporting service. Police, front line staff, victim services, and service providers (private sector orgs) must all be able to refer victims to this service where appropriate.