Кожна сучасна людина, щодня проводить час в інтернеті. Але інтернет це не тільки джерело інформації і можливість спілкуватися на відстані, але і загроза комп'ютерної безпеки. Ви можете завантажити з мережі комп'ютерний вірус, Ваш обліковий запис або адресу електронної пошти може зламати зловмисник, Ваші особисті дані можуть використовувати ... Щоб цього не сталося, ***потрібно дотримуватися правил безпеки в Інтернеті, про які ми розповідаємо нижче.***

9 правил безпеки в Інтернеті

1.Використовуйте надійний пароль.

Перше і головне правило збереження Ваших даних, облікових записів, поштових відправлень – **надійний пароль**! Багато разів хакери зламували сторінки в соціальних мережах або поштові адреси через те, що користувач ставив простий пароль. Ви ж не хочете, щоб Вашу особисту переписку дізнався хтось чужий? Використовуйте завжди індивідуальні і складні паролі, що складаються з літер, цифр і спеціальних символів. Виключіть використання паролів за замовчуванням, не зберігайте паролі в Ваших гаджетах і браузерах. Використовуйте генератор паролів, щоб отримати надійний пароль.

Чому ми говоримо про це в першу чергу? Статистика говорить про те, що люди мало приділяють уваги «парольній політиці». Третій рік поспіль найпопулярнішим паролем в світі є «123456». Підібрати такий пароль до Ваших порталів і персональних даних зловмисникові буде не важко.

Якщо в секретному питанні Ви вказали дівоче прізвище матері, яка зараз є у відкритому доступі на її сторінках у соцмережах, обов'язково змініть секретне запитання. Регулярно здійснюйте зміну паролів, забезпечуючи кожен раз їх конфіденційність. Змінюйте паролі хоча б раз в три місяці.

Якщо Ви працюєте за комп'ютером, до якого мають доступ інші люди (на роботі або в інтернет кафе), не зберігайте паролі в браузері. В іншому разі, будь-хто, хто має доступ до цього комп'ютера, зможе зайти на сайт, використовуючи Ваш пароль.

Пароль – це Ваш найбільший секрет, як ключ від замка вхідних дверей у Ваш будинок.

2.Використовуйте антивіруси.

Будь-якому комп'ютеру чи гаджету можуть нашкодити шкідливі програми (або віруси). Вони можуть скопіювати, пошкодити або знищити важливу інформацію, відстежити Ваші дії і навіть вкрасти гроші з рахунку.

Програми «Трояни», «Шпигуни» – їх безліч різновидів, а суть одна – все це шкідливі віруси!

Для захисту комп'ютера необхідно **встановити антивірус**. Не зберігайте програмні продукти з сумнівних джерел (файлообмінних мереж і торрентів). Не відкривайте і не зберігайте підозрілі файли – відразу видаляйте. Не відповідайте на незрозумілі Вам розсилки.

І головне – не відвідуйте ресурси з сумнівною репутацією, які викликають у Вас (або у Вашої антивірусної програми) підозри. Сумніваєтеся – не натискайте «ТАК» або «ENTER».

Тут можна провести просту паралель – тримаємося подальше від вірусів, миємо руки регулярно милом. Адже наші комп'ютери та гаджети потребують чистоти.

3. Не розголошуйте свої особисті дані.

Нікому не передавайте свої **конфіденційні дані** (логін, пароль), свідоцтво про народження, паспортні дані, адреса і прописку, і навіть Ваші фотографії. Такі «цифрові сліди», якщо їх створити, можуть тягнутися за Вами все життя. Можуть нашкодити Вам на шляху до досягнення поставленої мети. Ігноруйте в мережі Інтернет подібні запити.

Виходить дивно – вдома і на роботі ми зберігаємо свої документи в сейфі, закриваємо на ключ. Ми розуміємо їх важливість. А потім за неперевіреним запитом відкриваємо сейф, дістаємо документи, фотографуємо і посилаємо за допомогою ресурсів в мережі Інтернет. Кількість осіб, які можуть отримати доступ до таких послань, навіть важко прогнозувати.

4.Будьте обережні зі спамом і рекламою.

- Якщо Ви хочете завантажити якийсь матеріал з інтернету на сайті, де не потрібна реєстрація, але від Вас вимагають ввести адресу своєї електронної пошти, то, швидше за все, на Вашу адресу будуть висилати рекламу або спам. У таких випадках **користуйтеся одноразовими поштовими скриньками**. А найкраще – нічого не завантажуйте з сумнівних сайтів. Якщо це можливо, просто скопіюйте і перенесіть в свій документ. А потім просто самостійно обробіть отриману інформацію.
- Не **натискайте на красиві банери або рекламні блоки на сайтах**, якими б привабливими та інформативними вони не здавались. У кращому випадку, Ви допоможете автору сайту отримати гроші, а у гіршому – отримаєте вірус. Використовуйте плагіни для браузерів, які відключають рекламу на сайтах.

- **Не відкривайте листи від невідомих Вам користувачів** (адрес). Або листи з сповіщенням про виграш в лотереї, в якій Ви просто не брали участь.

Не натискайте на випливаючі вікна, в яких написано, що Ваш профіль у соціальній мережі заблокований. Це витівки зловмисників! Якщо Вас раптом заблокують, Ви дізнаєтеся про це, зайшовши в цю соціальну мережу, або адміністрація відправить Вам електронного листа.

- Пам’ятайте: **банки, сервіси та магазини ніколи не розсилають листів з проханням перейти за посиланням**, змінити свій пароль, ввести номер банківської карти і секретний код підтвердження або повідомити інші особисті дані!
- **Якщо Вам в месенджер прийшло повідомлення від знайомого з проханням терміново вислати грошей** або ж лист з незрозумілим файлом з проханням відкрити, **нічого не відправляйте і не відкривайте**! Спочатку передзвоніть йому і упевніться, що аккаунт не був зламаний зловмисниками.

5.Будьте обережні з платежами і покупками онлайн.

- Щоб ніколи не втрачати гроші на непомітних платежах, не купувати додаткових послуг помилково і точно заплатити за потрібні, завжди **читайте правила** перед тим, як поставити галочку навпроти чекбоксу «згоден» і перейти до оплати.
- Періодично **перевіряйте на телефоні Ваші підписки**, на які саме розсилки Ви підписані. Є такі сервіси, після відключення яких, з часом можуть поновитись. І для цього вони не питають у Вас дозволу. Є домовленість з мобільним оператором. Якщо Ви помітили, що сума рахунку за місяць збільшилася, терміново перевіряйте підписки, які можливо включилися автоматично і вже щодня списується плата за них. Для деяких додатків і сервісів передбачено безкоштовний тестовий період (наприклад, на 2-3 місяці), після чого Ви повинні самостійно відключити послугу. Якщо Ви цього не зробите, підписка може бути автоматично продовжена і стане платною, а з вказаної при реєстрації картки почнуть списувати гроші.

- Купуючи в інтернет-магазинах, **зберігайте здоровий скептицизм**. Пам’ятайте: ціна не може бути занадто низькою, тим більше, якщо Ви розраховуєте придбати оригінальну продукцію бренду. Вивчіть історію магазину в мережі, перевірте наявність контактів, з’ясуйте, чи можна туди приїхати і познайомитися вживу. Читаючи відгуки, зверніть увагу, щоб вони були різними. Замовні відгуки пишуть люди, яким доводиться робити це багато разів в день, тому такі тексти ніби написані за шаблоном. Подивіться, як на відгуки реагують продавці. Зверніть особливу увагу на негативні: якщо їх відпрацьовують, це хороший знак (причому ситуація повинна бути конкретна, містити номер замовлення тощо). Це означає, що продавець реальний і магазин функціонує.
- **Заведіть окрему (можна віртуальну) карту для платежів в інтернеті**. Якщо для оплати в інтернеті Ви користуєтеся своєю звичайною картою, не зберігайте на ній великі суми грошей. Підключіть в своєму банку СМС-інформування про всі операції по картах і рахунках. Так Ви зможете швидко помітити, якщо Ваша карта буде скомпрометована, і заблокувати її.

6.Робіть резервне копіювання даних.

Дотримуйтесь правила «3-2-1»: створіть одну основну копію і дві резервні. Збережіть дві копії на різних фізичних носіях, а одну – в хмарному сховищі (Google Диск, Яндекс.Диск тощо). Не забувайте підключати до цього процесу всі пристрої: смартфони, планшети, комп’ютери / ноутбуки.

7.Виключайте Wi-Fi, коли ним не користуєтеся.

Обов’язково вимкніть функцію автоматичного підключення до Wi-Fi в телефоні або планшеті. Не довіряйте неперевіреними Wi-Fi-з’єднанням, які не захищені паролем. Найчастіше саме такі мережі зловмисники використовують для крадіжки особистих даних користувачів.

Не заходьте в онлайн-банки та інші важливі сервіси через відкриті Wi-Fi-мережі в кафе або на вулиці. Скористайтеся мобільним інтернетом.

8.Встановіть безпечний режим для дитини.

Для цього створіть окремий обліковий запис на сайті обраної Вами пошукової системи або використовуйте дитячі пошуковики: “Гогуль” або “Спутник.дети”.

9.Перевіряйте сайти, якими користуєтеся.

Звертайте увагу на адресу сторінки, де Ви опинилися: якщо вона відрізняється хоча б на один символ (наприклад, paypa1.com замість paypal.com), введіть його вручну самостійно.

Шахраї створюють сайти, на яких Ви нібито можете безкоштовно подивитися або завантажити фільм, що Вам сподобався, але спочатку потрібно залишити телефон або відправити повідомлення на короткий номер. Таким чином, з Вашого рахунку можуть списати значну суму за СМС, а сам телефон потрапить в базу спамерів.

За посиланням http://www.tcinet.ru/whois/ можна дізнатися, коли був створений сайт. Зловмисники зазвичай створюють сторінки-одноденки, які дуже швидко закривають.

Користуючись цими правилами безпеки в інтернеті, Ви істотно зменшите ризик отримати вірус на свій комп’ютер або втратити обліковий запис на улюбленому сайті.