

Урок-тренінг «Інформаційна безпека в Інтернеті»

Мета: розширити й поглибити знання про безпечний Інтернет та соціальні мережі, сприяти обізнаності учнів про небезпеки, які існують в Інтернеті та соціальних мережах і про шляхи їх подолання, мотивувати поширювати цю інформацію у своєму середовищі, розвивати уважність, спостережливість, мовленнєві навички, пам'ять, виховувати любов до родини, навколишнього світу, етичне спілкування між однолітками, дорослими та молодшими друзями.

Завдання:

1. Розширити й поглибити знання про безпечний Інтернет.
2. Ознайомитися з соціальними мережами.
3. Дізнатися про небезпеки, які існують в Інтернеті та соціальних мережах.
4. Розробити шляхи подолання Інтернет небезпек.
5. Толерантно спілкуватися на уроці та поза школою.

Форма проведення: практичне заняття з елементами тренінгу.

Обладнання: маркери, стікери, малюнок 1, 2, аркуші А-4 (2), інтерактивна дошка, доступ до мережі Інтернет, гра.

Хід заняття

*Учись добру в мережі,
Шукай знання й новини,
А сайти злі, підступні,
Обходить ми повинні.*

Василенко Катерина

I. Організаційний момент

Доброго дня!

II. Вступне слово

Для успішної роботи нам необхідно спочатку домовимось про декілька правил:

- ❖ мобільні телефони відключити;
- ❖ говорити все, що думаєте;
- ❖ слухати інших, поважати себе та інших;
- ❖ бути активним учасником;
- ❖ діяти за принципом «тут і зараз».

III. Актуалізація опорних знань.

Сьогодні поговоримо про Інтернет його переваги та про вашу безпеку в Інтернет.

Проведемо мозковий штурм «Про користь Інтернету» (учні називають позитивні можливості Інтернету, роблять записи на дошці або на плакаті)

Крім цього, користь Інтернету полягає в тому, що він ніби стирає кордони між країнами або навіть континентами. Люди без проблем можуть спілкуватися, навіть якщо вони знаходяться один від одного на відстані тисяч кілометрів. Всесвітня павутина дає можливість відшукати нових друзів або навіть любов.

Час в інтернеті з користю можна провести, переглядаючи передачі, отримуючи нові знання, освоюючи іноземні мови. Деяким навіть вдається з допомогою нього отримати нову професію або влаштуватися на хорошу роботу. Та й сам Інтернет може стати стабільним джерелом доходів. За останні кілька років з'явилося дуже багато професій, пов'язаних саме з всесвітньою павутиною.

IV. Сприйняття нового матеріалу, осмислення зв'язків і відносин в об'єктах вивчення.

Інформаційне повідомлення №1.

Що таке Інтернет? *Відповіді дітей.* А що таке соціальні мережі? *Відповіді дітей, допомога педагога.* Сьогодні майже кожен комп'ютер підключений до мережі Інтернет. Шоста частина світу користується мережею, а через 2 роки, за прогнозами аналітиків, це робитиме кожен третій житель планети.

- Як раніше люди обходилися без Інтернету та соціальних мереж?

У давні часи, щоб отримати якусь інформацію про країну, життєвий статус про її народ та інше, люди використовували листи. А листи відправляли човном, пароплавом. «Доставка» інформації тривала місяць – півроку. Потім стільки ж люди чекали відповіді. З появою літаків на відправку листа і відповіді чекали вже не 2 місяці, а 2 тижні. З появою Інтернету лист відправляється і відповідь отримується через кілька секунд.

У наш час сучасна молодь вільно володіє можливостями Інтернету та мобільними телефонами. Сьогодні Інтернетом користується 710029070 людей.

У всьому світі діти та підлітки є найбільшими користувачами інформаційно-комунікативних технологій (ІКТ). Вони широко користуються мобільними телефонами, включаючи пересилки MMS і SMS, шукають інформацію на Інтернет-сторінках, спілкуються «онлайн» в соціальних мережах, створюють свої блоги, спілкуються в чатах, обмінюються музикою та фільмами, обговорюють проблеми на форумах, використовують веб-камеру, скуре та грають в онлайніві ігри.

Ніколи раніше не було так легко, швидко та зручно знайти людей будь-якого віку, соціального статусу, статі, національності, рівня досвіду й дискутувати з ними на які завгодно теми, що є цікавим для певних груп.

Гра «Подорож безпечною Мережею»

Умови гри.

Учасники гри ставлять фішки на лінію старту. Той, хто розпочинає гру, кидає кубик і рухається в напрямку до лінії фінішу, зробивши стільки кроків вперед, скільки очок показує кубик. Якщо фішка гравця попадає в зону «небезпеки» чи «безпеки», він повинен взяти відповідну картку, прочитати інформацію на зворотній стороні, виконуючи написані інструкції. Перемагає той, хто першим дійшов до фінішу. В ході гри беруться картки відповідного кольору з новою інформацією і зачитуються.

Гра «Подорож безпечною Мережею»

Завдання до гри:

Картки «небезпека»:

Я одержав листа з невідомою адресою. Відкривши його, я побачив, що там вірус. Зроби 2 кроки назад.

Я познайомився з новою людиною в Інтернет і не повідомив про це батьків. Зроби 1 крок назад.

Я скористався Інтернетом без дозволу батьків. Зроби 2 кроки назад.

Я завантажив у Мережу неправдиву інформацію. Зроби 1 крок назад.

Я повідомив у Мережу свою адресу. Зроби 2 кроки назад.

Я помістив фото в Мережу моїх друзів без їх дозволу. Зроби 1 крок назад.

Я користуюся забороненими для дітей сайтами. Зроби 1 крок назад.

Я веду непристойні розмови у Мережі Інтернет. Зроби 2 кроки назад.

Картки «безпека»:

Я зберігаю свій пароль у таємниці. Зроби 2 кроки вперед.

Я не повідомляю про себе і батьків приватну інформацію в Мережі. Зроби 1 крок вперед.

Я вірю не всій інформації віртуальних знайомих. Зроби 1 крок вперед.

Я обмежую свій час роботи в Інтернеті. Зроби 2 кроки вперед.

Я повідомлю батьків, якщо віртуальний знайомий запросить мене на побачення. Зроби 2 кроки вперед.

Щоб працювати в Інтернеті, я питаю дозволу батьків. Зроби 1 крок вперед.

Я не відкриваю незнайомі листи. Зроби 2 кроки вперед.

Я не відсилаю незнайомим людям фотографії. Зроби 1 крок вперед. 8. Підсумок заняття.

5 лютого 2019 року вже вкотре відзначають День безпечного Інтернету завдяки ініціативі компанії «Microsoft Україна». Ця організація є засновником веб-ресурсу «Он-ляндія – безпека дітей в Україні».

Інтернет – дуже потужний ресурс, який приховує досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути. Наші експерти виконали випереджувальне завдання і підготували чималий список інтернет - загроз. Прислухайтесь до них і зробіть висновки.

Віруси. Комп'ютерний вірус – це невелика програма, яка написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. комп'ютерних вірусів. Дія вірусів може проявлятися по-різному: від різних

візуальних ефектів, що заважають працювати, до повної втрати інформації. Основними джерелами вірусів є:

- дискета;
- комп'ютерна мережа;
- жорсткий диск;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

Основними ранніми ознаками зараження комп'ютера вірусом є:

- зменшення обсягу вільної оперативної пам'яті;
- уповільнення роботи комп'ютера та завантаження;
- незрозумілі зміни у файлах;
- помилки під час завантаження операційної системи;
- неможливість зберігання файлів у потрібних каталогах;
- незрозумілі системні повідомлення, музичні та візуальні ефекти тощо.

Кібер-хуліганство. Кібер-хуліганство – термін, який використовується для того, аби описати інформаційні атаки на дитину через Інтернет. На відміну від традиційного хуліганства, якого дитина може уникнути, знаходячись вдома, стати жертвою кібер-хуліганства можна й у власній оселі на очах у батьків. Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами є наступні.

Кібер-булінг. Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину (фото, відеозйомки тощо). З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, соціальні мережі, форуми та чати.

Кібер-грумінг. Цей термін розкриває суть ще одного різновиду кібер-хуліганства – входу у довіру до дитини з метою використання її у сексуальних цілях. Шахраї дуже добре ознайомлені з особливостями вікової психології дитини і досить легко можуть встановлювати з нею контакт у соціальних мережах, форумах.

Грифери. Інтернет-шахраї, які заважають учасникам он-лайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

Ця мережа використовується шахраями для розсилання спаму, вірусів та здійснення атак на інші комп'ютери та сервери.

Фішинг – технологія Інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фішинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та он-лайн-фішинг (створення ідентичної копії відомих сайтів Інтернет-магазинів з метою обманювання покупців).

Фармінг. Різновид шахрайства в Інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім відбувається зараження комп'ютера вірусами та шпигунським програмним забезпеченням.

Он-лайн-хижаки «Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в он-лайні, щоб знайти вразливих жертв. Он-лайн-хижаки виявляють по відношенню до них увагу та турботу, пропонують подарунки і таким чином намагаються поступово спокусити своїх жертв, не шкодуючи для цього ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які найчастіше цікавлять дітей. Вони вислуховують дітей і «співчують» їхнім проблемам.

Спам. Це масова розсилка комерційної, політичної та іншої реклами (інформації) або іншого виду повідомлень (у тому числі й підроблених) особам, які не висловлювали бажання їх отримувати. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку; номера дебетової або кредитної картки; коду валідації кредитної картки (CVC) або ідентифікаційного значення картки (CVV); коду соціального страхування. Таке повідомлення, зазвичай, маскується під офіційний лист від адміністрації банку.

V. Тренінг

1. «Нікнейм» в інтернет-спілкуванні

- Проведемо вправу «Квітка»

Питання. Чи знайоме вам слово «Нік»?

Відповіді. «Нік» – це вигадане ім'я, яке вживають користувачі Інтернет-форумів, не називаючи своє справжнє ім'я.

Вправа «Квітка»

Перед початком вправи педагог малює квітку без пелюстків на аркуші ватману або дошці. Психолог роздає кожному учню стікери та дає завдання учасникам.

Вигадайте собі ім'я («нікнейми»), яким вони користуються при спілкуванні в Інтернет-просторі або хотіли б використовувати, та написати його на пелюстці.

Кожний учень виходить до квітки, називає нікнейм, своє реальне ім'я і наклеює стікер із нікнеймом на квітку, так щоб стікер став пелюстком квітки. Аркуш з квіткою розміщується на стіні.

Запитання для обговорення.

- ❖ Навіщо потрібен Нік?
- ❖ Що може приховувати Нік?
- ❖ Чи є переваги у використанні Ніку? Які?

2. Сутність соціальних мереж

Пропоную наступну Вправу «Хто більше?»

Вам необхідно об'єднатися у три групи та за 1 хвилину написати якомога більше назв соціальних мереж. Кожна команда по черзі повинна зачитати по назві, якщо ця назва є в інших групах назви закреслюється. Перемагає та група, у якій залишиться більше незакреслених назв.

Увага на екран, перевіримо чи всі соціальні мережі ви знаєте?

ЗАВДАННЯ

<https://learningapps.org/watch?v=pmwsz0p0t18>

VII. Узагальнення, систематизація і застосування знань.

Задля вашої безпеки я підготувала кожному з вас **правила користування соціальними мережами**

<https://padlet.com/studentffmi/1m46829fod3p>

1. НЕ ПОВІДОМЛЯЙ ПРО СЕБЕ І БАТЬКІВ ПРИВАТНУ ІНФОРМАЦІЮ (домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи), НЕ ВИСИЛАЙ НЕЗНАЙОМИМ ЛЮДЯМ ФОТО.

2. НЕ ВІР ВСЬОМУ, ЩО КАЖУТЬ ПРО СЕБЕ ВІРТУАЛЬНІ ЗНАЙОМІ. Дівчинка познайомилась в соціальній мережі з своїм однолітком, хлопчиком, якого звали Войтек. Вони почали спілкуватися в мережі. Аня пише: «Привіт, я Аня, мені 13 років, я шукаю друзів».

Хлопчик їй відповідає: «Привіт, Аня, я Войтек, мені також 13 років і я хочу зустрітися з тобою». А насправді, цей Войтек дорослий чоловік, який обманює дівчинку, переслідуючи інші цілі, і не тільки її. Дуже часто, спілкуючись в мережі уявляєш собі одну людину, а насправді вона зовсім інша.

3. НЕ ПОГОДЖУЙСЯ НА ЗУСТРІЧ З ВИПАДКОВИМ ЗНАЙОМИМ. АБО РОБИ ЦЕ В ЛЮДЯНИХ МІСЦЯХ І ЗА УЧАСТЮ БАТЬКІВ.

4. ОБМЕЖУЙ СВІЙ ЧАС ПЕРЕБУВАННЯ В СОЦІАЛЬНІЙ МЕРЕЖІ.

5. БАТЬКИ МАЮТЬ ЗНАТИ, ЧИМ ТИ ЗАЙМАЄШСЯ, КОЛИ СИДИШ БІЛЯ КОМП'ЮТЕРУ!

6. НЕ ОБРАЖАЙ ІНШИХ, НЕ ЛАЙСЯ, БУДЬ ЧЕМНИМ.

7. ТРИМАЙ ПАРОЛЬ КОМП'ЮТЕРА У ТАЄМНИЦІ.

8. ЯКЩО ОПИНЯЄШСЯ В СКЛАДНІЙ СИТУАЦІЇ ПОГОВОРИ З БАТЬКАМИ.

2. Вправа «Хто надіслав тобі листа?»

- Повернемося до нашої квітки. Підготуємо невеликі листи однокласникам, напишіть позитивне побажання або просто хороші слова на стікері. А потім наклеїмо їх поряд з будь-яким зі стікерів з нікнеймами на аркуші з квіткою. Кожен з вас має наклеїти побажання до чужого нікнейму так, щоб власники нікнеймів не бачили, хто надає побажання. По завершенню Ви зможете забрати свої нікнейми і листи на ваше ім'я.

Спробуйте вгадати, хто надіслав Вам це «повідомлення».

Отже, зробимо висновок. У 99% учасники не можуть вгадати відправника повідомлення. Так само відбувається і зі спілкуванням в Інтернет просторі. Дуже складно перевірити, хто саме пише тобі листи, спілкується з тобою. Якщо учасники групи добре знайомі між собою, вони можуть

вгадувати відправника за почерком. В Інтернет просторі не існує почерків, тому ти ніколи не знаєш хто знаходиться по той бік комп'ютера або мобільного телефону.

- ми багато нового з вами дізналися, стали розумнішими. Пропоную виконати вправу «Знайди правильне рішення»

На Вашу електронну адресу надійшли листи.

Лист 1. Привіт! Мене звати Сашко. Мені 17 років. Я живу в Києві. Шукаю друзів по переписці. Я люблю комп'ютерні ігри, читати книги, дивитися телевизор. Я мрію подорожувати. Хочу побувати в Лондоні

- Дайте відповідь на лист, можливо щось запропонуйте?

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двоховерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

- Яку б коректну відповідь Ви надіслали б адресату?

Дякую.

Підведемо підсумок:

- Отже, що таке Інтернет?
- У чому його переваги?
- Яка небезпека чекає на користувачів Інтернет?
- Що для себе взяли найголовніше?

Сьогодні без соціальної мережі не може обійтися жоден з Вас, проте пам'ятай користуватися треба розумно. Нехай біля ваших комп'ютерів будуть ці

Шість правил розумного користувача Інтернету:

1. **Я буду поводитись в Інтернеті чемно і не ображати інших.**
2. **Я буду залишати негарні веб-сайти.**
3. **Я буду зберігати свій пароль в таємниці.**
4. **Я буду розповідати своїм батькам про проблеми й користуватися їхньою підтримкою.**
5. **Я буду шукати цікаві веб-сайти й ділитися посиланнями зі своїми друзями.**
6. **Я знаю, що можна бути легко обманутим і не буду повідомляти реальні імена, адреси й номери телефонів.**

VIII. Підведення підсумків уроку. Слово вчителя.

Безпечний Інтернет

Не можу уявити

Життя без Інтернету,

Що всі куточки світу

Заплів в свої тенета.

Лиш кнопку я натисну –

Відкриваються в вікні

Новин велика збірка

І правила, й статті.

Встають переді мною

Найвищі в світі гори.

Ліси стоять стіною,

Хлюпочуть хвилі моря.

Я побуваю в шахті

І в космос піднімуся.

Життя людини – це найдорожчий Божий дар на Землі. Цінуйте і бережіть його перебуваючи в Інтернеті!

З подругою в контактi

Я легко поділюся.

Та є у «павутинні»

Картинки нехороші,

І сайти підозрілі,

Настроєні вороже.

А є й такі там сайти,

Мов вовк в овечій шкурі –

Поки їх розпізнаєш,

Вони тебе обдурять.

Учись добру в мережі,

Шукай знання й новини,

А сайти злі, підступні,

Обходить Ви повинні!

Пропоную виконати вправу «Знайди правильне рішення»
На Вашу електронну адресу надійшли листи.

Лист 1. Привіт! Мене звати Сашко. Мені 17 років. Я живу в Києві. Шукаю друзів по переписці. Я люблю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні

- Дайте відповідь на лист, можливо щось запропонуйте?

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

- Яку б коректну відповідь Ви надіслали б адресату?

Дякую.

Пропоную виконати вправу «Знайди правильне рішення»
На Вашу електронну адресу надійшли листи.

Лист 1. Привіт! Мене звати Сашко. Мені 17 років. Я живу в Києві. Шукаю друзів по переписці. Я люблю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні

- Дайте відповідь на лист, можливо щось запропонуйте?

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

- Яку б коректну відповідь Ви надіслали б адресату?

Дякую.

Пропоную виконати вправу «Знайди правильне рішення»
На Вашу електронну адресу надійшли листи.

Лист 1. Привіт! Мене звати Сашко. Мені 17 років. Я живу в Києві. Шукаю друзів по переписці. Я люблю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні

- Дайте відповідь на лист, можливо щось запропонуйте?

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

- Яку б коректну відповідь Ви надіслали б адресату?

Дякую.

Пропоную виконати вправу «Знайди правильне рішення»
На Вашу електронну адресу надійшли листи.

Лист 1. Привіт! Мене звати Сашко. Мені 17 років. Я живу в Києві. Шукаю друзів по переписці. Я люблю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні

- Дайте відповідь на лист, можливо щось запропонуйте?

Лист 2. Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

- Яку б коректну відповідь Ви надіслали б адресату?

Дякую.

*Учись добру в мережі,
Шукай знання й новини,
А сайти злі, підступні,
Обходить ми повинні.*

Шість правил розумного користувача Інтернету:

- 1. Я буду поводитись в Інтернеті чемно і не образжати інших.*
- 2. Я буду залишати негарні веб-сайти.*
- 3. Я буду зберігати свій пароль в таємниці.*
- 4. Я буду розповідати своїм батькам про проблеми й користуватися їхньою підтримкою.*
- 5. Я буду шукати цікаві веб-сайти й ділитися посиланнями зі своїми друзями.*
- 6. Я знаю, що можна бути легко обманутим і не буду повідомляти реальні імена, адреси й номери телефонів.*

Інтернет- (від англ. Internet) — всесвітня система взаємополучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів. Інтернет також називають мережею мереж.

Соціальні мережі- соціальна структура, утворена індивідами або організаціями. Вона відбиває різноманітні зв'язки між ними через різноманітні **соціальні взаємовідносини**, починаючи з випадкових знайомств і закінчуючи тісними родинними зв'язками.

Віруси- Комп'ютерний вірус — це невелика програма, яка написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій

Кібер-хуліганство. Кібер-хуліганство — термін, який використовується для того, аби описати інформаційні атаки на дитину через Інтернет. На відміну від традиційного хуліганства, якого дитина може уникнути, знаходячись вдома, стати жертвою кібер-хуліганства можна й у власній оселі на очах у батьків. Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами є наступні.

Кібер-булінг. Одна із форм переслідування дітей та підлітків за допомогою ІКТ. Для цього можуть створюватися сайти, на яких розміщуються матеріали, що компрометують дитину (фото, відеозйомки тощо). З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, соціальні мережі, форуми та чати.

Кібер-грумінг. Цей термін розкриває суть ще одного різновиду кібер-хуліганства — входу до довіри до дитини з метою використання її у сексуальних цілях. Шахраї дуже добре ознайомлені з особливостями вікової психології дитини і досить легко можуть встановлювати з нею контакт у соціальних мережах, форумах.

Грифери. Інтернет-шахраї, які заважають учасникам он-лайн-ігор спокійно грати. Вони періодично пошкоджують ігрових персонажів, блокують певні функції гри та викрадають як персонажів, так і їхнє віртуальне життя.

Ця мережа використовується шахраями для розсилання спаму, вірусів та здійснення атак на інші комп'ютери та сервери.

Фішинг — технологія Інтернет-шахрайства, розроблена з метою крадіжки конфіденційної інформації. Різновидами її є поштовий фішинг (отримання листа від «державної установи» або «банку» із вимогою повідомити особисті дані) та он-лайн-фішинг (створення ідентичної копії відомих сайтів Інтернет-магазинів з метою обманювання покупців).

Фармінг. Різновид шахрайства в Інтернеті, коли оманливим шляхом користувач потрапляє на ідентичну копію відомих сайтів. Потім відбувається зараження комп'ютера вірусами та шпигунським програмним забезпеченням.

Он-лайн-хижаки «Хижаки» встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, електронною поштою або через дошки повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників з метою вирішення власних проблем. Хижаки часто відвідують такі зони в он-лайні, щоб знайти вразливих жертв. Он-лайн-хижаки виявляють по відношенню до них увагу та турботу, пропонують подарунки і таким чином намагаються поступово спокусити своїх жертв, не шкодуючи для цього ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які найчастіше цікавлять дітей. Вони вислуховують дітей і «співчують» їхнім проблемам.

Спам. Це масова розсилка комерційної, політичної та іншої реклами (інформації) або іншого виду повідомлень (у тому числі й підроблених) особам, які не висловлювали бажання їх отримувати. Метою розповсюдження підроблених повідомлень є отримання від споживачів таких особистих відомостей: власного імені та імені користувача; номера телефону й адреси; пароля або PIN-коду; номера банківського рахунку; номера дебетової або кредитної картки; коду валідації кредитної картки (CVC) а бо ідентифікаційного значення картки (CVV); коду соціального страхування. Таке повідомлення, зазвичай, маскується під офіційний лист від адміністрації банку.

1. НЕ ПОВІДОМЛЯЙ ПРО СЕБЕ І БАТЬКІВ ПРИВАТНУ ІНФОРМАЦІЮ (домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи), **НЕ ВИСИЛАЙ НЕЗНАЙОМИМ ЛЮДЯМ ФОТО.**

2. НЕ ВІР ВСЬОМУ, ЩО КАЖУТЬ ПРО СЕБЕ ВІРТУАЛЬНІ ЗНАЙОМІ. Дівчинка познайомилась в соціальній мережі з своїм однолітком, хлопчиком, якого звали Войтек. Вони почали спілкуватися в мережі. Аня пише: «Привіт, я Аня, мені 13 років, я шукаю друзів».

Хлопчик їй відповідає: «Привіт, Аня, я Войтек, мені також 13 років і я хочу зустрітися з тобою». А насправді, цей Войтек дорослий чоловік, який обманює дівчинку, переслідуючи інші цілі, і не тільки її. Дуже часто, спілкуючись в мережі уявляєш собі одну людину, а насправді вона зовсім інша.

3. НЕ ПОГОДЖУЙСЯ НА ЗУСТРІЧ З ВИПАДКОВИМ ЗНАЙОМИМ. АБО РОБИ ЦЕ В ЛЮДЯНИХ МІСЦЯХ І ЗА УЧАСТЮ БАТЬКІВ.

4. ОБМЕЖУЙ СВІЙ ЧАС ПЕРЕБУВАННЯ В СОЦІАЛЬНІЙ МЕРЕЖІ.

5. БАТЬКИ МАЮТЬ ЗНАТИ, ЧИМ ТИ ЗАЙМАЄШСЯ, КОЛИ СИДИШ БІЛЯ КОМП'ЮТЕРУ!

6. НЕ ОБРАЖАЙ ІНШИХ, НЕ ЛАЙСЯ, БУДЬ ЧЕМНИМ.

7. ТРИМАЙ ПАРОЛЬ КОМП'ЮТЕРА У ТАЄМНИЦІ.

8. ЯКЩО ОПИНЯЄШСЯ В СКЛАДНІЙ СИТУАЦІЇ ПОГОВОРИ З БАТЬКАМИ.