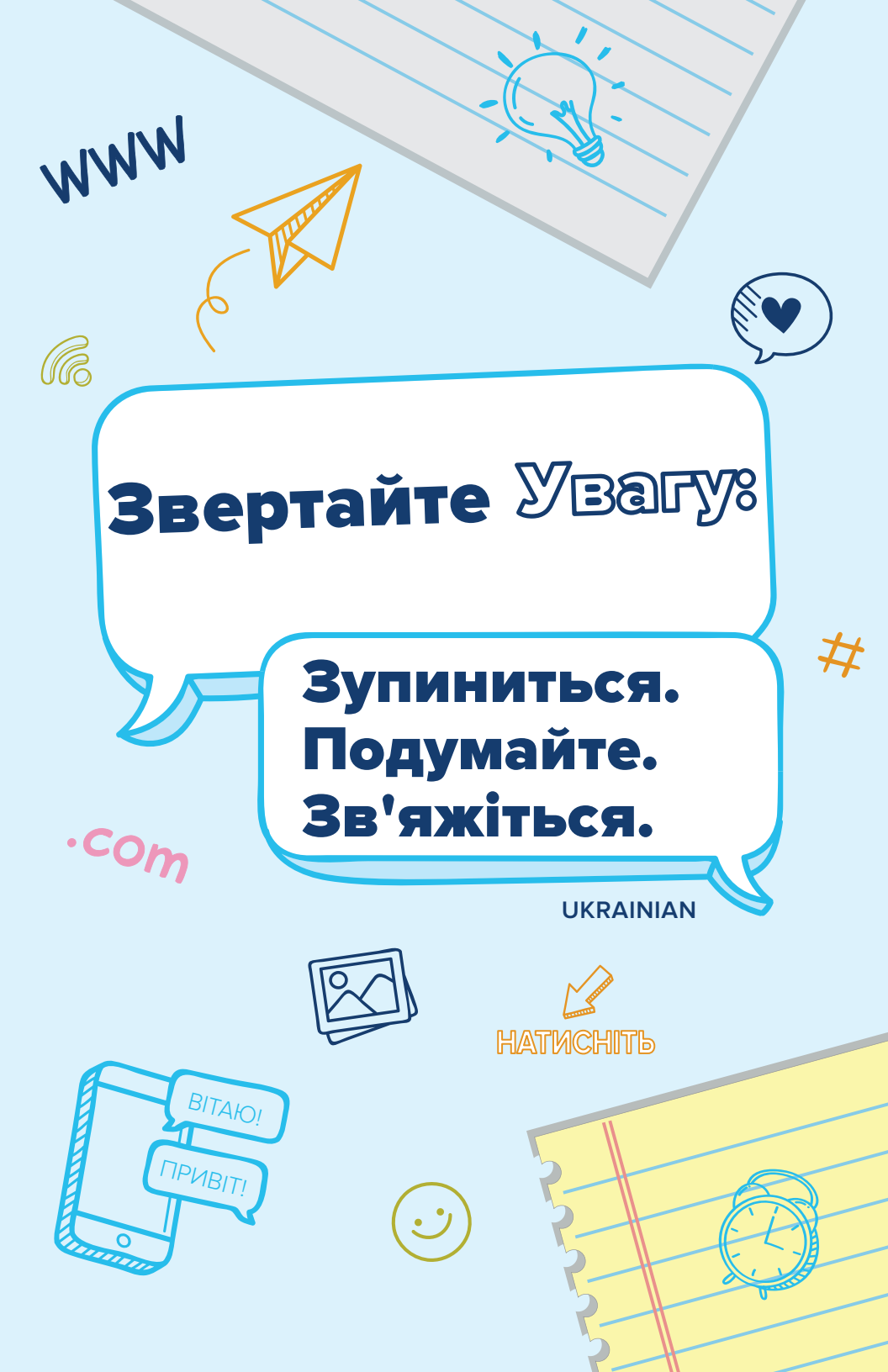
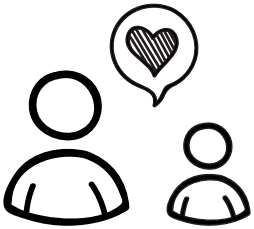

WWW
Звертайте Увагу:
Зупиниться.
Подумайте.
Зв'яжіться.
.com
UKRAINIAN
НАТИСНІТЬ
ВІТАЮ!
ПРИВІТ!



Щоб допомогти дітям у вашому житті бути безпечними в Інтернеті, *Звертайте увагу: Зупиниться. Подумайте. Зв'яжіться.* має кілька ідей, які допоможуть вам почати з ними розмову. Виберіть розділ і прочитайте його разом, щоб дізнатися, як обережно ділитися, бути добрим в Інтернеті, протистояти кіберзалякуванням і захищати їх (і свою) особисту інформацію в Інтернеті. Ці інструменти можуть допомогти вам показати дітям, як робити правильний вибір і відповідально використовувати технології. І, розмовляючи з ними, ви даєте дітям знати, що у них є довірений дорослий, який допоможе їм, коли вони роблять помилки.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Бути онлайн – це частина вашого життя. Ви переглядаєте та створюєте вміст, публікуєте фотографії та відео, граєте в ігри та ділитеся зі своїми друзями і сім'єю, де ви перебуваєте та що робите. Але є ризики, коли ви публікуєте, граєте та підключаєтесь до Інтернету. Деякі люди та ситуації, з якими ви стикаєтеся, не завжди такі, якими вони здаються.

Незалежно від того, наскільки швидко ваші пальці літають на клавіатурі, телефоні чи планшеті, найкращими інструментами, які у вас є, щоб уникнути ризиків в Інтернеті, є ваш мозок і час. Зупиніться та продумайте ситуації, щоб захистити себе, своїх друзів і родину, свої облікові записи та пристрої. Або ви можете закінчити надсилання, збентежити себе чи інших, зіпсувати свій комп'ютер або поговорити з людьми, які не є тими, за кого себе видають.

- *Поширюйте з обережністю*
- *Бути добрим - це круто*
- *Встаньте проти кіберцькування*
- *Зв'зок Захисту*

Поширюйте з обережністю

Подумайте, перш ніж поширювати

Те, що ви робите в Інтернеті, має наслідки в реальному світі. Фотографії, відео та повідомлення, якими ви ділитеся, впливають на вас, вашу конфіденційність, репутацію та людей навколо вас — зараз і в майбутньому. Зупиніться і подумайте, перш ніж публікувати.

Те, що ви публікуєте, може мати більшу «аудиторію», ніж ви думаєте.

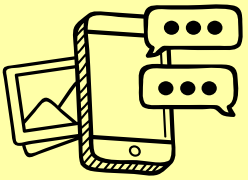
Неможливо повністю контролювати, хто бачить ваш профіль, зображення, відео чи тексти, навіть якщо ви використовуєте налаштування конфіденційності або програми, які видаляють ваш вміст після його перегляду або протягом 24 годин. Кожен, хто побачить вашу публікацію, може зробити знімок екрана або запис. Запитайте себе: «Чи хотів би я, щоб хтось встав посеред обіду та поділився цією фотографією чи відео з усім кафетерієм?»

Те, чим ви ділитеся, може вплинути на інших. Може бути незручно, несправедливо та навіть небезпечно надсилати або публікувати фотографії та відео без дозволу людей, які на них зображені. Спершу отримай дозвіл. Перш ніж опублікувати, запитайте: «Чи ви погодитеся, якщо я опублікую це в соціальних мережах?» Не публікуйте, якщо вам скажуть ні.

Як тільки ви опублікуєте щось в Інтернеті, ви не можете забрати це назад

Навіть якщо ви видалите те, що опублікували, або термін дії публікації закінчиться, цю фотографію чи коментар, які ви не хочете, щоб інші бачили, можна зберегти, поділитися ними та залишити десь онлайн — назавжди.

Секстинг: не робіть цього



Можливо, ви чули історії у школі чи в новинах про людей які «секстують» — надсилають оголені фотографії зі своїх телефонів. Не робіть цього. Крапка. Створення, пересилання або навіть збереження відверто сексуальних фотографій, відео чи повідомлень ставить під загрозу вашу дружбу та репутацію. Що ще гірше, ви можете порушити закон.

Пам'ятка про соціальні мережі

За словами Головного Лікаря США, користування соціальними мережами може завдати вам шкоди, залежно від того, скільки часу ви проводите на платформах, типу контенту, який ви бачите, і того, наскільки він заважає вам спати чи займатися фізичними вправами — тими видами діяльності, які є важливими для твоє здоров'я.

Бути добрим - це круто

Ввічливість має значення

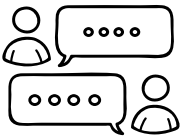
Якщо ви не можете побачити чиюсь міміку, мову тіла чи інші візуальні підказки в Інтернеті, ви можете сміливо опублікувати або сказати те, чого б не сказали особисто. Але текстові повідомлення, публікації, прямі повідомлення, гра у відеоігри та електронні листи – це те ж саме, що розмова з кимось віч-на-віч. Будьте уважні до того, як ви спілкуєтеся, і подумайте, перш ніж говорити або публікувати.

Сповільниться. В Інтернеті легко виникають непорозуміння. Перш ніж надіслати повідомлення, запитайте себе: «Які почуття це повідомлення викличе в інших людей?»

Звертайте увагу та поважайте точки зору та почуття інших людей в Інтернеті —так само, як і особисто. Пам'ятайте: за аватарками та іменами профілю стоять реальні люди.

Знизьте тон. Не використовуйте лише ВЕЛИКІ літери, довгі ряди знаків оклику чи великі жирні шрифти. Це те саме, що кричати.

Не розміщуйте все в груповому чаті.
Перш ніж надіслати групове повідомлення або натиснути «Відповісти всім», зупиніться й подумайте: кому потрібно бачити це повідомлення?



Не видавайте себе за іншу особу

Неправильно та потенційно шкідливо створювати профілі, коментарі чи дописи, які нібито надійшли від когось іншого, наприклад від когось у вашому класі чи вчителя.

Висловлюйтеся

Якщо ви бачите, що друг опублікував щось необдумане або небезпечне, скажіть йому. Ви можете вберегти свого друга від неприємностей і того, що може їх осоромити. Якщо ви бачите в Інтернеті щось неприйнятне, повідомте про це та розкажіть дорослому, якому довіряєте. У більшості додатків і платформ є спосіб повідомити, якщо чиясь поведінка є загрозливою або неприйнятною.

Встаньте проти кібербулінгу

Кожен заслуговує на те, щоб почуватися в безпеці під час повсякденної взаємодії з іншими людьми, незалежно від того, чи є вони в Інтернеті чи віч-на-віч.

Якщо хтось публікує злі коментарі, образливі меми, незручні фотографії або надсилає чати чи приватні повідомлення про вас, це є цькуванням. Це не гаразд. Поговоріть з дорослим, якому ви довіряєте, щоб отримати допомогу в ситуації та вирішити, як вам реагувати.

Якщо хтось переслідує вас в Інтернеті, ось що робити:

- **Ігноруйте** особу або заблокуйте її від подальшого зв'язку з вами.
- **Збережіть свідчення** і попросіть допомоги у дорослого, якому довіряєте.
- **Повідомте про це.** У більшості додатків і платформ є інструменти повідомлення, якщо чиясь поведінка є загрозливою або неприйнятною.

Цькування часто змушують людину, яку переслідують, почувати себе погано — і це змушує хулігана виглядати погано.

Цькування також може призвести до проблем зі школою чи поліцією.

Якщо ви стали свідком кібербулінгу, знайдіть способи стати сторонником — людиною, яка втручається, перебиває або говорить, щоб припинити цькування. Підла поведінка зазвичай припиняється досить швидко, коли хтось заступається за людину, яку цькують.

Зв'язок Захисту

Захистіть свою конфіденційність

Коли ви робите щось онлайн, ви залишаєте слід. Виконайте ці кроки, щоб переконатися, що слід не веде до інформації, якою ви, можливо, не збиралися ділитися.

Використовуйте налаштування конфіденційності. Дізнайтеся, як увімкнути налаштування конфіденційності для пристроїв, програм і облікових записів у соціальних мережах — тоді зробіть це. Це допоможе вам обмежити, хто може бачити, де ви перебуваєте, що ви публікуєте, і хто може зв’язуватися з вами.

Перевірте налаштування локації. Деякі програми дозволяють вам бачити, де знаходяться ваші друзі. Вони також повідомляють, де ви перебуваєте. Подумайте, коли має сенс ділитися своїм місцезнаходженням. Якщо цього не відбувається,

вимкніть надсилання геоданих. Функції ваших пристроїв, як-от камера, можуть мати інформацію про те, де ви були, коли робили фотографію. Якщо ви не хочете показувати, де ви були для кожного селфі, вимкніть своє місцезнаходження на камері телефону. Завжди запитуйте себе: «Чи потрібно цьому додатку знати, де я?»

Обмежте своїх друзів в Інтернеті людьми, яких ви дійсно знаєте. Спілкування з друзями через текстові повідомлення, соціальні мережі або відеоігри можуть бути весело, але деякі люди не ті, за кого себе видають в Інтернеті. І якщо ви не будете обережні, ви можете поділитися особистою інформацією з незнайомцем.

Захистіть інформацію про себе

Якщо ви надасте свою особисту інформацію, як-от номер соціального страхування, паролі чи інформацію про банківський рахунок, незнайомій людині, ви не зможете її повернути.

Ось як захистити інформацію про себе в Інтернеті:

Не відповідайте на повідомлення, які просять надати особисту інформацію. Навіть якщо повідомлення виглядає так, ніби воно надійшло від друга, члена родини чи компанії, яку ви знаєте, або говорить, що трапиться щось погане, якщо ви не відповісте. Швидше за все, це фейк і надіслано для викрадення вашої

інформації. Попросіть дорослого, якому ви довіряєте, щоб він допоміг вам повідомити про повідомлення як про небажане чи спам.

Перевірте, до якої інформації додаток хоче отримати доступ — перед завантаженням. Деякі додатки запитують дозвіл на доступ до інформації або функцій, які їм не потрібні, як-от список контактів, камера, пам'ять, місцезнаходження та мікрофон. Попросіть дорослого, якому ви довіряєте, допомогти прочитати політику конфіденційності додатка, щоб дізнатися, як використовуватимуться ваші дані та чи будуть вони надані. Потім вирішіть, чи дійсно цій грі слів потрібен доступ до ваших фотографій.

Поговоріть з дорослим, якому довіряєте, перш ніж робити покупки в додатку — особливо якщо дорослий за це платить.

Захистіть свої облікові записи

Ви зберігаєте багато особистої інформації у своїх облікових записах онлайн. Нижче наведено кілька кроків, які потрібно зробити, щоб інші люди не мали доступу до ваших облікових записів.

Створюйте надійні паролі.
Чим довший ваш пароль, тим важче його зламати. Використовуйте щонайменше 12 символів із поєднанням великих і малих літер, цифр і символів. Спробуйте використати парольну фразу з випадкових слів,

щоб зробити її більш запам'ятовуваною. Але не використовуйте загальні фрази, тексти пісень або цитати з фільмів, які легко вгадати.

Будьте унікальними. Вигадайте різні паролі для ваших різних облікових записів. Таким чином, якщо хто-небудь отримає ваш пароль для одного облікового запису, вони не можуть використовувати його для входу в інші ваші облікові записи. Один із способів відслідковувати всі ваші різні паролі – це використовувати менеджер паролів.

Тримайте їх приватними. Не діліться вашими паролями з ким завгодно, навіть не з вашим найкращим другом або кимось, з ким ви зустрічаєтеся.

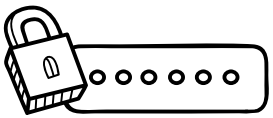
Будьте прискіпливі до секретних запитань. Спробуйте

вибрати секретні запитання, на які можете відповісти лише ви. Пропускайте запитання з відповідями, які хтось може знайти в Інтернеті, як-от ваш поштовий індекс, місце народження чи дівоче прізвище матері. Якщо ви не можете уникнути цих запитань, будьте творчими! Ставтеся до них як до паролів і використовуйте випадкові та довгі відповіді. Просто переконайтеся, що ви запам'ятали свої відповіді.

Використовуйте багатофакторну автентифікацію. Багато облікових записів пропонують додатковий захист для ваших облікових записів за допомогою «багатофакторної автентифікації» — вимагаючи щось

на додаток до пароля. Багатофакторна автентифікація поєднує те, що ви знаєте (наприклад, пароль), з тим, що у вас є (наприклад, код доступу, згенерований програмою), або тим, що ви є (наприклад, відбиток пальця).

Швидко змінюйте паролі, якщо є злом.
Якщо компанія повідомить вам про витік даних, у результаті якого хакер міг отримати ваш пароль, негайно змініть пароль, який ви використовуєте для цього облікового запису. Також змініть його для будь-якого облікового запису, який використовує подібний пароль.



Захистіть свої пристрої

Найкращий спосіб отримати задоволення від перебування в Інтернеті? Переконатися, що ваші пристрої безпечні. Почніть тут:

Налаштуйте програмне забезпечення безпеки на автоматичне оновлення для всіх ваших пристроїв, інтернет-браузерів і операційної системи. Це допоможе вам захиститися від нових загроз безпеці.

Не натискайте на посилання та не відкривайте вкладення. Якщо ви отримали неочікуване текстове повідомлення, електронний лист або повідомлення в Інтернеті, яке пропонує вам натиснути посилання або відкрити вкладений файл, не робіть цього! Навіть якщо це пропозиція безкоштовних речей. Посилання та вкладення можуть приховувати віруси або шпигунське програмне забезпечення, яке може зіпсувати ваш телефон, комп'ютер або планшет.

Захистіть свої пристрої паролем. Це допоможе вберегти ваші фотографії, повідомлення та облікові записи від потрапляння в чужі руки.

Зберігайте їх у безпечному місці. Будь то ваш телефон, ноутбук чи планшет, не залишайте його на людях навіть на хвилину.

Дізнайтеся більше на сайті

This booklet helps kids socialize safely online. There's help on how to share with care, be kind online, stand up to cyberbullying, and protect their personal information. Get free copies in English or Spanish at

ftc.gov/bulkorder

FEDERAL TRADE COMMISSION

Серпень 2023 року