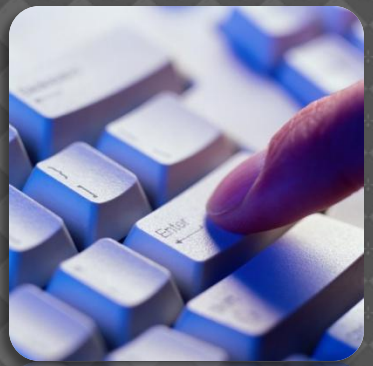
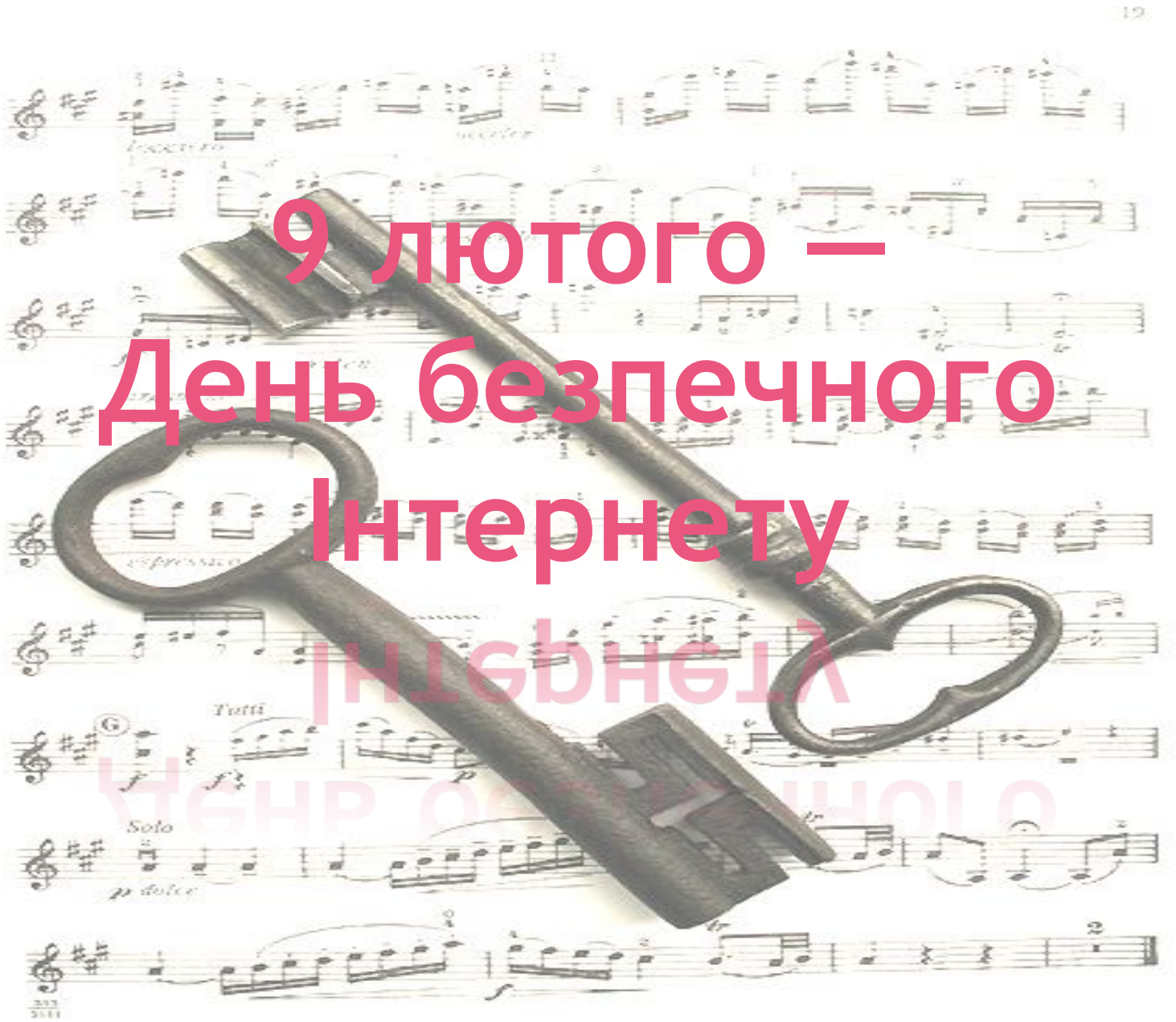
ПРОБЛЕМИ БЕЗПЕКИ В ІНТЕРНЕТІ



Роботу виконала: Федорів Анастасія
11-Б клас
2010 р.

ПЛАН

- Проблеми безпеки в Інтернеті
- Ваш пароль
- Як уберегтися від крадіжки пароля?
- Віруси і "троянські коні"
- Види антивірусних програм та їхня ефективність
  - KAV
  - Ad-Aware
  - AntiVir
  - Dr Web



9 лютого — День безпечного Інтернету

ПРОБЛЕМИ БЕЗПЕКИ В ІНТЕРНЕТІ

- Віртуальні подорожі по Інтернету, які ви здійснюєте, зручно влаштувавшись в м'якому кріслі, здавалося б, не можуть загрожувати якимись серйозними небезпеками. Але ваша спокійна самотність за монітором оманлива, оскільки весь час, поки встановлене Інтернет-з'єднання (і навіть в ті прочитані хвилини, за які ви перевіряєте електронну пошту), ваш комп'ютер є частиною величезної Мережі, в якій є і друзі, і вороги. Уберегтися від небезпеки завжди простіше, якщо знати, кого і чого боятися.

ВАШ ПАРОЛЬ

- Гроші і документи прибирають в сейф, щоб ніхто, крім їх власника, не міг ними скористатися. Ваш пароль - це ключ від вашого "сейфа" в Internet. Якщо хтось, крім Вас, буде знати ваше ім'я користувача і пароль, він зможе відкрити ваш "сейф".
- Інтернет зараз дуже популярний, але за його послуги треба платити, тому знайдеться немало комп'ютерних хуліганів, бажаючих погуляти по Інтернету за ваш рахунок. Пам'ятайте, що сейф відкривається не господареві, а тому, хто має ключ.
- Звернення до сервісів Internet з вашим ім'ям і вашим паролем система вважає вашим звертанням, хто б насправді його не здійснював. Відчуйте важливість свого пароля - пригадайте порівняння з ключем від сейфа.
- У багатьох людей поняття "пароль" ніяк всерйоз не пов'язано з їх повсякденною діяльністю. Мені нічого ховати на своєму домашньому комп'ютері - думають вони. А пароль - це просто зайва трудність, мені і без того треба тримати в голові безліч набагато кориснішої інформації. Якщо Ви думаєте так само, терміново змініть свою думку, поки ваша легковажність дорого Вам не обійшлася.

ЯК УБЕРЕГТИСЯ ВІД КРАДІЖКИ ПАРОЛЯ?

- Старайтеся запам'ятати свій пароль, а не записувати його. Якщо все ж доводиться записувати пароль, то ні в якому разі не залишайте записаний пароль в місці, доступному для чужих очей.
- Не записуйте пароль разом з своїм ім'ям користувача. Це приблизно те ж саме, що замкнути багаж в камеру зберігання, а секретний код написати на дверцях комірки. Порада не записувати пароль відноситься не тільки до паперу. Багато які програми пропонують "зберігати пароль" ("save password"), щоб не вводити його кожний раз, коли він необхідний. Вибирайте між зручністю і безпекою. Пароль, збережений в програмі, набагато небезпечніше записаного на папері, адже він вже "стоїть на своєму місці".
- Якщо Ви думаєте, що ніхто, крім вас, не має доступу до вашого комп'ютера, значить Ви забули про Інтернет-з'єднання, завдяки якому комп'ютери можуть обмінюватися інформацією. Гуляючи по Інтернету, Ви непомітно для себе можете обзавестися програмою - "троянским конем", яка буде в буквальному значенні тримати ваш комп'ютер "на долоні" у зломщика.
- Постарайтеся не зберігати свій пароль там, звідки він легко може бути витягнутий: Ні в якому разі не зберігайте ваш пароль в програмах, що встановлюють Інтернет-з'єднання!

ВІРУСИ І "ТРОЯНСЬКІ КОНІ"

- Якщо Ви маєте справу з комп'ютерами, то повинні знати про існування комп'ютерних вірусів. Останнім часом дуже широке поширення отримали специфічні шкідливі програми, що використовують Інтернет-з'єднання. Їх називають "троянськими кіньми", або "троянами".
- Досить точна назва, якщо пригадати історію Троянської війни: після довгої облоги Трої греки залишили біля воріт міста подарунок для мужніх троянців - величезного дерев'яного коня. Наївні троянці затягли коня в стіни міста, а вночі з коня вилізли солдати, що там ховалися... Троянці швидко зрозуміли свою помилку, а ось Ви, отримавши програму-трояна на свій комп'ютер, можете довго залишатися в невіданні з цього приводу. А в цей час шкідлива програма збирає відомості, що зберігаються на вашому комп'ютері, і посилає їх в "потрібне місце".
- Звичайно зловмисників цікавлять ваші збережені паролі. Самою гучною програмою-трояном є Back Orifice (по-українськи буквально: "задній прохід"). Отримати її у себе на комп'ютері - справжня біда. Це по суті справи міні-сервер, який дозволяє керувати вашим комп'ютером на відстані по Інтернет-з'єднанню: стягувати з нього будь-які файли, запускати на ньому програми, примусити ваш комп'ютер перестати відгукуватися на введення з клавіатури, перевантажити ваш комп'ютер і т.д. і т.п. Неприємно, правда? Бійтеся заражених дискет, неліцензійних компакт-дисків, програм, завантажених з випадкових Інтернет-сайтів, або присланих поштою невідомими особами, під яким би виглядом ці програми не були Вам запропоновані.
- Якщо Ви отримали невідомий лист з прикладеною програмою, не треба панікувати, сам по собі вірус не проникне на ваш комп'ютер. Просто видаліть такий лист і програму, не запускаючи її на виконання. Якщо цікавість сильніше за обережність, то обов'язково перевірте програму на наявність вірусів.

СПОСОБИ ЗАХИСТУ ВІД ВІРУСІВ

- Встановіть на комп'ютері, з якого здійснюється доступ до Інтернету, антивірусні програми Ad-Aware, AntiVir, EZAntivirus, Dr Web, KAV.
- Регулярно поновлюйте версії і антивірусні бази цих програм. Регулярно перевіряйте ваш комп'ютер за допомогою цих програм на наявність вірусів і троянів. Також обов'язково перевіряйте всі нові програми, які Ви маєте намір встановити або просто запустити на своєму комп'ютері, в тому числі і отримані по електронній пошті. Для виявлення і видалення двох найбільш поширених троянів Back Orifice і NetBus скористайтеся програмою BODetect.

ВИДИ АНТИВІРУСНИХ ПРОГРАМ ТА ЇХНЯ ЕФЕКТИВНІСТЬ

- KAV
- Ad-Aware
- AntiVir
- Dr Web

KAV

- Антивірус Касперського (англ. Kaspersky Antivirus, KAV) — антивірусне програмне забезпечення, яке розробляє Лабораторія Касперського. Надає користувачу захист від вірусів, троянських програм, шпигунських програм, руткітів, adware, а також невідомих загроз за допомогою проактивного захисту, який включає компонент HIPS. З самого початку, в 1990-х, називався -V, потім — AntiViral Toolkit Pro.
- На даний момент вважається одним із найкращих антивірусів.

ФУНКЦІЇ KAV

- Базовий захист
- Запобігання загрозам
- Відновлення системи і даних
- Захист конфіденціальних даних
- Зручність у користуванні

AD-AWARE

- Ad-Aware - програма, призначена для видалення шпигунського програмного забезпечення (spyware) з комп'ютера користувача. Також виявляє трояни, порнодіалери, malware, scumware, шкідливі доповнення до браузеру, а також компоненти, що відстежують переваги користувача без його згоди.
- Основні можливості:
  - Повне сканування комп'ютера, а також сканування вибраних дисків і папок
  - Сканування реєстру, файлів в архівах, обраного Internet Explorer і файлу Hosts
  - Виключення з сканування файлів більше заданого розміру
  - Сканування процесів в оперативній пам'яті комп'ютера
  - Автоматичне оновлення бази шкідливих програм через Інтернет
  - Підтримка скінів
  - Підтримка плагінів

КРИТИКА ПРОГРАМИ

- Програма легко вразлива до атак і можливості підміни баз, тому що:
  - Файли оновлення є zip-файлами, зашифрованими дуже простим алгоритмом, до того ж пароль розшифровки зберігається у відкритому вигляді в exe-файлі програми
  - Відсутні контрольні суми файлів оновлень
- Також:
  - Алгоритм сканування погано оптимізований, через що сканування займає багато системних ресурсів
  - Файли оновлення містять надмірну кількість даних, не потрібних для роботи програми

ANTIVIR PERSONAL

- Антивірус, безкоштовний для особистого використання. Продукт включає резидентний монітор (який перевіряє процеси при їх спробі звернутися до файлів), сканер і програму автоматичного/ручного оновлення (у якому відкривається вікно з рекламною пропозицією придбати комерційну версію premium). Починаючи з дев'ятої версії почала виявляти рекламні програми, програми-шпигуни і інші шкідливі програми (раніше було тільки в Premium версії).
- Має деякі недоліки у порівнянні з платною AntiVir Premium, що має ряд переваг.

DR. WEB

- Dr. Web — антивіруси цього сімейства призначені для захисту від поштових і мережевих черв'яків, руткітів, файлових вірусів, троянських програм, стелс-вірусів, поліморфних вірусів, безтілесних вірусів, макровірусів, вірусів, що приголомшують документи MS Office, скрипта-вірусів, шпигунського ПО (spyware), програм-викрадачів паролів, клавіатурних шпигунів, програм платного дозвону, рекламного ПО (adware), потенційно небезпечного ПО, хакреських утиліт, програм-люків, програм-жартів, шкідливих скриптів і інших шкідливих об'єктів, а також від спаму, ськамінг-, фармінг-, фішинг-повідомлень і технічного спаму.

ХАРАКТЕРНІ ОСОБЛИВОСТІ

- Можливість установки на заражену машину.
- Origins Tracing — алгоритм несигнатурного виявлення шкідливих об'єктів.
- Dr. Web Shield — механізм боротьби з руткітами.
- Підтримка більшості існуючих форматів упакованих файлів і архівів.
- Оновлення вірусних баз виробляються негайно у міру виявлення нових вірусів, до декількох разів на годину.
- Компактна вірусна база і невеликий розмір оновлень.
- Невеликий розмір дистрибутива.
- Кроссплатформенність — використовується єдина вірусна база і єдине ядро антивірусного сканера.
- Можливість повноцінної роботи сканера без інсталяції, що дозволяє використовувати антивірус для лікування заражених систем з використанням носіїв в режимі лише для читання.
- Виявлення і лікування складних поліморфних, шифрованих вірусів і руткітів.

БЕЗПЕЧНОГО ІНТЕРНЕТУ!