«Кібербезпека та інформаційна безпека»

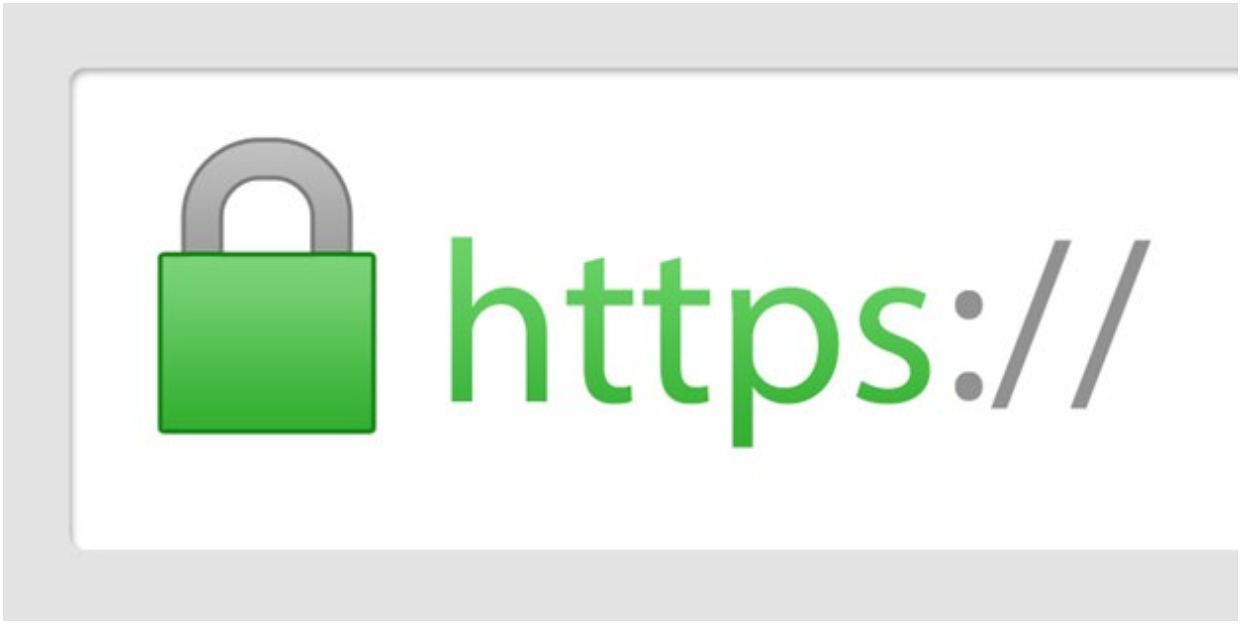
Чи завжди ви почуваєте себе безпечно в Інтернеті? Навіть, якщо на перший погляд Інтернет здається цілком безпечним місцем для роботи, спілкування та розваг, насправді це не зовсім так. На нас постійно чекають небезпеки, і це не перебільшення!

А чи існують правила, яких ми маємо дотримуватись працюючи в Інтернет? Що нам потрібно знати і чого дотримуватися, щоб залишитися здоровою людиною з усіх боків.

Інтернет – це лише інструмент, яким ми користуємся, щоб отримати відповіді на свої питання та задовольнити деякі потреби:

- Інтернет – безмежний простір для отримання інформації;
- через Інтернет ми можемо замовити і оплатити різні товари;
- в Інтернеті можна скачувати і розміщувати ігри, фотографії, фільми, музику, відео;
- в соціальних мережах можна вільно спілкуватися, знайомитися без обмежень;
- Інтернет містить велику кількість реклами;
- Інтернет – простір, де ти можеш бути ким завгодно.

Але віртуальний світ часто буває небезпечним. Ось деякі поради.



Як захистити свої особисті дані. Фішинг - атаки

Ознаки фішинг-атак і шахрайських повідомлень електронної пошти

Фішинг – один з видів шахрайства, спрямований на викрадення цінних особистих даних користувача, таких як номери кредитних карток, паролі, дані про банківські рахунки і т.д. Шахраї можуть розсилати безліч повідомлень, які відправлені ніби надійними веб-вузлами (наприклад, від банку) і містять запит особистих даних.

Як розпізнати шахрайське повідомлення електронної пошти?

Наводимо кілька прикладів фраз, що часто використовуються при проведенні фішинг-атак:

- «Підтвердіть свій обліковий запис». Представники компаній не повинні робити запит по електронній пошті про паролі, імена користувачів, номери соціального страхування та іншу особисту інформацію.
- «Якщо ви не дасте відповідь протягом 48 годин, ваш обліковий запис буде заблокований». Такі повідомлення викликають відчуття терміновості, щоб змусити людину відповісти не роздумуючи;
- «Клацніть на посилання, наведене нижче, щоб отримати доступ до свого облікового запису».

Фішинг-повідомлення зазвичай розсилаються масово і не містять ані імені, ані прізвища отримувача. У випадку фішинг-атаки повідомте компанію, чиє ім'я було використано. Для цього створіть нове повідомлення у вашій поштовій скриньці, вкладіть у нього шахрайське повідомлення і відправте на адреси відповідних організацій. Терміново змініть паролі для всіх облікових записів, якими ви користуєтесь у мережі.

Деякі сайти містять багато реклами, яка привертає увагу, відволікаючи від мети, з якою ви зайшли в Інтернет. Якщо у вас весь час з’являються вспливаючі вікна, ви можете позбутися них, клацнувши мишкою «закрити». Якщо ви купуєте щось у інтернеті, зв’язуйтеся з продавцем через телефон. Перевіряйте інформацію, яку читаєте у рекламі

Використання громадських комп'ютерів та відкритих мереж Wi-Fi несе серйозні ризики безпеки для вашої інформації. Такі комп’ютери можуть містити шкідливе програмне забезпечення для контролю переміщень в інтернет-мережі, збору паролів. А у відкритих мережах Wi-Fi зловмисники можуть збирати дані про відвідувані вами сторінки та навіть перехопити ваші паролі. У ситуації, коли підключення до мережі необхідне і єдиним варіантом є відкриті мережі, постарайтеся не користуватися засобами перевірки пошти, соціальних мереж, не реєструйтеся на будь-яких сайтах, і, тим більше утримайтеся від проведення банківських операцій та електронних покупок.

Як безпечно спілкуватися в мережі

Соціальні мережі сприяють вашій творчості, дозволяють постійно контактувати з друзями, надають багато можливостей – обмінюватися і переглядати відео, фото, слухати музику. І все це в одному місці. Але як уникнути небезпек і отримати користь і задоволення від відвідування соціальних мереж?

Фотографії і фільми – важлива частина мережевого простору. Завжди гарно подумайте, перш ніж завантажити свої фотографії чи відео. Зображення залишаються на сайтах надовго (інколи навіть після того, як ви їх видалили). Вони можуть бути скопійовані, відредаговані і використані де завгодно. Подумайте, чи хочете ви цього. Пам'ятайте, коли ви викладаєте щось у мережі, це стає доступним мільйонам людей в світі. Про що ви маєте подумати у першу чергу, коли оновлюєте свої сторінки у соціальних мережах? Про власну безпеку. Захистіть сторінки налаштуваннями приватності – так ви зможете контролювати тих, хто має доступ до вашої інформації. Оберіть людей, які матимуть доступ до ваших даних. Персональний профіль – це джерело інформації про вас. Додавання деталей – цікавий і веселий процес, але краще утриматися від додавання деякої інформації. Дату народження, адресу, номер мобільного краще не публікувати. Частіше перевіряйте персональні налаштування ваших сторінок, щоб захистити себе від небажаних контактів. Створюйте складні паролі і зберігайте їх у таємниці. Поважайте себе та інших у мережі. Не використовуйте образливих висловлювань, записуючи коментарі.

У своїй електронній скриньці відкривайте лише повідомлення від тих людей, яких ви знаєте і яким довіряєте. Не забувайте прочитувати тему повідомлення. Якщо тема викликає підозри і не схожа на те, про що ви могли б поговорити з друзями, не відкривайте ніякі вкладення. Це можуть бути віруси. Не пересилайте повідомлення-ланцюжки, у яких просять переслати їх десятьом друзям, а інакше відбудеться щось неприємне, жахливе. Домовтесь з друзями не пересилати подібний спам. Вони несуть загрозу, адже через них збирають інформацію чи поширюють віруси. Спілкуючись у чатах, будьте обережними і не повідомляйте особисту інформацію. Уникайте безпосередніх контактів з невідомими партнерами по спілкуванню. Якщо ви домовились з кимось про реальну зустріч, обов'язково повідомте про це дорослих.

Пам'ятайте: щоб ви не використовували для спілкування – мобільний телефон, комп'ютер тощо – правила безпеки завжди однакові.

Як безпечно слухати і завантажувати музику та як уникнути небезпеки, граючи в онлайн ігри:

- завжди читайте інформацію, написану в оголошенням дрібним шрифтом, перш ніж програти чи завантажити якусь мелодію чи рингтон;
- перш ніж завантажити пісню, прочитайте відгуки інших користувачів;
- якщо ви використовуєте якісь програми обміну файлами, переконайтесь, що вони встановлені вірно і не дозволяють стороннім особам отримувати доступ до всіх файлів вашого комп'ютера;
- поважайте авторське право. Якщо автор пісні не виклав її на своєму офіційному сайті для вільного завантажування, ви можете опинитися у категорії порушників авторських прав.

Ігри бувають найрізноманітнішими – від коротких і простих, до складних, у яких беруть участь багато гравців. Усі вони дуже різні, але якою б гра не була і на чому б ви не грали (комп'ютер, телефон, ігрова консоль), правила безпеки залишаються однаковими:

- вивчіть спеціальну мову ігор;
- якщо у процесі гри хтось почне використовувати нецензурні вирази у вашу адресу, ви можете зробити скріншот і надіслати скаргу адміністрації сайту, використавши скріншот як доказ;
- якщо гра несе для вас небезпеку, повідомте дорослих.
- не забувайте про мережевий етикет. Завжди будьте ввічливими у спілкуванні;

- переконайся, що при реєстрації у грі ви не видали особистої інформації.
- прочитайте терміни гри й умови використання даних сайтів, перевірте, чи є спеціальні функції безпеки;
- нехай ваші батьки знають ваш псевдонім, як перевірити ваш онлайн акаунт на предмет безпеки, якщо раптом щось піде не так;
- встановіть часові обмеження для себе. Використайте, наприклад, будильник у мобільному телефоні, щоб слідкувати за часом.

Слід всім пам'ятати, що необхідно вчитися користуватись Інтернетом із розумом!
А краще – знайдіть себе в реальному житті
та станьте в ньому авторитетною та вагомою людиною.

Тест: Чи в кібербезпеці ви?

Пропонуємо Вам по новому поглянути на свою кібербезпеку та проаналізувати її, пройшовши тест зі знання базових правил кібербезпеки за цим посиланням:
https://www.epravda.com.ua/tests/2018/07/18/638509/