Цифрова гігієна: яких правил варто дотримуватися в інтернеті?

Кожен з нас у середньому щоденно проводить понад 3,5 години в інтернеті та соцмережах. Із карантином ця цифра суттєво збільшилася і тепер люди майже увесь час перебувають онлайн. Саме тому варто приділяти особливу увагу безпеці в інтернеті та цифровій гігієні.

Цифрова гігієна — це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий пароль на всіх акаунтах, застосовувати двофакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення застосунків.

Також важливо вміти відрізняти фішингові листи від справжніх. Фішинг – це спроба оманливим шляхом отримати особисту інформацію користувачів в Інтернеті. Як правило, це підроблені електронні листи, оголошення або сайти.

Обов’язково потрібно перевіряти електронну адресу. "https" — безпечний протокол передачі даних. Особливо варто звертати увагу на це під час розрахунків в інтернеті та коли йдеться про банківські чи фінансові сервіси.

Зловмисники у фішингових листах або на сайтах можуть запитувати таку інформацію:

- імена користувачів і паролі, зокрема прохання змінити пароль;

- номери банківських рахунків та кредитних карток;
- PIN-коди;
- дату народження і т. д.

Тому, при отриманні електронного листа із запитом особистої інформації, варто бути обережними: не натискати посилання та не надавати особисті дані, доки не будете впевнені, що лист справжній.

Якщо надійшов підозрілий лист потрібно:

- переконатися, що електронна адреса й ім’я відправника збігаються
- перевірити, чи правильно написано назву компанії, від якої лист
- перш ніж натиснути на посилання, навести на нього курсор (URL-адреса має відповідати опису)
- не завантажувати файли, що мають невідоме вам або потенційно небезпечне розширення

Радимо дотримуватися цих простих правил цифрової гігієни .

У 2016 році Center for Cyber Safety and Education вивчав використання інтернету дітьми. Вчені опитали учнів 4-8 класів і з’ясували, що 40% з них спілкувалися з незнайомцями в мережі. Звіт Hootsuite і We Are Social показує, що у 2019 році людина проводить в інтернеті 6,5 годин в день. І зовсім не обов’язково, що весь цей час вона там навчається або працює. Цифри вражають, адже ми часто нехтуємо цифровою безпекою, про неї не розповідають ні у школах, ні дома, а багато з нас не чули термін «цифрова гігієна». Наповнимо цей прикрий пробіл і почнемо з відповіді на питання «Навіщо це потрібно»:

- Щоб захиститись від ризиків: контентних, комунікаційних, споживчих і технічних. Щоб навчити дитину адекватно реагувати на взлом облікового запису, наприклад, або кібербулінг. Щоб вона

розуміла, чому дуже небажано викладати в мережу фотографії квартири, школи й привласнювати постам геолокацію.

- Щоб уникнути інформаційного перевантаження. Щодня нас занурюють в бурхливий потік інформації самої різної якості. Але наш мозок не вміє всю її обробляти. Він втомлюється. Від цього знижується концентрація, розсіюється увага, ми перестаємо аналізувати явища, піддаємось рекламним маніпуляціям і так далі.
- Щоб раціонально використовувати свій час. Головне правило соцмереж — заробити на нашій увазі. Чим більше часу ми «залипаємо», тим більше грошей заробляє платформа. І все ніби нічого, але ми ж безцільно скролимо стрічку й витрачаємо час. А могли б присвятити його важливому, корисному заняттю.
- Щоб зрозуміємо, що дійсно важливо. Скільки з нас, прокинувшись, хапають телефон, щоб перевірити пошту і месенджери? А як часто ми бачимо там дійсно важливі повідомлення? І хочемо ми насправді читати це все?

Як захистити свої та дитячі дані

- Чистимо цифровий слід. Піти з усіх соцмереж і месенджерів, швидше за все, не вийде. Але пройтися налаштуваннями приватності та поставити/зняти потрібні галочки ми можемо.
- Відписуємось від непотрібних спільнот. Перегляньте і проаналізуйте на корисність контент у вашій стрічці новин. А потім безжалісно почистьте підписки. Причому списку друзів це теж стосується. Якщо ваш майстер манікюру нескінченно викладає фото чужих нігтів і для вас цей контент не несе ніякої цінності — тихесенько натисніть mute, unfollow, скасуйте підписку на оновлення.
- Стежимо за оновленнями безпеки пристроїв. Викачуємо програми лише в перевірених джерелах, наприклад: в App Store або Google Play.
- Перевіряємо паролі. Коли ми або наші діти використовуємо прості паролі на кшталт «password», «qwerty», дати народження або щось в цьому дусі, головна мета зловмисника — відгадати його та увести обліковку. Пароль повинен бути складний, складатися з цифр і букв, бажано — в нижньому і верхньому регістрі.

- Поговоріть з дітьми про те, що розповідати свій пароль друзям — погана ідея.
- Встановлюємо правила використання гаджетами. Те ж дослідження американського Центру з кібербезпеки показало, що 49% дітей заходили в інтернет після 23:00 і пізніше. Щоб бути спокійним, що син або дочка сплять ночами, а не шаряться по інстаграму, заведіть традицію здавати на ніч телефони на підзарядку. Так дитина виспиться, буде бадьорий в школі, а його рука не буде автоматично тягнутися до гаджета.
- Стежимо за поведінкою дитини. Кібербулінг — нова форма прояву агресії. Якщо «професійний втикальщік в телефон» раптово перестав використовувати гаджет — це сигнал для батьків.
- Вчимо пильності. Загрози цифрової безпеки існують не тільки в смартфонах і ноутбуках. Наприклад, існують шахраї, які використовують банкомати для отримання інформації про кредитні картки.
- Користуємося інструментами для генерації та зберігання паролів. Наприклад, сервіс Lastpass.