

Інформаційна безпека під час війни

Інформаційний простір дозволяє бути на зв'язку з рідними, дізнаватись останні новини з фронту, хоч якось контролювати те, що відбувається навколо. Для дітей та підлітків інтернет залишається світом розваг та спілкування з друзями. Але важливо пам'ятати, що за позначкою геолокації на пості чи фотографії, веселим відео в соціальній мережі чи одним повідомленням може ховатися справжня небезпека. Особливо під час війни, коли інфпростір використовують окупанти для військових нападів на українські міста.

Як можуть захистити батьки, педагоги себе та дітей в інформаційному просторі під час війни?

Актуальні правила поведінки в інформаційному просторі, своєрідна покрокова інструкція Чого не робити в жодному разі:

- ⊗ Якщо хтось із користувачів у мережі просить приватну інформацію (особистий номер телефону чи номер батьків, де батьки працюють, де родина зараз перебуває, яка ситуація в місті, де розміщується військова техніка в місті чи військові об'єкти) — таку інформацію в жодному разі не можна передавати. Навіть якщо це онлайн-друг, якого дитина знає в реальному житті. Адже зараз дуже часто особисті профілі зламують для отримання інформації або створюють фейкові профілі.
- ⊗ Не можна знімати розміщення та пересування військової техніки та військових у місті, де перебуває дитина. Оскільки окупанти можуть переглядати відкриті профілі українців для визначення місця розташування військових для подальшого нападу. А також злочинці можуть намагатися вести листування з дитиною для шантажу чи примушування до отримання інформації про розміщення техніки в місті.
- ⊗ Не знімати місця вибухів та потрапляння снарядів, оскільки окупанти можуть використовувати фото- та відеодані, які потрапили в мережу, для коригування подальшого нанесення вогню по місту.

⊗ Не переходити за невідомими посиланнями, які були надіслані в приватні повідомлення в будь-якій соціальній мережі чи месенджері. Адже за ними можуть ховатися хакерські атаки.

⊗ Якщо ви переглядаєте та обговорюєте новини з дитиною, варто переконатися в їхній правдивості. Усі новини, заяви високопосадовців та обмеження в містах краще повторно перевірити в офіційних каналах комунікації, на офіційних сайтах державних установ, в офіційних Telegram-каналах посадовців.

⊗ Якщо дитину автоматично додали до невідомих груп, важливо відписатися від них та заблокувати їх. А також розповісти про це дорослим.

⊗ Якщо до дитини хтось пише з проханням допомоги або виконати спеціальне завдання, важливо, щоб дитина повідомила про це дорослим. Варто разом зробити скріншот групи, повідомлень та через онлайн-форму звернутися до кіберполіції — <https://ticket.cyberpolice.gov.ua/>.

Варто також зробити:

⊗ Профіль дитини в соціальних мережах варто зробити закритим: щоб писати дитині, переглядати вміст її сторінки могли лише ті, кого дитина додасть у друзі.

⊗ Пам'ятайте, що все, що ми пишемо та публікуємо в мережі, навіть у приватних повідомленнях, назавжди залишається в інтернеті. Тому перед публікацією ще раз оцініть, чи може ця інформація будь-яким чином нашкодити вам або вашим близьким? А під час війни — нашим містам та захисникам?

З матеріалами сайту «Освіторія Медіа» та команди #stop_sexтинг

