Безпека в Інтернеті

Хто прагне проникнути до мого комп’ютера? Хто за мною спостерігає? Як уберегтися від непроханих візитерів? Як захиститися від тих, хто хоче використати мою персональну інформацію? Як саме й навіщо люди здобувають інформацію про мене? Як уберегти персональну інформацію від викрадення? Як захиститися від людей, які прагнуть завдати мені шкоди? Хто і як може завдати мені шкоди?

Інтернет охоплює майже весь світ, а отже ця мережа доступна і для тих людей, які мають далеко не найкращі наміри. Проблема збільшується ще й тому, що після підключення комп'ютера до мережі, а особливо до Інтернету, виникає ризик вторгнення зловмисника до цього комп’ютера та подальшого використання його для атак на інші комп’ютерні системи.

Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність хакерів, а також віруси та спам. Хакер - тепер так називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані. Хто прагне проникнути до мого комп'ютера?

Троянські коні. Це шкідливі програми, які розповсюджуються шляхом обману. Так, вам може надійти електронною поштою лист, де буде сказано, що програма, яка знаходиться у вкладенні, виконує якусь корисну функцію. Якщо ви запустите її на виконання, ваш комп'ютер буде заражений. Троянські коні відкривають хакерам доступ до системи, можуть спричинити руйнування інших та виконання інших програм. Перевантаження сайту або мережі. Генеруючи багато запитів довільного змісту до сайту або мережі, хакер збільшує їхнє робоче навантаження внаслідок чого цей сайт або мережа не можуть нормально функціонувати.

Способи проникнення Хакерів до чужих систем.

Підміна адрес. Хакер підмінює адреси сайтів у такий спосіб, що коли користувач зводить у браузері адресу якогось сайту, його спрямовують до зовсім іншого сайту. Іноді на такому альтернативному сайті міститься негативна інформація про власника того сайту, який збирався відвідати користувач. Аналіз пакетів. За допомогою спеціальної програми хакер читає певну інформацію що міститься у пакетах, які передаються мережею. Загалом програми - аналізатори пакетів призначені для контролю за мережею, проте вони ж використовуються хакерами для несанкціонованого збирання інформації.

Соціотехніка. Цей термін використовується для позначення шахрайських дій, спрямованих на отримання інформації. Соціотехніка зазвичай є грою хакера на довірі людини. Для цього використовуються сфальсифіковані сайти та фіктивні електронні повідомлення від імені реальних компаній з проханням надати особисту інформацію. Підміна веб-сторінки. Хакер дістається сайту та змінює на ньому певну веб-сторінку, після чого на ній відображається інша інформація.

Віруси. Програми названі на ім'я біологічних організмів, бо вони досить малі, розповсюджуються, роблячи копії з самих себе, та не можуть існувати без носія. Хробаки. Хробак схожий на вірус тим, що розмножується, роблячи власні копії, але на відміну від

останнього він не потребує носія й існує сам по собі. Часто хробаки передаються через електрону пошту. Хоча спершу хробаки не були шкідливими, нинішні їхні різновиди спричиняють значні перенавантаження мереж і можуть руйнувати файли. Існують програми, що мандрують Інтернетом та, потрапивши на комп'ютер чи до локальної мережі, завдають тієї чи іншої шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки. Першим відомим “хробаком" прийнято вважати програму Роберта Морріса , студента Корнелського університету. За 90 хвилин, використовуючи помилку переповнювання буфера, Morris Worm заразив 6000 комп'ютерів Глобальної Мережі.

Спамом називають небажану електронну пошту, тобто пошту, що надходить без вашої згоди. Боротися зі спамом дуже складно навіть корпорації, спроможні щорічно витрачати мільйони доларів на антивірусне програмне забезпечення, не здатні зупинити потік рекламних та інших небажаних повідомлень, які призводять до перенавантаження мережних каналів та зайвих витрат дискового простору. Перелік типових дій, які можуть призвести до того, що ваша адреса стане надбанням спамерів: підписка на безкоштовне отримання електронною поштою прайс-листів, новин та іншої подібної інформації; відповідь на спам, що надійшов на вашу адресу (цим ви підтверджуєте, що адреса дійсно комусь належить); надання згоди на участь у групі новин; заповнення онлайнових форм; участь у чаті.

Крім програм, за допомогою яких певні люди намагаються проникнути до вашої системи, існують також засоби, що застосовуються для спостереження за вами. Це насамперед програмне забезпечення, яке зазвичай називають adware та spyware, шпигунські програми, програми для батьківського контролю, блокуючи програми тощо. Ці програми можуть відстежувати ваші звички стосовно мандрування Інтернетом, надсилати комусь дані без вашого дозволу, змінювати адресу домашньої сторінки вашого браузера і навіть змінювати системні файли комп’ютера.

Хто за мною спостерігає?

Adware - так називають програми, які під час своєї роботи виводять на екран рекламні стрічки — банери. Подібні програми сповільнюють роботу вашої системи. Програми типу spyware без вашого дозволу надсилають комусь інформацію про те, що ви робите в Інтернеті. Зазвичай це здійснюється в рекламних цілях. Програмне забезпечення типу spyware також сповільнює роботу системи і навіть призводить до її збоїв. Існує декілька програм, що застосовуються з метою блокування програмного забезпечення типу adware і spyware. Це, зокрема, такі: Spybot Search & Destroy, Lavasoft Adware, Spyware Doctor 2.0 та інші.

Cookie-файли - зовсім не шпигунський засіб, і коли вони застосовуються за призначенням, то значно полегшують ваше перебування в Інтернеті. Це маленькі текстові файли, що містять дані, а не програми і тим більше не віруси. Коли ви налаштуєте для себе домашню сторінку сайту, то вона під час відкриття набуватиме бажаного вигляду автоматично. Це стає можливим завдяки тому, що відповідні настройки зберігаються в cookie-файлі на вашому комп'ютері, і програмне забезпечення сайту читає їх під час завантаження сторінки. Сайти, призначені для купівлі товарів через Інтернет, можуть зберігати кошик

для покупок у вигляді cookie. Прочитати cookie-файл може лише програмне забезпечення сайту, який його створив.

Існує безліч причин, з яких певні особи застосовують шпигунські програми, що стежать за вашими діями, аналізують вашу електронну пошту та фіксують адреси відвідуваних вами веб-сторінок. Найбільшими користувачами цих засобів є ФБР (у США), корпорації, які стежать за своїми робітниками, та навчальні заклади, що спостерігають за учнями чи студентами. Також існує багато засобів, які утруднюють несанкціоноване отримання персональної інформації. Серед них — програми батьківського контролю, що є дуже популярними. Ними користуються не лише батьки, щоб вберегти своїх дітей від відвідування сайтів з небажаним вмістом, а й керівники корпорацій та навчальних закладів, з аналогічною метою. Мандруючи мережею Веб, учні у такому разі стикаються з блокуванням у випадках, коли сторінка, яку вони намагаються відкрити, містить слова, розцінені блокуючою програмою як образливі чи неприйнятні для дитячої або підліткової аудиторії.

Отже, ви мали змогу впевнитись, що є багато людей, які намагаються отримати доступ до чужих комп'ютерів. Проте існують засоби, що утруднюють цей процес або навіть унеможливлюють його. Найпоширеніші з них — брандмауери, а також антивірусне та антиспамове програмне забезпечення. Велике значення має також дотримання користувачами правил безпеки під час роботи в Інтернеті.

Як уберегтися від непроханих візитерів?

Взагалі брандмауер — це стіна з вогнестійкого матеріалу, що розташована між буквами й захищає їх від пожежі. В комп'ютерній мережі брандмауером називати програмне та апаратне забезпечення, яке захищає локальну мережу від небезпек. Брандмауер розташовують між локальною мережею та Інтернетом або між окремими ланками локальної мережі. Він відстежує й аналізує весь потік пакетів з даними що надходить до нього, і пропускає лише дозволені пакети. Таким чином, небезпечний код з Інтернету не може потрапити до локальної мережі. Корпоративні брандмауери, що застосовуються в мережах підприємств та установ складаються з апаратного та програмного забезпечення. Для захисту домашніх комп'ютерів використовують так звані персональні брандмауери, які зазвичай реалізовані у вигляді програм.

Однією з найбільших загроз для комп'ютерних систем є віруси. Для боротьби з ними можна придбати програмне забезпечення, що називається антивірусним. Воно працюватиме у вашій системі й перевірятиме на вміст вірусів усі файли, які ви отримуєте електронною поштою, завантажуєте з Інтернету, переписуєте на жорсткий диск або запускаєте на виконання з компакт-дисках чи дискети. Це Антивірус Касперського, Symantec Antivirus, McAfee VirusScan, AVG Anti-Virus. Незалежно від того, яку з антивірусних програм ви оберете, важливо постійно її оновлювати. Зазвичай за певну річну оплату ви можете завантажувати оновлення з сайту виробника. Більшість програм самостійно щоденно підключаються до свого сайту й перевіряють, чи нема там «свіжих» оновлень.

Робота Антивіруса Касперського Антивірусне програмне забезпечення.

Після того як корпорацією Microsoft для операційної систем Windows XP був розроблений пакет оновлень Service Pack 2 (SP2), процес підтримки цієї операційної системи значно спростився. Основними нововведеннями цього пакету є Центр забезпечення безпеки, за допомогою якого користувач може встановити бажаний рівень захисту комп'ютера, а також вбудований засіб блокування спливаючих вікон у браузері Microsoft Internet Explorer. Центр забезпечення безпеки складається з трьох компонентів: брандмауера, засобу автоматичного оновлення системи та засобу антивірусного захисту. Для доступу до Центру забезпечення безпеки потрібно з меню “Пуск” визвати команду “Панель керування” та вибрати посилання “Центр забезпечення безпеки”.

Центр забезпечення безпеки Windows

Завдяки Центру забезпечення безпеки Windows процедури завантаження та встановлення оновлень значно спростилися. Користувачеві треба лише переконатись, що компонент Автоматичне оновлення Windows ввімкнено і за потреби змінити час, коли він виконуватиме перевірку наявності оновлень на сайті Microsoft, їх завантаження та встановлення на комп'ютер. Потрібно лише, щоб комп’ютер у цей час був увімкнений та підключений до Інтернету. Автоматичне оновлення Windows — це засіб, що демонструє турботу корпорації Microsoft про безпеку користувачів.

Крім хакерів, які намагаються завдати шкоди вашому комп’ютеру, існують зловмисники, що прагнуть отримати вашу персональну і конфіденційну інформацію та, використовуючи її, завдати вам шкоди. Як саме й навіщо люди здобувають інформацію про мене? Певна категорія людей здійснює атаки на чужі комп'ютери задля отримання персональної інформації. Зазвичай їхніми об’єктами стають бази даних великих корпорацій, де зберігаються такі відомості, як персональні ідентифікаційні номери, номери банківських рахунків та кредитних карток клієнтів. Проте відомо багато випадків, коли жертвами зловмисників стають приватні особи, особливо якщо вони передають конфіденційну інформацію через Інтернет без належного захисту. Часом зловмисники намагаються викрасти персональну інформацію для того, щоб від імені іншої людини відкривати рахунки, купувати товари тощо. Найчастіше викрадають дані про банківські картки. Анонімність і величезні розміри Інтернету роблять його «землею обітованою» для шахраїв усіх ґатунків.

Правила безпеки, яких слід дотримуватися під час передавання інформації Інтернетом Ніколи не надсилайте персональну інформацію незнайомим людям. Дітей молодшого віку потрібно вчити, щоб вони ніколи не повідомляли в Інтернеті свої справжні імена, адреси та будь-яку іншу інформацію. Не надавайте більше інформації, ніж потрібно. В кожному випадку треба бути впевненим, що одержувач інформації надійний. Не завадить також переконатися, що сайт захищений і на ньому використовуються технології шифрування. Захищені сайти зазвичай вимагають введення імені користувача та пароля. Робіть його довжиною щонайменше вісім символів, комбінуючи букви та числа. І головне, паролем не повинно бути щось очевидне, якісь слова чи дати. Захищена веб-сторінка Зверніть увагу на значок замка у правій частині рядка стану браузера та на URL-сторінки, де як протокол зазначений HTTPS. Значок замка показує, що сайт зашифрований з використанням протоколу SSL . Він підтримується всіма браузерами та застосовується для безпечного передавання інформації.

Коли зловмисник, вкравши ідентифікаційні дані, знімає гроші з чужого рахунку, це дуже неприємно, але значно гірше, коли він отримає персональну інформацію і це стане загрозою безпеці чи життю людини. Хто і як може завдати мені шкоди? Існують особи, які через Інтернет знайомляться з молодими людьми, здобувають їхню довіру, випитують особисті дані й призначають зустріч. Тож пам'ятайте, що ваш приятель із чату, який, скажімо, відрекомендувався 15-річним підлітком, що шукає друзів, насправді може виявитися дуже небезпечною людиною. Саме чати та системи обміну миттєвими повідомленнями ці особи обирають для налагоджування контактів з молодими людьми, оскільки почуваються там безпечно.

Як захиститися від людей, які прагнуть завдати мені шкоди?

В Інтернеті дійсно можна зустріти багато суб'єктів з недобрими намірами, але це не є приводом для того, щоб відмовитися від користування цією мережею. Дотримуйтесь кількох простих правил, і ви будете гарантовані, що жодна людина з нечесними намірами не отримає доступу до вашої персональної інформації. Завжди звертайтеся до батьків чи учителів з будь-яких питань, пов'язаних із користуванням Інтернетом. Візьміть за звичку не надавати свою персональну інформацію в кімнатах чату та системах обміну миттєвими повідомленнями. Ніколи не погоджуйтеся на зустріч із людиною, з якою ви познайомилися через Інтернет. Не надсилайте своє фото інтернет-знайомим. Ніколи не давайте незнайомим людям таку інформацію, як повне ім'я, адреса, номер школи, розклад занять або відомості про родину.

Як убезпечити себе в Інтернеті?

З початком широкого використання міжнародних мереж передачі даних загального користування темпи росту мережної злочинності зростають в геометричної прогресії. За оцінками експертів Міжнародного центру безпеки Інтернет (CERT) кількість інцидентів пов’язаних з порушенням мережної безпеки зросла в порівнянні з 2000 роком майже у 10 разів. Основними причинами, що провокують ріст мережної злочинності є недосконалі методи і засоби мережного захисту, а також різні уразливості у програмному забезпеченню елементів, що складають мережну інфраструктуру. Основними джерелами небезпек для користувачів Інтернету являється діяльність хакерів, вірусів та спамів. Існують засоби, що утруднюють доступ до чужих комп'ютерів – це брандмауери, антивірусне та антиспамове програмне забезпечення. Велике значення також має дотримання користувачами правил безпеки під час роботи в Інтернеті. Для отримання персональної інформації, небезпечні особи використовують чати, системи обліку миттєвими повідомленнями та сайти знайомств. Дотримання простих правил в спілкуванні через мережу Інтернет, дозволить захистити користувача від недобрих намірів зловмисників.