Бориспільський ліцей «Патріот» Бориспільської міської ради Київської області

Інформаційна безпека під час війни

Україна – унікальна держава, яка знаходиться в епіцентрі подій першої в світі війни, коли інформаційний простір стає полем бою. Інформація для України – зброя, броня та інструмент впливу. Інформаційний простір став потужним «фронтом» боротьби, як зі сторони громадянського суспільства, так і по відношенню до державних органів влади.

Інформаційний простір дозволяє бути на зв’язку з рідними, дізнаватись останні новини з фронту, хоч якось контролювати те, що відбувається навколо. Для кожного з нас Інтернет залишається світом безмежної інформації, 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 інфопростір використовують окупанти для військових нападів на українські міста.

Актуальні правила поведінки в інформаційному просторі.

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 ви знаєте 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. Оскільки окупанти можуть переглядати відкриті профілі українців для визначення місця розташування військових для подальшого нападу. А також злочинці можуть намагатися вести листування з вами для шантажу чи примушування до отримання інформації про розміщення техніки в місті.

Актуальні правила поведінки в інформаційному просторі

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 друзями, 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.

Актуальні правила поведінки в інформаційному просторі

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

Якщо до вас хтось пише з проханням допомоги або виконати спеціальне завдання, важливо, щоб ви повідомили про це дорослим. Варто разом зробити скріншот групи, повідомлень та через онлайн-форму **звернутися до кіберполіції** — https://ticket.cyberpolice.gov.ua/

Як діяти онлайн під час війни?

Користуйтесь офіційними джерелами інформації, офіційними сторінками держслужбовців і органів місцевого самоврядування, а також читайте перевірені медіа.

У жодному разі **НЕ ведіться на рекламні дописи** в соцмережах із псевдосторінок СБУ чи інших державних відомств.

Поширюйте правду про війну, яку веде РФ проти України у соцмережах.

Підтримуйте "гігієну" своїх пристроїв: блокуйте пристрої щоразу після закінчення роботи; встановлюйте застосунки лише з офіційних сервісів; не користуйтеся невідомим Wi-Fi.

Захистіть свої соцмережі: встановлюйте складні паролі; не додавайте в друзі невідомі акаунти; увімкніть двохетапну автентифікацію.

Підтримуйте дух Збройних Сил України: пишіть слова подяки, підбадьорюйте українців.

Безпека у месенджерах: як захиститись від ворога онлайн?

Діліться конфіденційною інформацією лише з тими, кому ви довіряєте.

Перевіряйте, чи є людина, з якою ви розмовляєте, тою, за кого вона себе видає, зателефонувавши або попросивши голосове повідомлення.

Ніколи й нікому не надавайте коди підтвердження SMS – навіть якщо ви знаєте цих людей.

Налаштуйте "конфіденційність", щоб контролювати, хто може бачити вашу фотографію профілю та додавати вас до груп.

Двічі перевіряйте точність пересланих повідомлень.

Перегляньте історію листувань та членство в групах. **Розгляньте можливість очищення історії чату.**

Надсилайте скарги на будь-які контакти, які здаються шахрайськими, з яких надсилають погрози чи інші небезпечні повідомлення.

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?