**Безпека користування Internet простором**

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 близьких і друзів.

Отже, джерела небезпеки наступні:

♦   комп'ютерні віруcи та троянські програми

**Комп'ютерний вірус** (англ. computer virus) — комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Комп'ютерні віруси бувають:

***Файлові вiруси***—проникають у файли, що виконуються (exe, com, bat), у системнi файли, файли драйверiв (sys, drv, vxd), файли бiблiотек (DLL), а також у ряд iнших типiв файлiв. Пiсля вкорiнення файловi вiруси починають розмножуватися пiд час кожного запуску файла.

***Завантажувальнi вiруси*** — заражають завантажувальний сектор диска (Boot сектор) або сектор, що мiстить програму системного завантажувача вiнчестера (Master Boot Record). Такий вiрус замiщає собою програму в завантажувальному секторi, внаслiдок цього потрапляє до оперативної пам’ятi й перехоплює керування вiдразу пiд час завантаження операцiйної системи.

***Файлово‑завантажувальнi вiруси*** можуть проникати як уфайли, такi в завантажувальнi сектори. До таких вiрусiв належать, зокрема, стелс-вiруси i найнебезпечнiшi екземпляри полiморфних вiрусiв.

***Макровiруси*** проникають у файли документiв (пакет Microsoft Office) й iншi файли, пiдготовленi в додатках, що мають свою мову макрокоманд. Формально цi вiруси є файловими, але заражають вони не файли, що виконуються, а файли даних. Небезпека макровiрусiв не стiльки в їхнiй руйнiвнiй дії, скiльки в поширеності документiв, пiдготовлених у популярних системах Word i Excel.

***Мережнi вiруси*** поширюються по комп’ютернiй мережi. Особливiсть цих вiрусiв полягає в тому, що вони заражають тiльки оперативну пам’ять комп’ютерiв i не записуються на носiї iнформацiї.

**Trojan, або троянська програма -**спрямовує свої дїї на видалення, блокування, зміну або копіювання даних користувача, розташованих на комп’ютері. Інколи їх завдання полягає в уповільненні роботи ПК або комп’ютерної мережі. Троянські програми здатні виступати як самостійне шкідливе ПЗ, а також нести в собі інші шкідливі програми. Так, наприклад:

-бекдори дають зловмисникам змогу віддаленого керування машиною і досить часто використовуються для об’єднання заражених комп’ютерів у ботнети;

- шпигунські програми мають змогу приховано спостерігати за даними, що вводяться з клавіатури, до цього різновиду можна зарахувати банківських і ігрових троянців;

- троянці, котрі використовують комп’ютер жертви у DDoS-атаках без відома власника;

- Trojan-FakeAV імітують роботу антивірусного забезпечення і вимагають у користувача кошти на вирішення примарних загроз;

- руткіти приховують в системі шкідливі об’єкти або їх дії.

♦   мережеві атаки

Основною особливістю будь-якої мережевої системи є те, що її компоненти розподілені в просторі, а зв'язок між ними здійснюється фізично, за допомогою мережевих з'єднань (коаксіальний кабель, вита пара, оптоволокно і т. п.), і програмно, за допомогою механізму повідомлень. При цьому всі управляючі повідомлення і дані, що пересилаються між об'єктами розподіленої обчислювальної системи, передаються по мережевих з'єднаннях у вигляді пакетів обміну. До мережевих систем, разом із звичними (локальними) атаками, здійснюваними в межах однієї комп'ютерної системи, застосовується специфічний вид атак, обумовлений розподілом ресурсів і інформації в просторі, - так звані мережеві (або віддалені) атаки (remote або network attacks). Вони характеризуються, по-перше, тим, що зловмисник може знаходитися за тисячі кілометрів від об'єкту, що атакується, і, по-друге, тим, що нападу може піддаватися не конкретний комп'ютер, а інформація, що передається по мережевих з'єднаннях. З розвитком локальних і глобальних мереж саме мережеві атаки стають лідируючими як по кількості спроб, так і по успішності їх застосування, і, відповідно, забезпечення безпеки обчислювальної системи з погляду протистояння мережевим атакам набуває першорядне значення. Під мережевою атакою зазвичай розуміється інформаційна руйнуюча дія на розподілену обчислювальну систему, програмно здійснювана по каналах зв'язку.

♦   соціальна інженерія

Соціальна інженерія - одна з технологій управління людьми. Тобто якщо інженер займається розробкою певних технічних рішень, наприклад, пристроїв, то людина, яка займається соціальною інженерією, створює технології, які повинні впливати на поведінку і психологію людей.Наприклад, створення повідомлення, яке спонукатиме користувача на певну дію, необхідне шахраям. Людина є одним з найважливіших елементів інформаційної мережі, і, за іронією долі, найбільш уразливим елементом. Щоб убезпечити себе - можна поставити суперскладні паролі або сучасні захисні програми: фаєрволи, антивіруси, системи обмеження та розподілу прав доступу. Тільки от людина, що працює за комп'ютером, завжди може відключити всі системи безпеки або обійти їх іншим способом, і дати можливість зловмиснику потрапити на свій комп'ютер.

**Електронні листи з використанням соціальної інженерії**
Вміст листа спонукатиме користувача запустити прикріплений до листа файл, і таким чином активується троянська програма. Наприклад, ви отримали лист з випискою від банку, в якому вас просять уточнити деталі, повідомляють про проблеми з рахунком. До листа прикріплюється файл, який має іконку Word або PDF-документа, однак, насправді документом він не є. Це програма, яка запускається і заражає ПК користувача. Багато поштових сервісів намагаються захистити користувачів від таких хитрощів, наприклад, вони блокують листи з прикріпленими виконуваними файлами. Зловмисники, у свою чергу, намагаються прікріпити до листів архіви, в які запаковують троянські програми. І, таким чином, можливо спостерігати як користувач сам розпаковує архів і запускає шкідливу програму, обійшовши при цьому систему захист поштових сервісів.

**Фішинг**

Дуже поширений вид шахрайства. Мова йде про створення сайтів, які зовні дуже схожі на справжні. Фішинг базується на некоректно введених адресах в браузері, підміні пошукових запитів і мімікрії сторінки. Наприклад, коли користувач хоче набрати «вконтакте ру» а набирає «вкотнакте ру». Як показує статистика, такі помилки при введенні адреси користувачі роблять досить часто. При цьому відкривається сторінка, абсолютно схожа на сторінку авторизації популярної соц-мережі. Користувач пробує авторизуватися, вводить свій логін і пароль, але, оскільки сайт - підробка, він не авторизується, і лише повідомляє свій пароль зловмисникам.

**Сайт + фішингові листи**

Користувачам розсилається лист або повідомлення в соціальній мережі з вмістом і лінком, на який пропонується перейти, щоб побачити деталі. Але насправді це посилання веде на підроблений сайт, який буде називатися дуже схоже, а користувач може і не помітить різниці. Цікаво те, що сайт знову попросить вас зайти в свій аккаунт. При цьому ви вводите свій логін і пароль, а зловмисники - отримують їх.

**Виклик емоційної реакції**

Дуже часто зловмисники розраховують на виклик потужної емоційної реакції. Вони складають такі заголовки для листів або тексти, що вкладений файл негайно хочеться відкрити. Наприклад, отримавши від користувача в Фейсбуці повідомлення з текстом «Вау, відмінно вийшов на відео!» І посиланням на скачування, ви скачаєте і з цікавості відкриєте його. Заразивши таким чином свій комп'ютер. Для того, щоб уникнути цієї помилки, необхідно подумати: у чому сенс повідомлення і що це може бути за відео, чому текст настільки загальний, чому немає конкретики. Головне - не поспішайте переходити за підозрілими посиланнями і відкривати підозрілі файли.

**SMS-шахрайство**

На телефон приходить повідомлення з загальним змістом, що ваша банківська карта заблокована. Після того, людина дзвонить по вказаному телефону і в процесі діалогу видає свій пароль. Іншим способом шахрайства є розсилка повідомлень про перемогу в тому чи іншому конкурсі та проханням про оплату невеликого податку або внеску. Також може бути виникнути інформація про помилкове перерахування певної суми на рахунок і проханням терміново відправити її назад. Для того, щоб уберегтися від подібного шахрайства, потрібно завжди пам'ятати, що смски від банку можуть приходити виключно з офіційного телефону банку.

Таким чином, існує достатня кількість способів шахрайства за допомогою сучасних технологій. Крім стандартних програмних засобів захисту, необхідно пам'ятати і про наступні.

**Вибирайте надійні паролі**

Створіть надійний пароль, який складається з комбінації великих і маленьких букв, спеціальних символів і цифр. Не використовуйте один і той же пароль для важливих сайтів - наприклад, не варто ставити пароль від основної пошти на електронний гаманець. Використовуйте 2-кроковий спосіб верифікації Багато сервісів дозволяє прив'язати свій аккаунт не тільки до логіну та паролю, а й до номеру телефону. У такому випадку, якщо хтось (ви в тому числі) буде заходити в вашу пошту з нового пристрою або місця, програма зажадає крім стандартних логіна і пароля - підтвердження з смски, надісланій на ваш номер телефону. Подібна міра серйозно підвищує ступінь захисту вашої персональної інформації.

**Оновлюйте свою систему і захисні програми**

Здійсніть оновлення системи яких захисних програм типу антивіруса, або фаєрвола відразу ж, як тільки будуть доступні нові оновлення. Це дозволить захиститися від самих недавніх виниклих загроз. Уважно ставтеся до підозрілих листів і пропозицій Якщо ви побачили підозрілий лист з невідомої адреси, краще видалити його навіть не відкриваючи. При виявленні якихось пропозицій, не поспішайте виконувати дії: зупиніться і подумайте про подробиці цієї пропозиції. Також, ніколи не вводьте свій пароль на невідомих сайтах.

**Регулярно перевіряйте за допомогою антивіруса**

Встановіть ліцензійну версію програми-антивіруса і перевіряйте комп'ютер регулярно. Оновлюйте свій антивірус, як тільки виникнуть нові оновлення. Будьте пильні й недовірливі Щоб уникнути проблем з банківською картою або банкоматом, а також шахрайство за допомогою телефону або смс-повідомлень, завжди намагайтеся з'ясувати якомога більше інформації про вхідні повідомлення і пропозиції, перш ніж погодитися на що-небудь або назвати свої персональні дані. Краще бути надмірно обережним, ніж втратити свої гроші. Таким чином, основні типи загроз сучасному користувачеві не так вже й відрізняються один від одного, можуть виглядати досить невинно, і головне - використовують не стільки програмні методи кібератак, скільки вашу довірливість, за допомогою методів соціальної інженерії. Пам'ятайте про те, що ваші гроші можуть знадобитися не тільки вам, і не втрачайте пильності!

Джерело:
© Сайт Департаменту Кіберполіції України - <https://www.cybercrime.gov.ua>

**Щоб не стати жертвою комп'ютерних вірусів, шпигунський програм і різного роду інтернет-шахраїв небхідно дотримуватись деяких правил:**

* 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.
* 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.
* 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.
* Банки та сервіси електронної пошти не будуть починатись з http – тільки https! (протокол шифрування переданих і отриманих даних).
* Завжди встановлюйте антивірусну програму і фаєрвол, своєчасно оновлюючи антивірусні бази.
* 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.
* 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.
* Своєчасно оновлюйте операційну систему і софт.

<https://www.youtube.com/watch?v=z2tD0Ug6_w0&feature=emb_logo>