Тема 5.11. Як убезпечити себе у віртуальному світі?

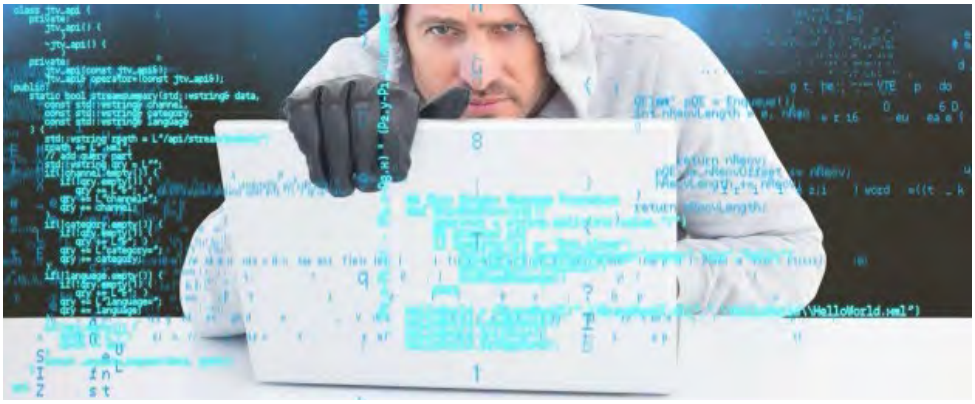
Вивчаючи тему, ви дізнаєтесь, як вберегти себе від небажаних наслідків користування Інтернетом, навчитеся аналізувати інформацію, отриману з Інтернет-джерел, ідентифікувати зловживання в Мережі, захищати власні права, які можуть бути порушені в Інтернеті. Вивчення таких термінів полегшить ваше розуміння і комунікацію: кіберзлочиність, кібербулінг, грумінг, секстинг.

Ключові здобутки у вивченні теми

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

Розуміємо, які маркери дій кіберзлочинців.

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



Модуль 1. Кіберзлочинність

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. На персональному рівні, 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 агресія може бути дуже болючою. Інформацію, опубліковану в Інтернеті, дуже важко видалити. Наслідки можуть бути небезпечними: самоізоляція, депресія та, в окремих випадках, спроба самогубства.

Грумінг — це стеження за дітьми та молоддю онлайн, сексуальні домагання. Відбувається через контакти різними способами з людьми, яких

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)).

вони не знають надто добре. 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.

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.

Є **чотири ключові теми / ситуації**, від яких молоді люди — користувачі Інтернету можуть постраждати:

- спілкування з незнайомцями (грумінг), Інтернет-зловживання;
- погрози, переслідування (кібербулінг, кіберхуліганство);
- секстинг;
- шахрайство, крадіжки та віртуальні фінансові пастки;
- Веб активність. Загрози інтернету.

Об'єднайтеся в чотири 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 кіберзлочиність, яку підписали держави-члени Ради Європи та інші держави з метою опрацювання спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності.

Ознайомтеся з текстом документу: http://zakon3.rada.gov.ua/laws/show/994_575

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 не благополучні та несоціалізовані діти, які, проте, «тримали в руках» усіх інших, перемістився в Інтернет-простір.

Але кіберхулігани також можуть піти далі, таємно дізнавшись номер мобільного телефону, і поширювати фотозображення «жертви» або поставити номер телефону на «поганий» сайт і компрометувати дзвінками.

Обговорюємо

Легше коментувати, критикувати та ображати офлайн чи онлайн? Чому?

Громадянська активність

Об'єднайтеся в декілька груп. Кожна група має вигадати фіктивного персонажа, який був підданий кіберзалякуванню. Учасники/ учасниці повинні визначити сценарій такого цькування і вказати, що саме найбільше лякає цю людину. У підсумку, необхідно написати короткого листа із пропозицією психологічної допомоги або проінформувати дорослих про ці факти. Яку з цих двох форм обрати, група має вирішити самостійно.

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, батьків, учителів. Не мовчіть про образи.

(Джерело: http://edukacjamedialna.edu.pl/lekcje/phishing-i-spam/)

У 2016 р. Уряд прийняв Стратегію кібербезпеки України.

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 посиланням. Інформацію буде опрацьовано у відповідності до Закону України «Про звернення громадян»:https://cyberpolice.gov.ua/declare/.

Телефони: 102 або найближчого відділення поліції.

Модуль 3. Права людини / дитини в Інтернеті

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

Конвенція про права дитини забезпечує доступ до інформації і медіа (стаття 17).

Подібний каталог основних прав можна знайти в Європейській конвенції з прав людини або Конституції України. Стаття 31 Конституції України від 1996 р. зазначає: «Кожному гарантується таємниця *листування, телефонних розмов, телеграфної та іншої кореспонденції.* Винятки можуть бути встановленні лише судом, у випадках, передбачених законом, з метою запобігти злочинові 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, недоторканність житла, таємницю кореспонденції або незаконного посягання на її честь і гідність.

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

Аналізуємо ситуації

Об'єднайтеся в декілька груп. Кожна група отримує один кейс.

Обговоріть його і визначте, які правові акти були порушені в цій ситуації 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 не робив.

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

Веб-активність. Загрози інтернету

Виберіть одну із поданих нижче проблем, дослідіть її в інтернеті. Як вона може реалізовуватись, наведіть приклади, до яких наслідків це може призвести, які існують способи її уникнення, Підготуйте невелику презентацію на основі проведеної роботи. Складіть пам'ятку дій, як запобігти чи боротися із такими ситуаціями:

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