ПОРАДИ БАТЬКАМ ЩОДО БЕЗПЕЧНОГО КОРИСТУВАННЯ ІНТЕРНЕТОМ:

- Вимкнути можливість пошуку через диктування на пристроях.
- Використовуйте батьківській контроль на всіх гаджетах, якими користується дитина, - це можна зробити через налаштування смартфону чи браузера, а також за допомогою встановлення програми Star Guard family або Kidslox.
- Для безпечного користування дітьми Інтернетом рекомендовано встановити YouTube Kids - це спеціальний формат звичного ютуба, який націлений саме на онлайн безпеку дітей під час перегляду мультфільмів чи відео, а також Safe Search Kids для безпечного пошуку в Інтернеті.
- Як тільки ви дозволяєте дитині користуватись телефоном, ноутбуком, планшетом чи комп'ютером, то одразу розпочніть бесіду щодо того, як довго та коли донька чи син можуть використовувати пристрій, а також поясніть основні правила Інтернет безпеки і що це має бути тільки під наглядом дорослих. Таку бесіду можна розпочати за допомогою розмальовки чи кросворду, які знайдете в додатках.
- Встановіть паролі на гаджети, які будуть відомі тільки вам, - таким чином дитина не може використовувати гаджет та додатки без вашого відома.
- Встановіть ліміт часу на гаджетах чи у додатках - вони самостійно вимикаються, коли пройде встановлений час.
- Також, якщо є старші діти, то варто поговорити з ними про те, що вони можуть показувати брату чи сестрі в смартфоні, до чого залучати в Інтернеті, а що є забороненим.
- Рекомендуємо не викладати фотографії дітей під час спортивних занять чи на відпочинку у купальнику, чи оголеними, оскільки це може привернути увагу злочинців.
- Всі ці правила мають діяти серед всіх членів родини, з якими дитина проводить час.
- Допоможіть дитині дізнатись більше про Інтернет та світ довкола за допомогою розвиваючих ігор.
- Якщо син чи донька прийшли до вас розповісти про щось неприємне, що з ними трапилось в мережі, то вислухайте його чи її без осуду.

- Будьте відкритими до запитань та розповідей дитини про різні ризики й ситуації в мережі. Також поговоріть з донькою чи сином про те, що не вся інформація, яка знаходиться в Інтернеті є безпечною і підходить для перегляду неповнолітнім. Як і в реальному житті, в онлайні є те, що дозволено тільки дорослим.
- Поспілкуйтесь з батьками однокласників вашої дитини щодо користування гаджетами під час навчального процесу, про можливі онлайн ризики, встановлення батьківського контролю та реєстрацію у соціальних мережах з 13 років, оскільки згідно офіційних правил соц.мереж саме такий вік є дозволеним для створення акаунта.
- Досліджуйте разом – цікавтесь у дитини щодо ігор та додатків, якими вона користується.
- Домовтесь про «зони» вдома, де можна використовувати гаджет. Наприклад, рекомендується, щоб дитина не відвідувала ванну кімнату з телефоном та не проводила час наодинці з ним.
- Звертайте увагу на віковий рейтинг ігор та додатків – це допоможе зрозуміти, чи підходить така розвага вашій дитині чи ні.
- Не викладайте фотографії дитини без її згоди на те. Рекомендуємо не викладати фотографії дітей під час спортивних занять чи на відпочинку у купальниках, чи оголеними, оскільки це може привернути увагу злочинців.
- Нагадуйте підлітку про те, щоб перед поширенням будь-якого матеріалу варто уявити, що все, що підліток хоче написати або надіслати, висить на великому білборді перед школою, який бачать усі. Якщо син чи донька не хоче, аби будь-хто міг це побачити, тоді не варто публікувати такі матеріали чи навіть надсилати його в особисті повідомлення.
- Якщо підліток став жертвою кібербулінгу, то поговоріть з нею та підтримайте її. Разом зверніться до адміністрації соціальної мережі чи ігрової платформи зі скаргою на користувача-булера. Якщо булер навчається в одній школі з вашою дитиною, то ви маєте право звернутись до директора школи зі скаргою та з заявою до поліції.

ОСНОВНІ ПРАВИЛА БЕЗПЕЧНОГО КОРИСТУВАННЯ ІНТЕРНЕТОМ:

- Долучати «в друзі» лише тих людей, кого дитина знає в реальному житті;

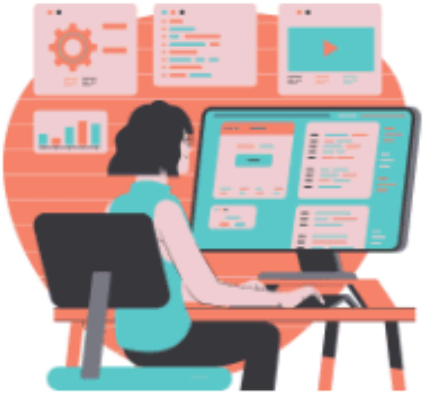
- Мати «закритий профіль» у соціальних мережах;
- Не відписувати у приватних повідомленнях незнайомим людям;
- Не зазначати приватну інформацію: домашня адреса, номер телефону, номер школи, де дитина навчається та/або адреси позашкільних занять, логін та пароль від особистої сторінки;
- Бажано не відмічати свою геолокацію, але не варто відмічати її в місцях, де дитина живе, навчається та часто буває;
- Не надсилати свої інтимні фото у приватні повідомленнях ані тим, кого вже знає дитина, а ні тим, з ким вона познайомилася в Інтернеті.

КУДИ МОЖНА ЗВЕРНУТИСЬ:

- Якщо дитина стала жертвою шантажу (наприклад, якщо дитину шантажують надісланими раніше фото чи відео), то це визнається злочином, що передбачено Кримінальним кодексом України, тому слід звернутися із заявою до поліції (за телефоном 102 або онлайн: https://ticket.np.gov.ua/). Можливо на початку буде простіше звернутися до ювенальної превенції чи кіберполіції (https://ticket.cyberpolice.gov.ua).
- Якщо дитина бажає анонімно повідомити про те, що трапилось із нею в Інтернеті – слід зателефонувати на гарячу лінію Ла Страда (за номером 116 111; з понеділка по п’ятницю з 12:00 до 16:00).
- Також, якщо у дитини з’являються питання щодо психічного, сексуального та репродуктивного здоров’я, або якщо вона хоче дізнатися більше про свої права у сфері охорони здоров’я - організація Teenergizer надає консультації “рівний-рівному” та з психологом безкоштовно і конфіденційно будуть раді допомогти за посиланням: teenergizer.org/consultations/
- Якщо Ви натрапили в Інтернеті на контент зі сценами сексуального насильства над дітьми (дитячої порнографії) — повідомте на https://stop-sexting.in.ua/ send/. Ми знаємо, що неприємно і емоційно важко бачити такий контент, але повідомлення про нього допомагають вилучити його з мережі, таким чином захистити дітей та не допустити їх подальшої сексуальної експлуатації.

Не варто сердитися на дитину за те, чого самі не дотримуєтесь! Звідки ж їй брати приклад для наслідування? Ви можете чути про шкоду Інтернету й залежності від нього, але часто дитина занурюється у світ комп’ютерних ігор і віртуальний простір тільки тому, що їй не вистачає батьківської уваги та любові.

СПІЛКУЮЧИСЬ В ІНТЕРНЕТІ ТИ, ЗАРАДИ СВОЄЇ БЕЗПЕКИ, НЕ ПОВИНЕН:



- відправляти поштою або передавати через когось свої особисті речі співрозмовнику по Інтернету;

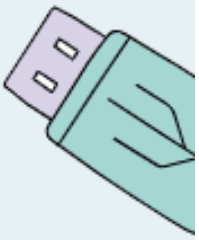
- розміщувати фотокартки, на яких ти оголений або у нижній білизні чи піжамі, а також відправляти комусь свої фото електронною або звичайною поштою;

- повідомляти пароль до своєї Інтернет-сторінки. Твій пароль як ключ від твоєї квартири, тому нікому його не віддавай!;

- казати, що ти вдома знаходишся один;

розповідати багато про своїх друзів, знайомих та родину, особливо, видавати їхні таємниці

- повідомляти своєму віртуальному другу своє прізвище, домашню адресу, номер свого мобільного або домашнього телефону, номер та місцезнаходження своєї школи та інші дані;



Увага!

Ніколи за жодних умов не погоджуйся на особисту зустріч у реальному світі зі своїм Інтернет-другом. Якщо ти все-таки вирішив зустрітися з ним, то нехай обов'язково батьки чи інші дорослі, яким ти довіряєш,прийдуть з тобою на зустріч.

КОРИСТУЙСЯ
ІНТЕРНЕТОМ
БЕЗПЕЧНО

Поради для безпеки в інтернеті

НАДІЙНІ ПАРОЛІ

Намагайся не використовувати свою дату народження чи інші прості комбінації.

БЕЗПЕЧНИЙ КОНТЕНТ

Уникай сайтів, які не є надійними. Заважантуй файли тільки з офіційних джерел.

КОНФІДЕНЦІЙНІСТЬ

Контролюй те, як компанії використовують ваші дані, увімкнувши функції конфіденційності.

ОБЕРЕЖНІСТЬ

Уникай публікування конфіденційної особистої інформації в інтернеті.

АНТИВІРУС

Оновлюй антивірусне програмне забезпечення, щоб воно могло виявляти потенційні загрози.

ІНТЕРНЕТ-БЕЗПЕКА: ПОШИРЕНІ ЗАГРОЗИ

Щоб зберегти конфіденційність та безпеку в інтернеті, важливо знати про різні типи інтернет-атак. Нижче наведено поширені загрози інтернет-безпеці.

Фішинг – це кібератака із використанням підроблених листів. Зловмисники намагаються обдурити одержувачів електронної пошти, переконавши їх у справжності та актуальності повідомлення. Наприклад, вони маскують листи під запити з банку або повідомлення від колег, щоб користувачі переходили за посиланнями або відкривали вкладення. Ціль атаки полягає в тому, щоб обманним шляхом змусити користувачів розкрити особисту інформацію або завантажити шкідливі програми.

Фішинг – одна із найстаріших загроз інтернет-безпеці, що виникла ще у 1990-х роках. Він залишається популярним і сьогодні, оскільки є одним із найдешевших і найпростіших способів крадіжки інформації. Останніми роками фішингові повідомлення та використовувані методи стають дедалі витонченішими.

Злом та віддалений доступ

Зловмисники завжди прагнуть використовувати вразливість приватної мережі або системи для крадіжки конфіденційної інформації та даних. Технологія віддаленого доступу надає додаткові можливості. Програмне забезпечення для віддаленого доступу дозволяє користувачам отримувати доступ до комп’ютера та керувати ним віддалено. Його використання значно зросло під час пандемії, коли дедалі більше людей працюють віддалено.

Протокол, що дозволяє користувачам віддалено керувати комп’ютером, підключеним до Інтернету, називається RDP – протокол віддаленого робочого столу. Багато компаній, незалежно від розміру, широко використовують RDP, тому високі шанси недостатньо надійного захисту мережі. Зловмисники використовують різні методи виявлення та експлуатації вразливостей RDP, щоб отримати повний доступ до мережі та її пристроїв. Вони можуть самостійно здійснювати крадіжку даних, і продавати облікові дані в даркнете.

Шкідливі програми та шкідлива реклама

Термін шкідливих програм охоплює всі програми: віруси, черв'яки, трояни та інші, які зловмисники використовують для заподіяння шкоди та крадіжки конфіденційної інформації. Будь-яке програмне забезпечення, призначене для пошкодження комп'ютера, сервера або мережі, може розцінюватися як шкідливе.

Термін «шкідлива реклама» визначає онлайн-рекламу, яка розповсюджує шкідливі програми. Інтернет-реклама – це складна екосистема, що включає веб-сайти рекламодавців, рекламні біржі, рекламні сервери, мережі ретаргетингу та мережі доставки контенту. Зловмисники використовують цю складність для розміщення шкідливого коду там, де рекламодавці та рекламні мережі не завжди можуть виявити його. Користувачі, які взаємодіють зі шкідливою рекламою, можуть завантажити шкідливі програми на свій пристрій або перейти на шкідливі веб-сайти.

Програми-вимагачі – це шкідливі програми, які блокують використання комп'ютера або доступ до певних файлів на комп'ютері, доки не буде сплачено викуп. Вони часто розповсюджуються як троянські програми – шкідливі програми, замасковані під легальні. Після встановлення програма-вимагач блокує екран системи або певні файли доти, доки зловмисники не отримають викуп.

Для збереження анонімності зловмисники зазвичай вимагають платежі в криптовалютах, наприклад, біткойнах. Вартість викупу варіюється в залежності від програми-вимагача та курсу обміну цифрових валют. Проте зловмисники не завжди розблоковують зашифровані файли після отримання викупу.

Кількість атак програм-вимагачів зростає, продовжують з'являтися нові варіанти програм-вимагачів. Найбільш обговорювані програми-змагачі включають Maze, Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky та WannaCry.

Ботнети

Термін ботнет означає мережу комп'ютерів, спеціально заражених шкідливим програмним забезпеченням з метою виконання автоматичних завдань в інтернеті без дозволу та відома власників цих комп'ютерів. Коли комп'ютер керується ботнетом, він може використовуватися для виконання зловмисних дій. До них відносяться:

- Створення фальшивого інтернет-трафіку на сторонніх веб-сайтах з метою отримання прибутку.

- Використання комп’ютера для участі в розподілених атаках типу «відмова в обслуговуванні» (DDoS-атака), що викликають збої в роботі веб-сайтів.
- Розсилка спаму мільйонам користувачів інтернету.
- Вчинення шахрайських дій та крадіжка особистих даних.
- Атаки на комп’ютери та сервери.

Комп’ютери стають частиною ботнета так само, як і заражаються будь-якою іншою шкідливою програмою: наприклад, при відкритті вкладень електронної пошти, завантаженні шкідливих програм, відвідуванні веб-сайтів, заражених шкідливими програмами. Ботнети також можуть передаватися з одного комп’ютера на інший через мережу. Кількість роботів (заражених комп’ютерів) у ботнеті залежить від здатності заражати незахищені пристрої.

КІБЕРБУЛІНГ

Кібербулінг – психологічне насильство в мережі, переслідування з боку однолітків, що проявляється у вигляді знущань, насмішок, залякувань, інших дій, які негативно впливають на психічний стан підлітка.
Вільне володіння необхідними технологіями дозволяє «агресорам» створювати іменні сайти образливого змісту, поширювати чутки, викладати фото-або відеоматеріали, що принижують гідність дитини або займатися від його імені кібер тероризмом, що загрожує безпеці дітей.
У дитини створюється відчуття безвиході, навіть вдома його не залишає почуття тривоги, він впадає в депресію. Інформаційна атака може призвести до суїциду.
Тінейджери рідко звертаються за допомогою, сумніваючись, що будуть зрозумілими та бояться заборони на користування інтернетом. Необхідно знати, знущання в мережі карається чинним законодавством. Варто відразу звернутися в правоохоронні органи з наданням доказів.

Кібермисливці

Ким є типові інтернет-співрозмовники?
Соціологічні опитування про безпеку дітей-підлітків в інтернет мережі надають такі дані про контакти:

- родичі – 43 %;
- віртуальні друзі – 21%;
- незнайомі люди – 36%.

Однак за великим рахунком віртуальні друзі – теж незнайомці. Таким чином, велику частину свого часу в мережі діти приділяють спілкуванню з сторонніми людьми, діляться своїми переживаннями, секретами, планами. Кібермисливці – хороші психологи, встановивши контакт на форумі, при обміні миттєвими повідомленнями в чаті, вони досить швидко набувають статусу друзів.

Спочатку входять в довіру, оточуючи турботою і розумінням проблем, вислуховують, підтримують. Після цього «друг» поступово вносить до розмови нотки сексуальності, відбувається обмін фото, демонстрація матеріалів еротичного характеру.

Мета кібермисливця – особиста зустріч.

Шахрайство

Шахраї і способи їх дії йдуть в ногу з часом. Необізнаність і наївність дітей роблять їх легкою здобиччю. Один із способів обману – це «виграш». Повідомлення про приз (автомобіль, комп'ютер, телефон тощо). І для цього просто потрібно повідомити дані електронної картки (батьків) і повідомити цифри, які прийшли в смс на номер.

Чи варто пояснювати, до яких наслідків призведе подібна інформація в руках шахраїв? Для того, щоб здійснити покупку в інтернет-магазині, зазвичай достатньо повідомити реквізити банківської картки і смс-код підтвердження платежу. І те, і інше підліток добровільно повідомляє «щедрим дядькам», які обіцяють приз.

Все це і багато іншого виключає саме поняття – безпечний інтернет. Повністю обмежити доступ в кіберпростір неможливо, та й не потрібно. Величезна кількість розвиваючої корисної інформації, літератури, музики і просто спілкування за інтересами, зв'язок з родичами і друзями – все це можна знайти в інтернеті. Достатньо знати правила поведінки, щоб забезпечити особисту безпеку дитини шкільного віку в інтернеті.

КОРИСНЕ ПОСИЛАННЯ

https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti - тут можна знайти всю необхідну інформацію для батьків, дітей та педагогічних працівників.

Зв'язки з громадськістю

Служба у справах дітей та сім'ї - 04212, м. Київ, вул. М. Левка Лук'яненка, 2-Д. e-mail: ssds_obolon@kyivcity.gov.ua

Оболонське управління поліції - адреса: вулиця Героїв полку «Азов» 2-А, пошта: r05_sdz@kyiv.npu.gov.ua, телефон: +380 63 445 8160
Оболонський районний в місті Києві центр соціальних служб - 04211, м. Київ, вул. Йорданська, 7-г; Тел/факс: 426-87-75, e-mail: orcssdm@obolonrda.gov.ua
Територіальний центр соціального обслуговування (надання соціальних послуг) Оболонського району м. Києва - 04209, м. Київ, вул. Озерна 18-а, телефон: 414-09-41, 411-97-75, електронна скринька: tcobl@ukr.net
Управління труда та соціального захисту населення - телефон для консультацій: 467-99-73, 467-82-56, 37445416@kyivcity.gov.ua, вул. Озерна, 18-А.
Районна державна адміністрація - 04205, м. Київ, вул. Лук'яненка Левка, буд. 16, телефон: +38 (44) 419-66-66, +38 (44) 418-38-49, пошта: rda.obolonska@kyivcity.gov.ua

Соціальний педагог 216 школи
Анастасія Зарайська