**Формування безпечної поведінки в Інтернеті**

 Сьогоднішня можливість отримувати доступ до всього, що підключено до Інтернету, це розкіш, яку ми не можемо дозволити собі втратити. Проте чим більше людей використовують онлайн системи, тим більше кіберзагроз.

 Проте у віртуальному онлайн світі звичайній людині можна нашкодити цілком реально, як і у реальному житті. Шахраї постійно відточують свої вміння і шукають способи ошукати людей, Інтернет — є одним із шляхів, які допомагають їм в цьому. Тому обережними слід бути не тільки дітям, а й дорослим. Адже навіть з віком люди не перестають бути жертвами. Зараз особливо актуальний тиск аферистів. Я думаю, що кожен мав дзвінки на свій телефон з невідомих номерів, від невідомих компаній, які вже володіють особистими персональними даними. Тому обережними потрібно бути ВСІМ!

 В наш час зловмисники можуть роздобути ваші персональні дані, історію хвороби, приватні переписки у месенджерах, проникнути у смартфон дитини і почати спілкуватися з нею, отримати доступ до ваших рахунків та онлайн-банкінгу або до ваших гаманців із криптовалютами.

 Якщо озирнутись навколо себе, то одними з найвразливіших місць віртуального світу є мобільний телефон із доступом до соціальних мереж, месенджерів, та десятків мобільних додатків часто невідомого походження, де учні з легкістю діляться приватною інформацією, яка, на перший погляд, не є критичною.

 Хакерів та зловмисників в інтернеті цікавить будь-хто, навіть якщо ви не публічна людина. Вас можуть зламати для атаки на ваших колег, керівництво, родичів, або навіть просто випадково.

 Для того, щоб не стати жертвою, потрібно іноді виконувати прості вправи та підтримувати так звану кібергігієну.

 Пофантазуйте і замисліться, яку інформацію могли б використати проти вас потенційні зловмисники, і спробуйте максимально унеможливити такий сценарій. **Кібергігієна - це, перш за все, самооцінка своїх ризиків.** Так само, як мити руки перед їжею, важливо дотримуватись таких правил зі своїми гаджетами:

1.   Не підключатись до публічного WiFi. Використовуйте краще мобільний інтернет. Якщо дуже треба підключитись, то робіть це із використанням VPN (не безкоштовного).

2.   Не переходьте за посиланнями, які вам невідомо чому присилають, навіть якщо це ваші знайомі зі знайомих акаунтів. Часто зловмиснику потрібно від вас тільки один клік за посиланням, щоб отримати доступ до вашого профілю.

3.   Не додавайте незнайомих людей у друзі в фейсбук, бо вони можуть відправляти інформацію вашим колегам вже у статусі вашого друга.

4.   Змінюйте паролі кожні 2-3 місяці, використовуйте різні складні паролі, які важко вирахувати, та двофакторну аутентифікацію не через смс, а через додаток.

5.   Завжди встановлюйте автоматичні оновлення версій програмного забезпечення. Якщо вже вийшло оновлення, цілком можливо, що у старій версії є вразливості.

6.   Робіть регулярні бекапи важливої інформації, сегментуйте дані.

7.   Перевіряйте, щоб сайт, яким ви користуєтесь, був https а не http.

Спробуйте "загуглити" своє ім'я і подивіться, скільки відкритої інформації про вас є в інтернеті. Де і з ким ви відпочивали, як звати ваших батьків, яке дівоче прізвище вашої мами, або навіть як звати ваших домашніх улюбленців.

Всі ці дані можуть використати проти вас. Потрібно привести до ладу таку публічну інформацію, налаштувавши персональні параметри у соцмережах, і періодично перевіряти це.

Персональні дані наразі - найцінніше, що є у віртуальному світі.

Перед тим, як завантажувати будь-який додаток, бажано дізнатись, хто розробники, як вони зберігають ваші дані і як використовують.

Нині на рівні держави також запускають багато цікавих ініціатив: E-health, ДІЯ та інші проєкти. Приємно розуміти, що ми одні з небагатьох країн світу, хто запустив і продовжує запроваджувати такі послуги онлайн.

 **РЕКОМЕНДАЦІЇ ДЛЯ ВЧИТЕЛІВ**

Дотримуйтеся цих правил самі й розкажіть учням:

1.                  **Переконайтеся, що всі пристрої надійно захищені (паролями) і заблоковані тоді, коли ви ними не користуєтесь.** Якщо вам потрібно вийти з класу, заблокуйте всі пристрої, які використовували, або завершіть сеанс роботи чи вийдіть з облікового запису. Встановіть на всіх пристроях ліцензійну антивірусну програму та стежте за тим, щоби вона регулярно оновлювалася.

2.                  **Встановіть правила в школі, де й коли можна користуватися мобільними пристроями.** А також правила, що учнів можна фотографувати лише після отримання згоди батьків / опікунів / самих учнів на це. Ці правила мають бути закріплені в шкільній політиці щодо онлайн-безпеки. Така політика має встановлювати ще й порядок реагування на інциденти, пов’язані з безпекою дітей, зокрема, у цифровому середовищі. Так, у школі може бути призначений спеціальний координатор для обліку та реєстрації порушень та інцидентів, пов’язаних з онлайн-безпекою, задля формування цілісного уявлення про наявні в школі проблеми та тенденції, що вимагають уваги.

3.                  **Забезпечте фільтрацію й моніторинг даних, які передаються через шкільну мережу, встановивши необхідні програми.** Допомогти їх встановити можуть інтернет-провайдери. Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільну мережу. Такі системи фільтрації та контролю контенту допомагають звести до мінімуму передавання неприйнятного (наприклад, насильницького чи порнографічного) контенту в шкільній мережі. А системи фільтрації даних допомагають відстежувати, хто, що, коли й на якому пристрої завантажує. Такий механізм є одним зі способів запобігання кібербулінгу.

4.                  **Пам’ятайте, що ваші дії та слова в інтернеті можуть вплинути на вашу онлайн-репутацію, а також на репутацію навчального закладу.** Ви як користувач/-ка інтернету залишаєте свій цифровий слід – адже різні сайти, соціальні мережі, платформи, відповідно до своїх політик, збирають дані про вашу онлайн-активність. Перевіряйте інформацію, яку поширюєте в соціальних мережах. Перед тим як опублікувати інформацію, подумайте, хто може її побачити. Розповідайте дітям про важливість онлайн-репутації та як правильно її формувати.

5.                  **Слідкуйте за своєю професійною комунікацією**. Для будь-яких контактів між працівниками школи, учнями, батьками чи іншими зацікавленими сторонами завжди використовуйте шкільну електронну пошту замість особистої. У деяких випадках кодекс ділової етики, якщо він погоджений у школі, може передбачати заборону на контакти з учнями на платформах, які не мають стосунку до школи. Наприклад, у месенджерах чи соцмережах. Також рекомендується встановити в школі чіткі правила – як для працівників, так і для учнів – щодо проведення відеоконференцій чи занять у віддаленому режимі. Наприклад, правила, який вигляд має мати місце для проведення уроків, наявність фото профіля тощо.

6.                  **Сприяйте формуванню цифрових навичок та цифрової грамотності дітей.** Говоріть із ними про це на уроках. Намагайтеся включити до навчальних планів аспекти цифрової грамотності. Проводьте заходи в школі про онлайнбезпеку дітей. Водночас, показуйте високий рівень власної цифрової компетентності. І не забувайте проводити регулярну перевірку всіх заходів у школі на дотримання онлайн-безпеки дітей та її можливого удосконалення.

7.                  **Навчайтеся нового та постійно покращуйте навички цифрової грамотності**. Будьте в курсі того, які ризики на дітей можуть чекати в інтернеті, як діти проводять свій час у мережах. Це допоможе вам краще зрозуміти дітей та встановити з ними довірливі взаємини швидше й легше.

Пам’ятайте, що **інтернет – одночасно й ризик, і можливість для дітей**. Тому освітянам варто робити все можливе, щоби зробити цифрове освітнє середовище максимально безпечним для дітей.