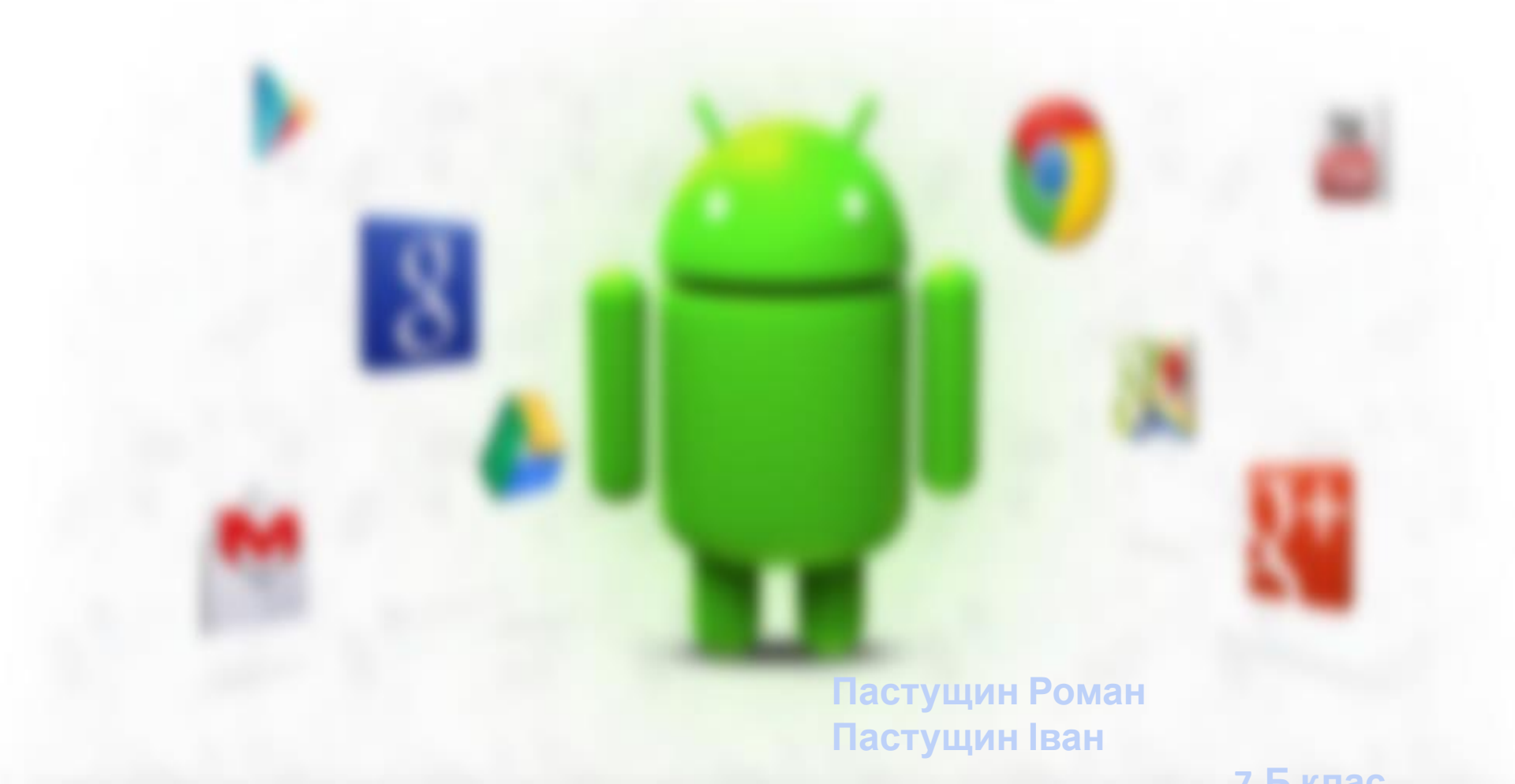
Мобільні віруси – це загроза чи



Пастущин Роман
Пастущин Іван

7-Б клас

ПРОЕКТУ

проект, щоб допомогти вам з проблемами або розказат[illegible]сь нове у IT-сфер[illegible]

Тож почнемо показ проекту по темі

IT-сфера* - це процеси, методи пошуку, поширення інформації тощо. (більше на Wikipedia)

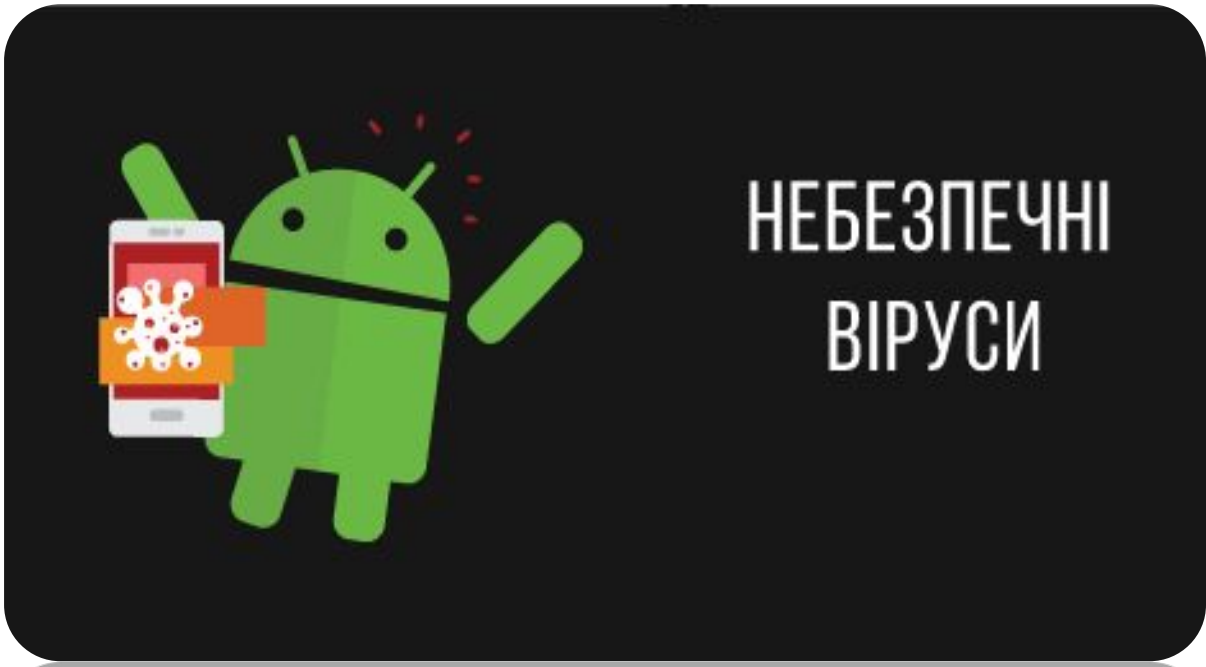
Що ж таке мобільні віруси?

Мобільні віруси – це непомітні маленькі програми, які порушують роботу мобільного пристрою Android, Apple (або інші)* та можуть видалити данні пристрою й поширити їх в Інтеренет*. Віруси на пристроях вперше були згадані ще в 2000 році. Вони виглядали як набір звичайних команд, які передавалися через SMS*. Коли їх намагалися видалити, мобільні віруси блокували телефон.

Android, Apple (або інші)* - це операційні системи, які підтримують роботу мобільного пристрою.
Інтернет* - це всесвітня система взаємосполучених комп'ютерних і мобільних мереж.
SMS* - це невеликі за розміром текстові листи, які пересилають за допомогою сотового телефона.

загрожують віруси й інформація про декілька небезпечних вірусів

Віруси зазвичай записуються у систему і стають не помітними для ока. Чи всім мобільним пристроям вони загрожують? Відповідь – Так. Тому, що кожен коли встановлює будь-яку програму з не відомого сайту, може не помітити, як вірус через програму проникне у ваш пристрій. Тому варто встановити Анти-вірус* з довіреного офіціального сайту. Слідкуйте за тим, що ви встановлюєте.
Декілька небезпечних



Анти-вірус* - це програма, яка попереджує про встановлення віруса або намагається видалити його.

вони роблять з мобільним пристроєм

Shedun

«Вбивця гаджетів» найчастіше потрапляє на пристрої через програми, які викачуються в неофіційних магазинах-додатків. Вірус маскується під популярні додатки, наприклад, Facebook, WhatsApp і Twitter.

Shedun працює, як adware - показує користувачеві зараженого пристрою величезну кількість реклами, яке не можна закрити не переходячи на шкідливий сайт. Також встановлює інше шкідливе ПЗ без згоди з власником. Shedun не дарма прозвали «Вбивця гаджетів», оскільки навіть повернення до заводських налаштувань не врятує заражений пристрій. Панацеєю може стати тільки «перепрошивка» пристрою або покупка нового.

Mazar

Mazar - це різновид троянської програми. Він здатний читати повідомлення і відправляти інформацію своїм власникам, дзвонити на номери зі списку контактів та платні номери. Шкідливе ПО також збирає особисті дані зі смартфона, самостійно підключається до Інтернет. Особливістю Mazar, як і у Triada, є схильність до отримання повного управління пристроєм. Це в кращому випадку, несе загрозу змін налаштувань смартфона, а також видалення всіх даних, запис вірусу в прошивку телефону (що робить неможливим видалення вірусу навіть при скиданні телефону до заводських налаштувань).

Geinimi

Один з найвідоміших, хоча і дещо застарілих, вірусів для мобільних пристроїв - троянець Geinimi.

Шкідливе ПО завантажується з сайту, якщо користувач перейшов за посиланням, що в свою чергу прийшло в тексті sms. Як правило, користувач припускав, що завантажує якийсь додаток, проте насправді встановив собі вірус. Geinimi збирає інформацію про діяльність й дані

Як боротися з вірусами й який антивірус вибрати?

Як уберегтися від мобільних вірусів?

Для безпеки мобільних пристроїв необхідно дотримуватися трьох головних правил:

1. **Користуватися** тільки офіційним магазином додатків.
2. **Використовувати** антивіруси для мобільних пристроїв.
3. **Не переходити** за посиланнями які приходять в sms.

Що повинен уміти мобільний антивірус

Сучасний мобільний антивірус повинен мати кілька обов'язкових «**умінь**».

По-перше, сканувати як внутрішню пам'ять пристрою, так і дані на карті пам'яті, виявляти і блокувати «віруси», а також інші загрози.

По-друге, перевірка пристроїв повинна бути автоматичною, наприклад, використовуючи планувальники завдань в самій програмі. У той же час обов'язково повинна бути можливість у будь-який момент провести сканування вручну.

По-третє, в сучасному мобільному антивірусі просто зобов'язана бути присутнім специфічна функція перевірки додатків.

Четвертим важливим пунктом залишається актуальність вірусних баз. Програма повинна постійно оновлювати ці дані автоматично, хоча можливість ручного оновлення також бажана. Причому, важливо, що б це відбувалося не тільки по Wi-Fi, але й по поширеному сьогодні 3G каналу передачі даних.

інформації
та щодо пошуку (веб-сайтів)

Тож ми робимо висновки, що віруси дуже небезпечні для мобільних пристроїв й загрожують багатьом з них. Тому потрібно завжди мати при собі довірений антивірус.

Сайти щодо пошуку потрібної інформації:
http://zillya.ua – інформація про віруси та анти-віруси.
https://www.wikipedia.org – Інтернет-Енциклопедія.