## Година спілкування «Загальні правила безпеки при використанні соціальних мереж»

**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.

### Хід заняття

**Інтернет.** Що це? Останні роки це слово щільно увійшло в наше життя. Це цікавий та захоплюючий світ, який дозволяє тобі дізнаватись про світ цікавого, спілкуватись з людьми в різних кінцях світу не виходячи з власної кімнати, грати в цікаві ігри та ділитись з іншими своїми думками та захопленнями. Сучасна людина не уявляє собі життя без Інтернету.

Саме тому сьогоднішнє наше заняття присвячено темі безпечного інтернету.

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку особистості, спілкування, навчання, дозвілля. Але разом з тим, в Інтернеті приховано досить багато небезпек. Знання цих небезпек дозволить їх уникнути. Тому прислухайтеся та зробіть висновки.

**Віруси.** Комп'ютерний вірус – це невелика програма, яка написана програмістом високої кваліфікації, здатна до само розмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тисяч комп'ютерних вірусів, дія яких може проявлятися по-різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації.

Основними джерелами вірусів є:

* дискета, на якій знаходяться заражені вірусом файли;
* комп'ютерна мережа, в тому числі електронна пошта та Інтернет;
* жорсткий диск, на який потрапив вірус у результаті роботи із зараженими програмами;
* 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, а також зміни розмірів та дати останньої модифікації файлів;
* помилки під час завантаження операційної системи;
* неможливість зберігання файлів у потрібних каталогах;
* незрозумілі системні повідомлення, музичні та візуальні ефекти тощо.

**Кібер-хуліганство** – термін, який використовується для того, щоб описати інформаційні атаки на дитину через Інтернет. Варіанти кібер-хуліганства досить різноманітні. Основними їх різновидами їх є наступні.

**Кібер-булінг** – одна з форм переслідування дітей та підлітків за допомогою Інтернету. Для цього можуть створюватися сайти, на який розміщуються матеріали, що компрометують дитину. З метою кібер-булінгу використовуються сервіси миттєвих повідомлень, електронна пошта, соціальні мережі, ігрові та розважальні сайти, форуми та чати.

**Виманювання інформації** про дитину та її сім'ю з метою подальшого пограбування або шантажу. Це відбувається завдяки використанню певних Інтернет-технологій. Шпигунське програмне забезпечення. Це комп'ютерні програми, які збирають інформацію без відома власника комп'ютера. Збірна інформація може містити:

* список рекламних сайтів, на які переходить користувач під час перебування в Інтернеті;
* особисту інформацію: ім'я, адресу та номер телефону;
* Web – сторінки, які відвідує користувач, та відомості форм, які він заповнює на цих сторінках;
* перелік файлів, які завантажує користувач на свій комп'ютер;
* інформацію, необхідну для доступу до Інтернету.

**Спам –** це масова розсилка комерційної, політичної та іншої реклами або інформації, або іншого виду повідомлення 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 і адреси; паролі; номер банківського рахунку; номер кредитної картки; коду соціального страхування. Таке повідомлення,зазвичай, маскується під офіційний лист від адміністрації банку.

**Недостовірна інформація.** Інформація, якою користуються учні чи студенти при підготовці рефератів є часто недостовірною, неповною або застарілою. Якщо при підготовці рефератів недостовірна чи неправдива інформація до життєвого ризику не призводить, то у випадку пошуку інформації, що стосується здоров'я, ризик істотно збільшується. В Інтернеті на різноманітних форумах легко знайти інформацію, яка є не лише антинауковою, але і небезпечною для життя, якщо нею скористатися.

А зараз давайте поговоримо про соціальні мережі та виконаємо декілька вправ.

**Вправа «Хто більше?»**

Об'єднайтеся у дві групи та за 1 хвилину напигіть якомога більше назв соціальних мереж. Кожна команда по черзі зачитує по назві, якщо ця назва є в обох групах, то назви закреслюють. Перемагає та група, у якій залишиться більше не закреслених назв.

**Запитання для обговорення**

1. Навіщо створюються соціальні мережі?
2. Скільки часу в день вони можуть забрати?
3. Назвіть альтернативи «сидінню» в мережі.

**Вправа «Колаж»**

Об'єднайтеся у дві групи та зробіть колаж за темою « Соціальні мережі – «ЗА» і «ПРОТИ». Презентуйте свої роботи на ватманах.

Отже, знайте загальні правила безпеки при використанні соціальних мереж:

1. Контролюйте інформацію про себе, яку ви розміщуєте, намагайтеся не використовувати особисті дані, які легко знайти в мережі.
2. Без дозволу батьків не надавайте приватну інформацію про себе: прізвище, імена членів своєї родини, номер телефону,адресу, номер школи, місце прогулянок, час,коли вдома відсутні батьки, номери банківських карток,наявність цінних речей вдома та інше.
3. Будьте обережні при переході на посилання, які ви отримуєте в повідомленнях від інших користувачів або друзів.
4. Щоб не розкрити адреси електронної пошти своїх друзів, не дозволяйте соціальним мережам сканувати адресну книгу вашого ящика електронної пошти.
5. Намагайтеся не користуватися соціальними мережами з місця навчання, оскільки ви можете забути закрити свою сторінку.
6. Не варто виконувати тих операцій, які коштують грошей.
7. Будьте ввічливі при спілкуванні у мережі.

**Підведення підсумків заняття**