Інтернет-загрози для учнів

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості, спілкування, навчання, дозвілля. Але разом з тим, в Інтернеті приховано досить багато небезпек як для дітей, так і для дорослих. Знання цих небезпек дозволить їх уникнути.

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. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .EXE та .COM, хоча останнім часом все більшої популярності набувають віруси, що розповсюджуються через систему електронної пошти.

Основними ранніми ознаками зараження комп'ютера вірусом є:

- зменшення обсягу вільної оперативної пам'яті;
- уповільнення роботи комп'ютера та завантаження;
- незрозумілі (без причин) 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.

Нелегальні та шкідливі матеріали, що не відповідають віковим особливостям і негативно впливають на фізичне та психічне здоров'я дітей (небажаний контент)

Контент для дорослих.

Понад 95% батьків вважають найголовнішою небезпекою «дорослий» контент, який можуть переглядати діти, зокрема порноконтент. Інтернет може надати дітям швидкий та (у більшості випадків) безкоштовний доступ до порноконтенту. Необхідно лише ввести ключові слова або фрази для того, аби отримати тисячі посилань на сайти із дорослим контентом. Практично гарантовано, що дитина зіткнеться із порноконтентом, навіть якщо вона і не шукала його.

Пропагування сексуального насилля над дітьми, жорсткої поведінки, шкідливих звичок тощо.

Перегляд матеріалів, що містять сцени насилля та жорсткості по відношенню до людей або тварин, перешкоджає нормальному формування моральних цінностей та може завдати психологічних травм.

Онлайн - звабленння учнів.

Злочинці намагаються завоювати довіру дитини, щоб втягти її в ситуацію сексуального насилля. Знайомство та встановлення довіри між злочинцем та жертвою відбувається під час спілкування в мережі Інтернет: миттєві повідомлення, блоги, соціальні мережі, дошки оголошень та інше.

Діти не лише можуть легко знайти порнографічні сайти, вони так само легко можуть отримати інформацію, яка підштовхне до скоєння злочину, наприклад:

інформацію про виготовлення та розповсюдження наркотиків, способи крадіжки грошей або про те, як зробити саморобну вибухівку. Необхідно лише набрати відповідну ключову фразу і відповідь на екрані монітора!

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. На жаль, багато дорослих навіть і не підозрюють про це.

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, форуми та чати.

Кібер-грумінг. Цей термін розкриває суть ще одного різновиду кібер-хуліганства – входження 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. Починаючи із віртуального спілкування та входячи у довіру до дитини, злочинці пропонують потоваришувати, а потім поступово переходять до розмов про зустріч у реальному житті та переводять тему спілкування у сексуальну площину. Як варіант, виділяють ще один вид кібер-грумінгу - наполегливе чіпляння в мережі із сексуальними пропозиціями, розмови на теми сексу, насильства та (або) виготовлення, розповсюдження і використання матеріалів зі сценами насильства над дітьми (у більшості випадків – сексуального).

Виманювання інформації про дитину та її сім'ю з метою подальшого пограбування, шантажу.

Шпигунське програмне забезпечення. Це комп'ютерні програми, які збирають інформацію без відома власника комп'ютера. Зібрана інформація може містити:

- список рекламних сайтів, на які переходить користувач під час серфінгу в Інтернеті;
- особисту інформацію: ім'я, адресу та номер телефону;
- Web-сторінки, які відвідує користувач, та відомості форм, які він заповнює на цих сторінках (треба пам'ятати про обережність при повідомленні паролів своєї електронної пошти та акаунтів у соціальних мережах; не слід називати дівоче прізвище матері – подібна інформація використовується при оформленні банківських документів у якості ключових слів);
- перелік файлів, які завантажує користувач на свій комп'ютер;
- інформацію, необхідну для доступу до Інтернету: номер з'єднання модему телефонної лінії, ID та інше.

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 онлайн -

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.

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 «співчувають» їхнім проблемам. Вони намагаються позбавити комплексів молодих людей, поступово вводячи у свої розмови сексуальний контекст або показуючи відверто сексуальні матеріали.

Деякі «хижаки» працюють швидше, одразу ж втягуючи дітей у розмови на сексуальну тему. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижаки також можуть спонукати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

Створення у мережі профайлів для виявлення інтересів дитини

Як зазначалося вище, соціальні мережі набувають все більшої популярності у дітей та підлітків. Більшість існуючих соціальних мереж заохочують користувачів надавати якомога більше особистої та конфіденційної інформації (прізвище та ім'я, домашня адреса, номери телефонів, місце роботи, інтереси та нахили). Шахраю неважко обрати потенційну жертву та вивчити її за наданою у профайлі інформацією. До речі, користувачі викладають подібну інформацію у більшості випадків добровільно, не усвідомлюючи можливих наслідків такої необережності. Діти охоче розміщують фотографії, які можуть також бути використані шахраями у своїх власних цілях. Іноді підлітки охоче розміщують свої пікантні фотографії, не замислюючись над тим, що опублікована в Інтернеті інформація залишається у мережі назавжди.

Торгівля людьми

Враховуючи вищенаведені ризики, легко змоделювати декілька ситуацій в Інтернеті, які можна використати з метою торгівлі людьми: від сайтів, що пропонують роботу (роботодавці можуть виявитися звичайними торговцями людьми), до шантажу з метою викрадення жертви та її подальшого продажу.

Пам'ятайте, спілкування, одержання інформації у становленні особистості людини посідає одне з найважливіших місць. Але завжди слід враховувати, що найважливіше для людини є її здоров'я і фізичне, і психічне , і соціальне. При будь-якій загрозі збоку мережі Інтернет не бійтеся звертатися до батьків, вчителів та інших дорослих, яким ви довіряєте.