*Безпека в цифровому середовищі*

**Кілька простих порад для дітей та їх батьків,**

 **як безпечно користуватись Інтернетом,**

**щоб не накликати на себе неприємностей.**
**ДІТЯМ**

1. Нікому без дозволу батьків не давати особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи, свої паролі.

2. Якщо знайдете якусь інформацію, що турбує вас, негайно повідомте про це батьків.

3. Ніколи не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті. Якщо все ж таки це необхідно, то спочатку потрібно спитати дозволу батьків, а зустріч повинна відбутися в громадському місці й у присутності батьків.

4. Не відповідати на невиховані і грубі листи. Якщо одержите такі листи не з вашої вини, то повідомте про це батьків, нехай вони зв’яжуться з компанією, що надає послуги Інтернет.

5. Розробити з батьками правила користування Інтернетом. Особливо домовитися з ними про прийнятний час роботи в Інтернеті і сайти, до яких ви збираєтесь заходити.

6. Не заходити на аморальні сайти і не порушувати без згоди батьків ці правила.

7.Не робити протизаконних вчинків і речей в Інтернеті.

8.Не шкодити і не заважати іншим користувачам.

**БАТЬКАМ**

1. Підвищуйте власну комп’ютерну та інтернет-обізнаність. Щоб убезпечити свою дитину у мережі Ви маєте знати про інтернет, принаймні, не менше за неї.

2. Станьте для дитини порадником. Опановуйте інтернет разом. Повідомте дитині, що вона може звернутися до Вас у будь-якій ситуації. Якщо в інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось не зрозуміло, хвилює або загрожує, дитина завжди має звертатися по допомогу до Вас. Інформація та послуги в інтернеті не завжди безпечні, тому перш ніж завантажувати, копіювати чи встановлювати будь-що з інтернету, дитина має порадитися з Вами. Навчіть перевіряти інформацію з мережі за допомогою додаткових запитів і звернення до перевірених джерел.

3. Станьте для своєї дитини другом у соціальних мережах, або попросіть близьких знайомих зробити це. Якщо Ваша дитина не бажає підтверджувати дружбу з Вами, попросіть Ваших друзів молодшого віку подружитися з нею у соціальних мережах. Ви завжди маєте знати, чим займається та з ким спілкується Ваша дитина у Мережі.

4. Встановіть на мобільному телефоні своєї дитини безкоштовну соціальну послугу «Батьківський контроль». Регулярно оновлюйте антивірус.

5. Створіть територію безпечного Інтернету. Використовуйте поновлюваний перелік безпечних для дитини сайтів. Запропонуйте дітям пізнавальні, цікаві та захоплюючі інтернет-ресурси. Щоб захистити дітей від ризиків віртуального світу, використовуйте поновлюваний список рекомендованих сайтів для дітей.

***21 правило цифрової безпеки***

Важливо розуміти, що цифрова безпека – це процес. Ви не можете сьогодні щось встановити, придбати якусь магічну кнопку, яка б дозволила захистити усі ваші дані, інформацію ваших друзів, колег і т. д. Ви постійно дізнаєтесь про нові загрози та про нові інструменти, які з’являються – щось використовуєте, а щось ні.

Важливо розуміти, на які загрози ви можете натрапити.

* Використовуйте ліцензійне програмне забезпечення скрізь, зокрема на телефонах і планшетах, робочих та домашніх комп’ютерах.
* Регулярно оновлюйте все програмне забезпечення.
* Встановлюйте антивірусні програми
* Встановлюйте пароль на вхід у пристрій (телефон, планшет, комп’ютер).
* Вам потрібен саме складний унікальний пароль. Кожен обліковий запис повинен мати власний пароль.
* Використовуйте менеджер паролів.
* Не використовуйте ненадійні поштові сервіси, соціальні мережі, месенджери.
* Розділяйте облікові записи.
* Блокуйте пристрої.
* Використовуйте повнодискове шифрування пристроїв.
* Якщо ви користуєтесь останніми моделями iPhone або телефонами преміум- 10. Видаляйте історію з браузера та кеш.
* Не зазначайте очевидні відповіді для відновлення доступу до свого облікового запису.
* Не використовуйте для відновлення доступу незахищені поштові скриньки.
* Користуйтесь секретними месенджерами, якщо вирішили вести таємну переписку.
* Використовуйте месенджери з шифруванням від пристрою до пристрою – Signal, WhatApp, Viber, а в Telegram - секретний чат.
* В такому випадку у сервіс-провайдера немає можливості читати вашу переписку.
* Не клікайте на підозрілі посилання.
* Не ловіться на фішинг. Фішинг - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.
* Робіть резервні копії важливих файлів в хмарних сховищах.
* Робіть двофакторну авторизацію для важливих облікових записів.
* Використовуйте технології VPN (Virtual Private Network — віртуальна приватна мережа) при підключенні до публічного Wi-Fi.
* Використовуйте мережу Tor, якщо хочете бути анонімними.
* Змінюйте дефолтний пароль на домашньому Wi-Fi-роутері.