Десять правил безпеки мобільних пристроїв

Купуйте смартфон у перевірених місцях

Купуючи пристрій із невизначеного джерела, ми ризикуємо не тільки проблемами з гарантією, а й тим, що на ньому будуть шкідливі програми або модифіковане програмне забезпечення. У кращому випадку шахрай може використовувати їх, щоб закидати нас великою кількістю реклами. У гіршому, що вже серйозніше, вкрасти наші дані, у тому числі для входу в систему електронної пошти або онлайн-банкінгу. Особливо небезпечно купувати старі смартфони, оскільки колишній господар міг завантажити й встановити шкідливий застосунок, який потім принесе неприємності вам.

Встановлюйте найсвіжіше оновлення системи вашого пристрою

в програмному забезпеченні завжди є й будуть прогалини. І це проблема будь-якої операційної системи, у тому числі тієї, що встановлена на вашому смартфоні. Особливо це стосується пристроїв на Android OS, адже вона заснована на відкритому ядрі. У її розробках і доробках беруть участь багато розробників. Звідси й деякі нестиковки та проблеми. Хоча останнім часом не менше проблем й у iPhone, які, нагадаємо, працюють на iOS.

Паролі завжди повинні бути складними

- Про проблему слабких паролів експерти говорять вже багато років. Так, згідно зі звітом британської компанії NCSC за 2019 рік, пароль, який найчастіше зустрічається у світі, як не дивно, 123456. Як ви можете здогадатися, такий рядок символів не зможе ефективно захистити ваш обліковий запис. Аналогічно – дата народження, друга половина імені або слово PASSWORD не працюватимуть ефективно.

Використовуйте біометрію

- Паролі, незалежно від того, наскільки вони продумані, можуть потрапити до чужих рук із різних причин. Рецептом вирішення цієї проблеми є біометрія. Він захищає пристрій таким чином, що його може використовувати тільки його власник. Додатковою перевагою використання біометрії є зручність. Усе, що вам потрібно, всього лише один дотик пальця, і доступ до всього пристрою відкритий. Без паролів, без запам’ятовування, але все ж у безпеці.

Встановлюйте програми лише з надійних джерел

Схема зараження проста: користувач шукає застосунок, знаходить його інсталяційний файл, встановлює, знімає позначку з усіх погоджень і використовує його. Усе працює, як треба. Проте, вірус встановлений поряд із правильним застосунком, який працює у фоновому режимі та намагається його ігнорувати. Однак протягом цього часу він має доступ, наприклад, до SMS-повідомленнями й платіжних даних.

Щоб уникнути подібних несподіванок, встановлюйте застосуноки тільки з офіційного магазину, який призначений платформі (наприклад, App Store, Google Play, Galaxy Store, AppGallery та інші) або ж з офіційного веб-сайту виробника

Не підключайтеся до невідомих, загальнодоступних Wi-Fi-мереж

Шахраї не дрімають і намагаються саме в таких місцях зловити на вудку неуважних, безтурботних власників пристроїв. Справа в тому, що вони створюють помилкові, відкриті точки доступу, іноді з дуже схожою, а іноді й ідентичною назвою. Таким способом вони намагаються отримати важливу інформацію за допомогою смартфона. Працює це досить просто. Шахраї за допомогою ноутбука та спеціальної антени створюють свою точку доступу. Ви підключаєтеся до неї, а вони отримують доступ до вашої електронної пошти, акаунтів у соціальній мережі, персональних даних, у тому числі й до банківських карток.

Конфіденційні дані повинні мати додатковий захист

У сучасних смартфонах майже всіх виробників є спеціальні утиліти та програми, які допоможуть зберегти найважливіші персональні дані користувачів. Щоправда, мало хто з нас їх активує та користується ними. Для цього достатньо пройти в розділ Конфіденційність та ввімкнути цю функцію. У різних виробників вони по-різному називаються, але суть їх роботи майже однакова.

Постійне увімкнення геолокації

Не варто відключати геолокацію, хоча часто користувачі бажають її приховати. Адже з допомогою додаткових сервісів в будь-який момент можна виявити телефон, навіть якщо він був викрадений або загублений. Наприклад, Google розробила для таких випадків сервіс Find My Phone для Android. Він не тільки дозволяє активувати дзвінок (навіть якщо до цього гаджет був поставлений на беззвучний режим), але й заблокувати пристрій і видалити всі особисті дані на ньому. Іншими словами, власник телефону зможе самостійно контролювати його навіть на відстані. Єдине що для цього потрібно – підключення до інтернету.

Вкрадений або втрачений iPhone – що робити?

Якщо ваш пристрій iOS був вкрадений, ви, імовірно, зможете використати функцію «Знайти мій iPhone», яка розташована в налаштуваннях. За замовчуванням вона ввімкнена.

Застосунок «Знайти мій iPhone» дозволяє не тільки знайти втрачений пристрій, алей перемкнути його у втрачений режим, повністю деактивувати та навіть віддалено видалити всі дані. Усе це можна зробити з веб-браузера на будь-якому комп’ютері або з будь-якого іншого пристрою на iOS.

Вкрадений або загублений Android-смартфон – що робити

Якщо у вас смартфон на базі системи Google, то інструкції виглядають дуже схожими на ті, що описані вище. У цьому випадку знадобиться застосунок під назвою «Android Device Manager» або комп’ютер із веб-браузером.

Увійдіть у застосунок або на веб-сайт із пошуку Android-смартфонів. Виберіть свій втрачений смартфон зі списку ваших пристроїв. Ви побачите карту з його поточним місцезнаходженням.