Безпека в Інтернеті

Сучасне життя неможливе без Інтернету. Ми використовуємо доступ до мережі для пошуку, публікації та обробки інформації. Переваги використання інтернету очевидні. Як будь-яка складна інфраструктура, інтернет містить багато небезпек, нехтування якими може призвести не просто до втрати спокою, але й істотних грошових коштів. Кожен, хто працює з мережею, щоб не випробовувати на собі її «темні» сторони, повинен знати потенційні джерела небезпеки та вміти захищати себе й своїх менш «просунутих» близьких і друзів.

Джерела небезпеки

- **Комп'ютерні віруси і троянські програми**

Трояни і віруси можуть бути приховані в безкоштовних, доступних для скачування з інтернету програмах або на піратських дисках.

Як це працює: ви запускаєте програму, і вона, використовуючи відому зловмисникові вразливість вашої операційної системи або іншої програми, захоплює контроль над комп'ютером. З цього моменту вірус чи троян безперешкодно володіє комп'ютером, доставляючи масу неприємностей виконуючи неочікувані для вас дії. Трояни при цьому щедро діляться вашою персональною та фінансовою інформацією зі своїм господарем, відправляючи її по інтернету.

- **Мережеві атаки**

Мережева атака на ваш комп'ютер - це спроба знайти вразливі місця в його операційній системі й програмах, які можуть бути використані зловмисником для різних цілей, наприклад:

- виведення вашого комп’ютера з ладу;
- відключення його від інтернету (у випадку, якщо комп’ютер є сервером, що надає якийсь корисний інтернет-сервіс клієнтам, це може спричинити за собою репутаційні й фінансові втрати, якщо він не зможе надавати ці послуги)
- запуск на вашому комп'ютері шкідливої програми;
- крадіжка ваших даних;
- блокування ваших даних з метою здирництва;
- додавання вашого комп'ютера під шкідливий бот-нет.

І це далеко не повний перелік цілей зловмисників.

Як це працює: з комп'ютера зловмисника, чи зараженого спеціальним вірусом комп'ютера ще однієї жертви через інтернет або іншу мережу, проводиться спроба підключення до комп'ютера жертви за допомогою знайденої вразливості. Метою мережевої атаки може бути й сам пошук такої вразливості.

- **СОЦІАЛЬНА ІНЖЕНЕРІЯ**

Методу заснованому на психологічних прийомах, який існує та ефективно використовується з самого початку розвитку комп'ютерних мереж, не загрожує зникнення. Він не пов'язаний безпосередньо з комп'ютерами: перші соціальні інженери взагалі займалися зломом телефонних мереж.

Як це працює: зловмисник намагається видати себе за того, кому ви довіряєте (банк, ваш друг, мама, брат або сестра, шкільний учитель), і виконати необхідні дії, які ви ніколи б не виконали на прохання чужої людини (перерахували гроші на картку, відкрили дивне вкладення в листі, тощо).

Список прийомів, придуманих хакерами в розрахунку на довіру користувачів, величезний. Вам можуть зателефонувати або надіслати листа від імені адміністрації сервісу з проханням вислати їм нібито загублений пароль або лист, що містить нешкідливий, на перший погляд файл. А насправді, в ньому прихований троян, на що й розраховують зловмисники: вашу цікавість і відкриття, а отже й запуск програми.

- **ФІШИНГОВІ САЙТИ ТА РОЗСИЛКИ**

Шахрайські сайти та листи електронної пошти, своїм дизайном і змістом мімікрують під відомі організації, що користуються авторитетом і довірою.

Як це працює: нічого не підозрюючи клієнт банку вводить пін-код кредитної картки на сторінці банку, посилання на яку надіслано поштою нібито самим банком. Ця сторінка виглядає точнісінько так, як і раніше, коли ви неодноразово відвідували її. Але якщо уважно придивитись до адреси посилання, то можна помітити зайву літеру в назві банку.

- **«СОЦІАЛЬНИЙ ЕКСГІБІЦІОНІЗМ»**

Ви любите у статусі профілю Facebook повідомляти друзям про свої плани та місце перебування? Круто поділитися такою радістю: «завтра на цілий місяць відлітаємо всією сім'єю на Гоа! Вау!..» Що ж, комусь же потрібно буде стежити за вашою квартирою поки ви відсутні. Наприклад, квартирним злодіям, які разом із друзями, із захопленням стежать за вашими пригодами та новими повідомленнями у Facebook. Водночас, вони і «поприбирають» в квартирі, й «мотлох» повиносять всякий..

Причини проблеми

За статистикою більшість авіакатастроф відбуваються внаслідок так званого «людського фактора», а не збою техніки. «Людський фактор» - це, іншими словами, помилки пілотів та авіадиспетчерів. У комп’ютерному світі все так само: як правило причини проблем, які виникають не в технологічних аспектах Інтернету, а в психології самих користувачів.

Недооцінка небезпеки

Кому може знадобитися наш жалюгідний персональний комп'ютер, на якому ми дивимося фільми і «лазимо» в інтернеті? Кому ми взагалі цікаві зі своїм абсолютно звичайним профілем соцмережі? Та таких як ми – мільйони!

Але ви просто не про все знаєте. Ви не можете передбачити абсолютно всі шляхи потенційного використання зловмисниками інформації про вас в своїх корисних цілях! Не уявляєте, де може бути використана ваша інформація та наслідки такого використання для вас.

Ваш комп'ютер сам по собі дійсно не потрібен нікому. Але як одна з тисяч осередків шкідливої бот-мережі він слугуватиме зловмиснику. Тому інтернет-шахрай з радістю його туди додасть.

Безпечність

Виконання сумнівних інструкцій або прохань з неперевірених листів від знайомих, натискання підтверджувальних кнопок у вікнах, які випливають та повідомлення, які нам не дуже зрозумілі (швидше б вони закрилися і не заважали дивитися на картинки кошенят!) – це найкоротший шлях до проблем в інтернеті. Ми пильні й обережні, потрапивши увечері до незнайомого району. Так що ж заважає нас повністю втрачати пильність у невідомих закутках інтернету?

Прості паролі та їх повторне використання

Часто користувачі, яким набридло весь час вводити довгі та складні паролі до банк-клієнту або в соцмережах, змінюють їх на свою дату народження, телефон чи щось типу «password123». Деякі йдуть ще далі, встановлюючи однаковий пароль на всі свої інтернет-акаунти. Але встановлення простого пароля настільки нерозумно, як і купівля замку для вхідних дверей квартири, до якого існує всього десять варіантів ключів. Квартирному злодієві, для якого це як хобі, не складно буде роздобути всі десять і, за хвилину перепробувати їх на Вашому замку. Так само сучасні комп'ютери здатні вгадати Ваш пароль, перебравши мільйони різних комбінацій та символів за лічені секунди. Що ж стосується використання єдиного пароля для всіх своїх інтернет-акаунтів, то потрібно пам'ятати одну просту річ: брелок – це чудова штука, яка дозволяє загубити всі ключі одночасно.

НЕХТУВАННЯ ЗДОРОВИМ ГЛУЗДОМ

Вам прийшов лист від незнайомого африканського принца, який у безвихідній і терміновій ситуації просить допомогти вивести з країни кошти його королівської родини у зв'язку з початком народних хвилювань? Вас чекає скромна винагорода у розмірі однієї двадцятої всіх виведених з його бідної африканської країни багатств, які протягом багатьох років крав його деспотичний татусь-диктатор. Вам потрібно тільки допомогти з перекладом і сплатити деякі мита в розмірі всього кілька сотень євро. Якщо для вас цей сценарій здається цілком реальним, то це і називається зневагою здоровим глуздом з вашого боку.

ВІДСУТНІСТЬ АНТИВІРУСНОЇ ПРОГРАМИ І БРАНДМАУЕРА

Якщо для вас у сучасному світі наявність антивірусу та брандмауера при роботі з комп'ютером не є чимось обов'язковим, то ви – потенційний клієнт різного роду зловмисників і вірусів. Це все одно, що відключити домофон під'їзду, позбутися вхідних дверей у свою квартиру, а вашу вівчарку, яка одночасно була другом та сторожем вашої оселі відправити на дачу.

Що робити та як бути?

Власне, що робити, щоб не стати жертвою комп'ютерних вірусів і різного роду інтернет-шахраїв, можна зрозуміти з прочитаних попередніх абзаців. Але ще раз підсумуємо:

1. Завжди будьте уважні в інтернеті. Не довіряйте листам і сайтам, невідомого автора. Якщо у вас є хоч якісь сумніви в їх достовірності – краще відмовитись від операції. Пам'ятайте, що адресу відправника електронного листа дуже легко підробити. Краще зателефонувати знайомому (від імені якого надіслано лист), переконавшись особисто у потребі допомоги.
2. Не відкривайте ніякі підозрілі посилання. Пам'ятайте, що реальні посилання та те, що ви бачите на екрані, можуть різнитися. Ідентичність посилання та її відображення на веб-сторінці дуже легко перевірити.
3. Завжди перевіряйте правильність адреси веб-сайтів, на яких ви виконуєте якісь фінансові операції або вводите конфіденційну інформацію. Часто шахрайські (фішингові) сайти мають адреси дуже схожі на адреси реальних веб-сайтів, але відрізняються, наприклад, однією літерою.
4. Банки та сервіси електронної пошти не будуть починатись з http – тільки https! (протокол шифрування переданих і отриманих даних).
5. Завжди встановлюйте антивірусну програму і фаєрвол, своєчасно оновлюючи антивірусні бази.
6. Десять разів подумайте, перш ніж опублікувати в соцмережах будь-яку інформацію про себе та свої плани. Завдяки роботі сучасних пошукових систем типу Google ви більше ніколи не зможете її звідти вилучити.

7. Не лінуйтеся заводити складні паролі (щонайменше 8 символів, де є як маленькі, так і великі літери) і не призначайте один і той же пароль для всіх Ваших облікових записів.

8. Своєчасно оновлюйте Операційну Систему і софт.