

**Відокремлений структурний підрозділ
« Донецький фаховий коледж СНУ ім.В.Даля»**

**Інструкція № 9.
Інформаційна безпека в умовах воєнного стану.**

м. Дніпро

**Відокремлений структурний підрозділ
« Донецький фаховий коледж СНУ ім.В.Даля »**

ЗАТВЕРДЖЕНО

Наказ в.о директора

ВСП «ДФК СНУ ім. В. Даля»

Олена ВНУКОВА

03 січня 2025 р. № 35.01-03/7



**Інструкція № 9.
Інформаційна безпека в умовах воєнного стану.**

Актуальні правила поведінки в інформаційному просторі. Можливі ризики та чому правила інформаційної безпеки студентів під час війни особливо важливі

Через природну цікавість, довірливість і брак досвіду здобувач освіти (студент), сам того не усвідомлюючи, може завдати шкоди як своїй сім'ї, так і питанням безпеки країни в цілому. В умовах війни інформаційний фронт є максимально активним, зокрема він використовується для планування ворогом нападів та ракетних ударів на українські міста. Тому важливо пам'ятати про правила інформаційної безпеки:

- У жодному разі не слід нікому передавати інформацію про себе, свою родину ситуацію в місті та місця розміщення військової техніки. Про це не варто говорити навіть тим, кого дитина знає особисто, адже їхні сторінки можуть бути зламані або з метою вивідання інформації можливе створення фейкових профілів.
- Не можна фіксувати та викладати у мережу фото та відео з військовими підрозділами, технікою, роботою протиповітряна оборона (ППО) та місцями вибухів і прильотів. Ці дані можуть бути використані ворогом для коригування подальших ударів. З цих же міркувань не варто листуватися з незнайомими людьми.
- Якщо дитину без її відома додали до нового групового чату, необхідно відписатися від цієї групи та заблокувати її. Також не слід переходити за

невідомими посиланнями — вони можуть бути джерелом вірусу та подальших хакерських атак.

- Якщо до дитини звертаються невідомі з проханням виконати спеціальне завдання, необхідно заблокувати цей чат та звернутися до кіберполіції. Краще зробити профіль приватним, щоб повідомлення могли надсилати лише ті, хто перебуває у друзях.

Інформаційна безпека дітей — це надзвичайно важливо. Виконання цих порад стане гарантією того, що необдумані дії не зашкодять ані вашій родині, ані силам оборони України.

Як забезпечити безпеку в інтернеті?

Цифрові платформи дозволяють нам отримувати доступ до останніх новин та світових подій буквально в режимі онлайн. Це може стати гарним способом дізнатися, що відбувається у світі. Однак через велику кількість контенту про війну і бойові дії ваша дитина може бути спантеличена і стурбована тим, що відбувається.

Неможливо проконтролювати потік інформації з безлічі сайтів. Це означає, що ваша дитина може зустріти в інтернеті тривожний контент, навіть не виконуючи його пошук.

Ось кілька порад, які допоможуть вам слідкувати за безпекою в інтернеті для дітей:

- Підтримайте свою дитину, допоможіть їй зрозуміти те, що вона побачила, і дайте їй можливість поставити будь-які питання, що можуть виникнути.
- Вимкніть повідомлення про новий контент, щоб допомогти дитині відпочити.
- Використовуйте фільтри та налаштування, які допомагають обмежити небажаний контент.
- Нагадайте дітям, що інколи інформація в інтернеті не ґрунтується на фактах. Це особливо вірно і для подробиць про війну. Існує багато фейкових новин та дезінформації, тому заохочуйте дитину перевіряти факти на сайтах, яким ви можете довіряти.
- Нагадайте дитині не ділитися чутливим контентом, оскільки це може засмутити інших.

Чого не робити у 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 у 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 намагатись вести листування з дитиною для шантажу чи примушування щодо отримання інформації про розміщення техніки в місті.
- Не знімати місця вибухів та потрапляння снарядів, оскільки окупанти можуть використовувати фото та відео дані, які потрапили до мережі, для коригування подальшого нанесення вогню по місту.
- Не переходити за невідомими посиланнями, які були надіслані у приватні повідомлення у будь-якій соціальній мережі чи месенджері. Адже за ними можуть ховатись хакерські атаки.
- Якщо ви переглядаєте та обговорюєте новини з дитиною, варто переконатися у їхній правдивості. Усі новини, заяви високопосадовців та обмеження в містах краще повторно перевірити у офіційних каналах комунікації, на офіційних сайтах державних установ, у офіційних телеграм-каналах посадовців;
- Якщо дитину автоматично додали до невідомих груп, то важливо відписатись 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. Разом зробити скріншот групи, повідомлень та через онлайн форму звернутись до кіберполіції.

Що варто зробити:

Профіль дитини у соціальних мережах варто зробити закритими: 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 будь-яким чином ця інформація нашкодити вам або вашим близьким? А під час війни — нашим містам та захисникам?

Правила інформаційної безпеки під час війни: як захиститись цивільним

Громадська організація “Гільдія ІТ-фахівців” склала для українців правила інформаційної безпеки під час війни. Айтішники підкреслили, звичайним людям достатньо знати базові правила (4 перші пункти) та ще дещо:

1. Двухфакторна автентифікація має бути увімкнута скрізь, в усіх сервісах.
2. Оновіть паролі та зробіть їх безпечними — мінімум 8 символів, літери великого та малого регістру, цифри та спецсимволи; не повторюйте паролі у різних сервісах.
3. Не відповідайте на дзвінки з незнайомих номерів.
4. Також для дзвінків найкраще користуватися захищеними Месенджерами, такими як Signal. Дзвінки по мобільній мережі перехопити набагато простіше
5. Читати лише офіційні джерела інформації.
6. Не довіряти чуткам та пліткам — те що ви або члени вашої родини не бачили на власні очі, варто сприймати максимально-критично.
7. Дуже важливо — не можна допустити паніки! Тому будь які панічні пости ігнорувати, та блокувати їх авторів. Паніка — це найстрашніше під час війни.
8. Не фотографувати та не викладати в соціальні мережі фото військових, бойових дій, ракет та літаків у небі, результатів обстрілів. Якщо ви вважаєте, що маєте важливу інформацію, топовідомте найближчому військовому, бійцю тероборони, поліцейському.
9. Якщо ви знаходитесь у зоні окупації — сидіть вдома, почистить свій телефон від фото, переписок та підписок у соцмережах. Пам'ятайте: це — тимчасово.
10. Якщо можете — допомагайте одне одному та нашим захисникам (це найголовніше). Якщо ви прихистили пораненого захисника — не пишіть й не кажіть цього, передайте інформацію його командуванню (якщо поранений у свідомості та має документи та канал зв'язку) або по наданим вище каналам.

Загальні поради з питань безпеки дітей у мережі

Тримайте комп'ютер на відкритому місці

Якщо ваш комп'ютер знаходиться в зоні з інтенсивним рухом людей, вам буде легше відстежувати активність дитини. Ця доступність не тільки утримує дітей від небажаних дій, але також дозволить вам втрутитися, якщо ви помітите поведінку, яка може мати негативні наслідки.

Встановлюйте правила та попередьте про небезпеку

Переконайтеся, що дитина знає межі того, що їй дозволено робити за комп'ютером. Ці межі повинні відповідати віку, знанням та зрілості дитини. Обмеження можуть включати те, як довго дитині можна перебувати за комп'ютером, які сайти дозволено відвідувати, які програми використовувати та які завдання чи дії виконувати.

Визначте типи веб-сайтів або ігор, до яких дитина може отримати доступ

Це особливо важливо для дітей молодшого віку, оскільки вони можуть грати в новітні ігри, не усвідомлюючи при цьому дорослих тем та змісту. Небезпека тут не лише в самих іграх, а й у тому, з ким ваші діти можуть взаємодіяти без вашого відома. Наприклад, якщо дитина грає в онлайн-гру переважно з підлітками старшого віку, з неї можуть знущатися або піддавати його неналежній поведінці.

Будьте відкритими

Щоб забезпечити безпеку в інтернеті для дітей, дайте дитині знати, що вона може звернутися до вас з будь-якими питаннями чи побоюваннями щодо проблем, з якими вона могла зіткнутися в онлайн-просторі.

Розгляньте можливість поділу вашого комп'ютера на окремі облікові записи

Більшість операційних систем надають можливість створити окремий обліковий запис для кожного користувача. Якщо ви стурбовані тим, що ваша дитина може випадково отримати доступ, змінити та/або видалити ваші файли, ви можете надати їй окремий обліковий запис та зменшити обсяг доступу та кількість наявних у неї привілеїв.

Провідний інженер з охорони праці



Олександр РЯЗАНОВ