Кібергігієна під час війни

Цифрове середовище вже давно стало невід'ємною складовою життя людини і суспільства. Наш гайд «Онлайн-безпека під час війни» стане у пригоді широкій аудиторії — дітям, батькам і опікунам, людям поважного віку та молоді. Оскільки в умовах повномасштабної війни росії проти нашої держави стало ще простіше скористатися вразливістю користувачів в онлайн-просторі. У ці часи потрібно подбати про свою цифрову безпеку та дотримуватися правил, які допоможуть захистити себе та своїх близьких.

Ми зібрали рекомендації, як говорити з дитиною про війну. Якщо ви плануєте перетнути кордон або шукаєте роботу онлайн за кордоном, дізнайтеся, як уникнути можливих ризиків та не потрапити до злочинців. Підготували основні правила кібергігієни, яких варто дотримуватися, щоб захистити свої дані та бути на зв‘язку.

Даний матеріал створено командою МІНЗМІН у партнерстві з Міністерством цифрової трансформації та Консультативною місією ЄС в Україні.

Міністерство цифрової трансформації України

EUAM UKRAINE

МІНЗМІН

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в межах грантового компоненту проєкту EU4USociety. Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу».

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

ПРЯМУЄМО РАЗОМ

Кібергігієна стала ще важливішою під час першої повномасштабної кібервійни. В умовах інформаційно-психологічних атак варто дотримуватися правил онлайн-безпеки, залишатися пильними та обережними.

Правила інформаційної гігієни на цифровому фронті під час війни

Зараз у соцмережах і медіа багато фейків та дезінформації. Усе це вороги роблять для того, щоб українці втратили віру в перемогу й опустили руки.

Тож просимо дотримуватися правил, які допоможуть вам вистояти під час інформаційної атаки окупантів:

1. Користуйтеся офіційними джерелами інформації (зібрали їх тут), а також офіційними сторінками держслужбовців та органів місцевого самоврядування.

2. У жодному разі не ведіться на рекламні дописи в соцмережах із псевдосторінок СБУ чи інших держустанов. Їх публікує ворог, щоб викликати у вас довіру. Перевіряйте офіційні сторінки установ на достовірність такої інформації.

3. У жодному разі не поширюйте інформацію про переміщення українських військ, так ви здаєте позиції ворогу!

4. Поширюйте правду про війну, яку веде рф в Україні, у своїх соцмережах. Пам'ятайте: вони теж є інформаційною зброєю проти ворога!

5. Робіть дописи для своєї аудиторії в соцмережах, спілкуйтеся зі знайомими адміністраторами груп і каналів в інших країнах та поширюйте інформацію через них. Поширюйте правду до росіян, оскільки там повністю обмежений доступ до правдивої інформації.

Правила інформаційної гігієни на цифровому фронті під час війни

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

6. Захистіть свої соцмережі: встановлюйте складні паролі, не додавайте в друзі невідомі акаунти, увімкніть двоетапну автентифікацію.

7. Підтримуйте дух нашої армії! Пишіть слова подяки, підбадьорюйте українців!

8. Долучайтеся до лав IT-армії України або до Інтернет-Війська.

Поради, які допоможуть мінімізувати ризики для дітей в інтернеті під час війни

💻 Перевіряйте, якими додатками користуються діти та яку інформацію додатки про них збирають. Для цього потрібно читати умови та політики використання застосунків чи соціальних мереж.

💻 Подавайте скарги на контент або профілі, який ви бачите в мережах і який не слід бачити дітям. Розповідайте також і дітям, як це робити. Що більше ви скаржитеся, то менше незрозумілих профілів і шкідливого контенту буде в соцмережах. Те саме стосується реклами, яка не відповідає інтересам дітей або є дуже нав'язливою.

💻 Намагайтеся забезпечити наявність доступу до інтернету для дітей. Не варто забороняти дітям користуватися смартфонами та новітніми технологіями. Навпаки, їх потрібно зробити друзями та помічниками, а не ворогами.

💻 Потрібно знати, що для користування соцмережами дітям має бути щонайменше 13 років. Або ж навіть якщо їм уже виповнилося 13 років, для використання TikTok, наприклад, потрібна згода батьків. Не забувайте про функцію батьківського контролю. Так ви можете фільтрувати контент і профілі, за якими стежать діти.

💻 Говоріть з дітьми про приватність. Розповідайте, яку інформацію про себе краще не публікувати. Це, наприклад, документи, дані кредитних карток, місце перебування. Нагадайте, що діти мають певну онлайн-репутацію. І контент, який вони публікують, може побачити будь-хто. Змінити його після публікації може бути складно. Тому в соцмережах рекомендовано налаштовувати приватний доступ до профілів, щоб контролювати, хто може бачити публікації дітей, коментувати дописи тощо.

💻 Перш ніж фотографувати та публікувати світлини дітей в інтернеті, запитайте в них дозволу. Або якщо ви вчитель, потрібно мати дозвіл батьків для цього.

💻 Стежте за своєю онлайн-репутацією.
Особливо це стосується вчителів.
Перевіряйте інформацію, на яку натрапляєте в інтернеті, та нагадуйте про це дітям. Не поширюйте сумнівні дописи.

💻 Намагайтеся облаштувати безпечне середовище для дітей із використанням технологій.
Перевірте, чи встановлені на комп'ютерах у школі та вдома антивірусні програми, та чи оновлене ліцензійні програмні засоби. Встановлюйте складні паролі на телефони й комп’ютери та переконайтеся, що вони є на пристроях у дітей. І не забувайте про двофакторну автентифікацію.

💻 Якщо дитина має онлайн-друга та хоче зустрітися із ним вживу, то не дозволяйте йому іти самому на таку зустріч, оскільки люди не завжди можуть виявитися в реальному житті тими, за кого видають себе в соцмережах.

💻 Говоріть з дітьми про їхню онлайн-активність. Цікавтеся тим, що вони роблять в інтернеті, з яких джерел отримують новини тощо.
Важливо, щоб у дітей не виникало відчуття, що батьки їм не довіряють. Отже, завданням батьків і вчителів залишається розповідати дітям про їхні цифрові права, критичне мислення і цифрову безпеку, а також самим дотримуватися порад та правил.

Якщо деякі з рекомендацій для вас незрозумілі чи складні, обов’язково перегляньте безоплатний курс «Цифрові права та безпека для дітей», онлайн-курс для батьків «Приватність дітей в інтернеті» та серіал для батьків «Безпека дітей в інтернеті». В онлайн-курсі та серіалі ви знайдете прості рекомендації, які допоможуть захистити вас від інтернет-загроз та покажуть, як відрізняти правду від фейків.

Вчіться самі та навчайте дітей, бо цифрові компетенції є основою для безпечного життя в цифровому світі, який давно став новою реальністю не лише для дітей, але й кожного з нас.

Дізнатися більше про те, як захистити себе можна за допомогою гарячої лінії з цифрової безпеки Nadiyno. Цей інструмент можна використовувати для посилення власної онлайн-безпеки.

Гаряча лінія Nadiyno допоможе підвищити цифрову грамотність і подолати актуальні онлайн-загрози. На платформі можна поставити питання щодо захисту персональних даних/пристроїв, проблем зламу акаунтів чи безпекових налаштувань. Відповіді оперативно готують та надають фахівці з кібербезпеки через e-mail, вебчат чи зручний месенджер. Лінія працює в будні дні з 08.00 до 22.00.

Поради, які допоможуть подбати про інформаційну безпеку дитини під час війни

Що потрібно зробити батькам:

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

   Як налаштувати приватність дитини в соціальних мережах та месенджерах, ви можете дізнатися за посиланнями:
   - Про приватність у Telegram
   - Про приватність у TikTok
   - Про приватність в Instagram
   - Про приватність у Facebook

   Потрібно пам'ятати: 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.

2. Про те, чому дописи в соціальних мережах про дітей можуть зашкодити їхньому майбутньому, можна дізнатися за посиланням.

Поради, які допоможуть подбати про інформаційну безпеку дитини під час війни

Що потрібно зробити батькам:

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

   Як налаштувати приватність дитини в соціальних мережах та месенджерах, ви можете дізнатися за посиланнями:
   - Про приватність у Telegram
   - Про приватність у TikTok
   - Про приватність в Instagram
   - Про приватність у Facebook

   Потрібно пам'ятати: 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.

2. Про те, чому дописи в соціальних мережах про дітей можуть зашкодити їхньому майбутньому, можна дізнатися за посиланням.

Про що потрібно знати батькам:

1. Якщо хтось з 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.

2. Не можна знімати розміщення та пересування військової техніки та військових у місті, де перебуває дитина. Оскільки окупанти можуть переглядати відкриті профілі українців, щоб визначити місце розташування військових для подальшого нападу. Також злочинці можуть листуватися з дитиною, щоб шантажувати чи примушувати інформацію про розміщення техніки в місті.

3. Не знімати місця вибухів та потрапляння снарядів, оскільки окупанти можуть використовувати фото- та відеодані, які потрапили в мережу, для коригування подальшого вогню по місту.

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

5. Якщо ви переглядаєте та обговорюєте новини з дитиною, переконайтеся в їхній достовірності. Усі новини, заяви високопосадовців та обмеження в містах краще повторно перевірити в офіційних каналах комунікації, на офіційних сайтах державних установ, в офіційних телеграм-каналах посадовців.

6. Якщо дитину автоматично додали до невідомої групи, відпишіться від неї та заблокуйте її.

7. Якщо дитині хтось пише з проханням допомогти або виконати спеціальне завдання, важливо, щоб вона повідомила про це дорослим. Варто разом зробити скріншот групи, повідомлень та через онлайн-форму звернутися до кіберполіції.

Як відрізняти правдиву інформацію від неправдивої та фейків?

Для розвитку критичного мислення спочатку потрібно навчитися відрізняти правдиву інформацію від неправдивої та завести звичку завжди перевіряти інформацію, яку споживаєш.

Як з першого погляду помітити ознаки неправдивої або маніпулятивної інформації? Звертайте увагу на декілька характеристик:

1. Наявність дуже великих чисел, сенсаційний характер новини або ж інформація відразу викликає дуже негативні емоції.

2. Відірваність заголовка від змісту всієї новини. Цей прийом використовується для привернення уваги. Сама ж інформація в новині вже не така важлива. Тому потрібно читати як і загаловок, так і текст новини, щоб не допустити впливу фейків на себе.

3. Дата, яка не відповідає дійсності. Часто старі публікації видаються за нові, тому рекомендуємо дивитися на дату новини або ж статті.

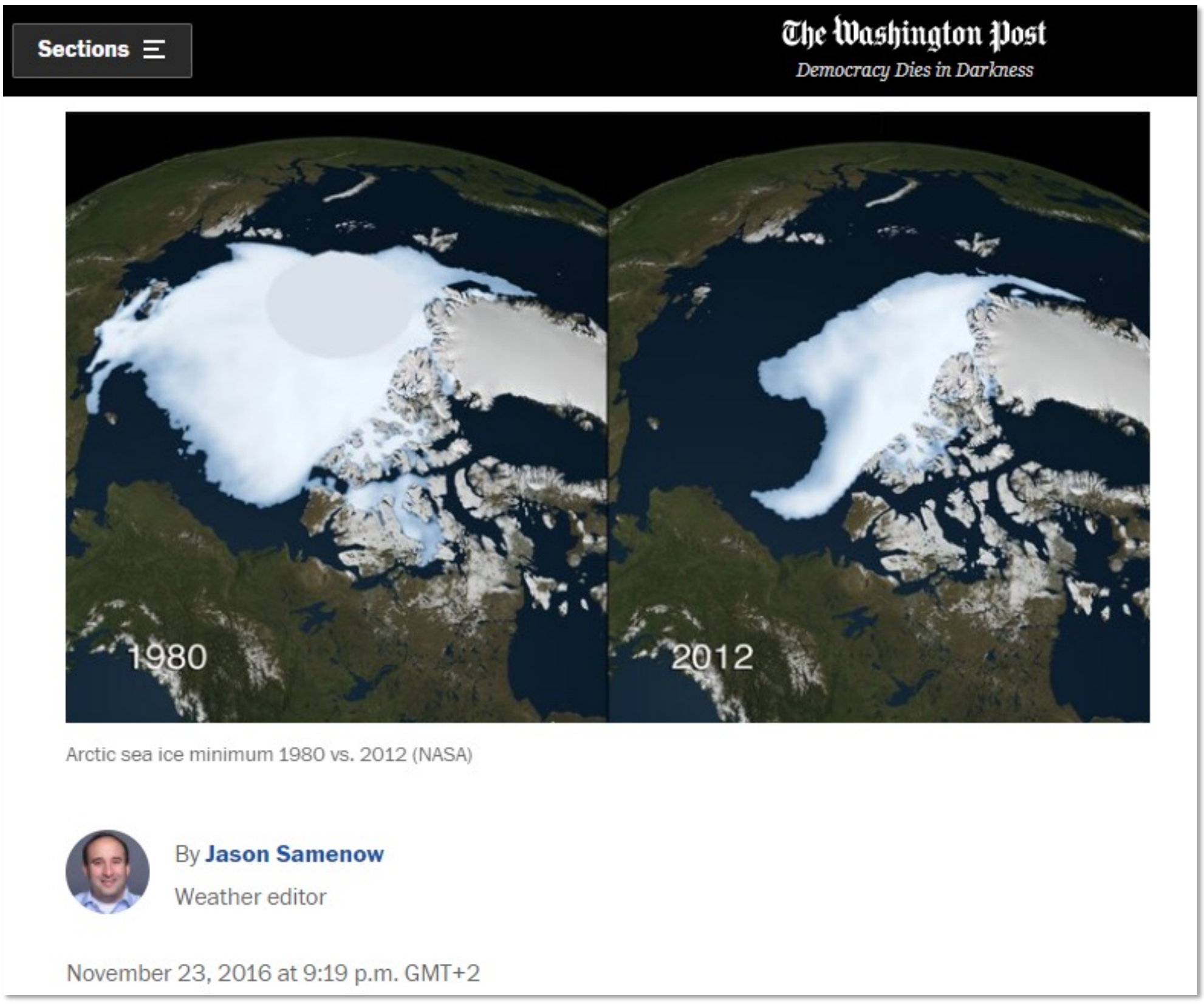
4. Апелювання до надприродних речей та згадування відомих людей у невластивому для них контексті. Така інформація швидко поширюється та гарно запам’ятовується, бо суперечить нашим звичайним поглядам на життя.

5. Часто у неправдивих новинах, публікаціях використано неправдиві фото або старі фото видають за нові. Розглянемо для прикладу цей пост в інстаграмі.

На фото зображені льодові покриви Арктики нібито у 2009 та у 2019 роках. Правдивість фото можна легко перевірити через такий сервіс, як Google Search Image. Для цього треба просто зробити скріншот фото без тексту й завантажити їх зображення в пошуковик.

Після перегляду результатів пошуку можна зрозуміти, що фото справді не фейкові, але зроблені у 1980 та у 2012 році, а не в тих, які записані в публікації.

Підтвердженням є ось ця стаття американського видання “Washington Post”.



Тому якщо фото чи відео здається дуже неймовірним або викликає сильні емоції, то воно може бути неправдивим або його використовують у неправдивому контексті, як у нашому разі.

Який алгоритм перевірки інформації на правдивість?

Суть інструкції в тому, щоб ставити собі три прості запитання кожного разу, коли читаєте новини чи гортаєте стрічку в соціальній мережі.

☐ **1. З’ясуйте першоджерело (автора) інформації.**

Якщо це інформація в соцмережах, перегляньте акаунт автора. Якщо автор публікації взагалі відсутній, такій інформації не потрібно довіряти. Якщо це новина чи стаття в ЗМІ, перевірте, чи має її автор ще якісь публікації і чи взагалі він існує.

☐ **2. Перевірте, які аргументи наведені в тексті для підтвердження думки чи факту.**

Задумайтеся, а чи взагалі є підтвердження думки або факту в тій інформації, яку ви читаєте? Чи є посилання на джерело даних? Чи можна цьому джерелу довіряти? Наскільки правдиві дані, використані в публікації? Перевіряйте аргументи та пам’ятайте, що даними можна легко маніпулювати.

☐ **3. Дізнайтеся, що говорять інші про це.**

Один з недоліків й одночасно одна з переваг інтернету — це надмірна кількість інформації, тому гарна ідея — дізнатися, що інші джерела говорять про цю тему.

Для повного розуміння ознак неправдивої інформації та того, як розвинути своє критичне мислення рекомендуємо наступне відео.