

Тема 5.11

Як убезпечити себе у віртуальному світі

Вивчаючи тему, ви дізнаєтесь, як вберегти себе від небажаних наслідків користування Інтернетом, навчитесь аналізувати інформацію, отриману з Інтернет-джерел, ідентифікувати зловживання в Мережі, захищати власні права, які можуть бути порушені в Інтернеті. Базові поняття: кіберзлочинність, кібербулінг, гримінг, секстинг.

Ключові здобутки
у вивченні теми

3D

Дізнаємося, як захистити свої права і приватність у віртуальному світі.

Розуміємо, які маркери дій кіберзлочинців.

Діємо, застосовуючи алгоритм дії, коли ви чи ваші знайомі стали жертвою кіберхуліганів.



Обговорюємо

Лист від шахраїв

Вітаємо!!!

Ваша електронна адреса виграла суму 5 000 000 доларів США готівкою. Ваша електронна адреса прикріплена до виграшних номерів 10-14-27-31-32-47-41. Бонусний номер: (41) WVV309553. Дайте відповідь на цей лист, вказавши вашу контактну інформацію. Після того, як вона буде підтверджена, розпочнеться процес оплати.

Зверніть увагу, що процес здійснення оплати потребує додаткової плати з вашого боку в розмірі 350 доларів, яка покриває плату за заявку, обробку, плату за оцінку та авторизацію / вартість розсилки.

Протягом 72 годин надішліть свою відповідь та особисті дані:

- 1) повне ім'я; 2) адреса; 3) вік, стать; 4) діяльність; 5) національність;
- 6) номер телефону.

- Ознайомтеся із текстом. Які факти доводять те, що це шахрайство.
- Чи отримували ви колись такі листи?
- Чи можете навести інші приклади кібершахрайства.
- Як, на вашу думку, не потрапити на «гачок» шахраїв?

Модуль 1

Кіберзлочинність



■ Понад 30 % дитячої порнографії в Інтернеті розміщують провайдери з СНД, і найчастіше у порнографічних роликах та фото фігурують діти з України та Білорусі.

Джерело: Міжнародна правозахисна організація «End Child Prostitution, Child Pornography & Trafficking of Children for Sexual Purposes» (ECPAT International).

Кіберзлочини — це шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, розміщення протиправного контенту, який пропагує екстремізм, тероризм, порнографію, расизм тощо.

Об'єктом кіберзлочинів може стати кожен Інтернет-користувач. Кіберзлочинність — це різні форми агресії, що ґрунтуються на висміюванні, публікації компрометуючих матеріалів, залякуванні або приниженні інших людей. Залякування в Інтернеті — це не тільки глузування, а й виключення когось зі спільноти, публікація фотографій, погрози по телефону. В Мережі така поведінка може бути дуже небезпечною. Інформацію, опубліковану в Інтернеті, дуже важко видалити. Наслідки можуть бути небезпечними: самоізоляція, депресія та, в окремих випадках, спроба самогубства.

Є **чотири загрози**, від яких молоді люди — користувачі Інтернету можуть постраждати:

- спілкування з незнайомцями (грумінг);
- погрози, переслідування (кібербулінг, кіберхуліганство);
- секстинг;
- шахрайство, крадіжки та віртуальні фінансові пастки.

Грумінг — це стеження за дітьми та молоддю онлайн, сексуальні домагання. Відбувається різними способами через контакти з чужими людьми. Наприклад, мова може йти про використання функції чату у грі або через сайти соціальних мереж. Ризики не очевидні, коли грумер відправляє через Інтернет свій контакт дитині та завойовує довіру з подальшим наміром зустрітись.

Основні маркери ризиків:

- використання чатів;
- розмови про секс онлайн;
- відправлення особистої інформації або фотографії людям, з якими знайомство відбулося через Інтернет.

Кібербулінг — це залякування через Інтернет або соціальні медіа. До нього належать: відправлення негативного повідомлення, глузування, розсилання фотографій або відео в Мережі. Поширена думка, що шкільний задвірок, де збиралися неблагополучні та несоціалізовані діти, які, проте, «тримали в руках» усіх інших, перемістився в Інтернет-простір.

Наприклад, кіберхулігани можуть таємно дізнатись номер мобільного телефону та поширювати фотозображення «жертви» або розмістити ваші контактні дані (ім'я, номер телефону) на тому чи іншому сайті і компрометувати дзвінками.

Секстинг — це поширення або обмін сексуально відвертими текстами, фотографіями та відео через мобільний телефон або Інтернет-додатки, такі як *WhatsApp, Facebook, YouTube, Instagram, Twitter* тощо. Ганебність секстингу полягає в тому, що це несанкціоноване перенаправлення інтимного образу особи без її згоди.

Web-активність. Загрози Інтернету

- Об'єднайтеся у групи відповідно до кожної із загроз Інтернету.
- Підготуйте невеликі презентації на основі наявного в Інтернеті матеріалу. Складіть програму дій, як запобігти чи боротися із такими ситуаціями.
- Попрацюйте над маркерами, які дозволяють ідентифікувати небезпеку.

У 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність, яку підписали держави-члени Ради Європи та інші держави з метою опрацювання спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності.

Громадянська активність

Об'єднайтеся в декілька груп. Кожна група має розглянути ситуації кіберзалякування. Учасники/ учасниці мають визначити, що саме найбільше лякає людину, яка потерпає від кіберзалякування.

Що робити, якщо ви стали жертвою кіберзалякування?

Крок 1. Якщо хтось вас образив онлайн, дуже важливо перечекати перші хвилини, поки пориви гніву чи страху пройдуть. Спробуйте утриматися і не відповідати.

Крок 2. Збережіть докази. Якщо вас образили в Мережі, то переконайтеся, що у вас є запис. Відразу ж зробіть скріншот.

Крок 3. Якщо це відбулося декілька разів, розпочніть вести щоденник фіксації, де записуватимете все, що відбувалося. Опишіть всі деталі.

Крок 4. Зверніться до тих, кому довіряєте: друзів/подруг, батьків, учителів/вчительок. Не мовчіть.

Куди звернутися, якщо ти став жертвою кіберзлочину?

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та, відповідно до законодавства України, забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю.

Для отримання онлайн-допомоги та надання даних для оперативного реагування на кіберінциденти, перейдіть за QR-посиланням. Інформацію буде опрацьовано відповідно до Закону України «Про звернення громадян».

Зателефонуйте: 102 або до найближчого відділення поліції.

Модуль 2

Права людини / дитини в Інтернеті

Від часу створення Загальної декларації прав людини, технології активно розвивалися, докорінно змінивши життя людей у всьому світі. Вважається, що права людини поширюються також на Інтернет-простір.

Розділ 5.11 Як убезпечити себе у віртуальному світі

Стаття 31 Конституції України від 1996 р. зазначає: «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом, у випадках, передбачених законом, з метою запобігти злочині чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо».

Конвенція ООН про права дитини

Стаття 13

1. Дитина має право вільно висловлювати свої думки. Це право включає свободу шукати, одержувати і передавати інформацію та ідеї будь-якого роду, незалежно від кордонів, в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів, на вибір дитини.

Стаття 16

1. Жодна дитина не може бути об'єктом свавільного або незаконного втручання у здійснення її права на особисте і сімейне життя, недоторканість житла, таємницю кореспонденції або незаконного посягання на її честь і гідність.

2. Дитина має право на захист закону від такого втручання або посягання.

Аналізуємо ситуацію

- Об'єднайтеся в декілька груп. Кожна група отримує один кейс.
- Обговоріть його і визначте, які правові акти були порушені в цих ситуаціях і які наслідки можуть бути для зловмисників?

Кейс 1. Андрій зустрічається з Мариною. Він попросив її надіслати йому фото в купальнику, оскільки хотів похвалитися перед друзями. Хтось з його друзів виклав фото на сайт знайомств, і Марина почала отримувати дзвінки і пропозиції про зустрічі. Вона була дуже ображена на Андрія, хоча він виправдовувався, що нічого поганого не хотів зробити.

Кейс 2. Один із друзів Сергія розмістив їхню розмову в чаті, де вони обговорюють свою однокласницю. Ті вислови, які вони дозволяли між собою, стали відомі всім однокласникам і знайомим. Сергій не хотів такого резонансу. Дівчина довго не відвідувала школу.

Кейс 3. Олександр познайомився з Настею і розпочав зустрічатися з нею. Розмістив її фото на своїй сторінці і отримав численні принизливі коментарі щодо зовнішності дівчини.

Кейс 4. Ваша ситуація із життя.

Застосуйте набуті знання і досвід

- Складіть Пам'ятку дій, як запобігти чи боротися із інтернет-загрозами:
 - спілкування з незнайомцями (грумінг);
 - погрози, переслідування (кібербулінг, кіберхуліганство);
 - секстинг;
 - шахрайство, крадіжки та віртуальні фінансові пастки.