УДК 004.056

Пфо О.М.
Кіровоградський національний технічний університет

Захист в соціальних мережах

Останнім часом досить часто чую про злом сторінок в соціальних мережах. Дуже сподіваюся, що ця стаття допоможе Вам убезпечити себе в інтернеті.

Щоб вміти захищатися треба знати способи злому. Розглянемо основні з них:

Спосіб 1: Підбір пароля. Дуже часто при реєстрації користувачі вводять дуже прості паролі складаються, наприклад, з імені та дня народження. Знаючи ці дані і використовуючи спеціальні програми можна підібрати пароль за кілька годин. Щоб максимально убезпечити себе від ситуації коли пароль можуть підібрати потрібно використовувати безпечні паролі складаються з цифр, великих і маленьких літер латинського алфавіту. Так само в паролі не повинно бути слів, що зустрічаються у словнику (навіть набраних в іншій розкладці клавіатури) і загальновідомих даних про користувача. Якщо довжина пароля буде більше 8 символів (краще 10-15), тоді час, необхідний на підбір пароля, буде обчислюватися сотнями років і в підборі не буде сенсу. Єдиний мінус таких паролів - їх важко запам'ятати. За-цьому потрібно записувати паролі. При створенні пароля можна чергувати випадкові голосні і приголосні букви. Тоді пароль буде читати і легше запам'ятовується. Для створення безпечного пароля можна користуватися генераторами безпечних паролів, наприклад як цей.

Спосіб 2: Через систему відновлення пароля. Один із способів відновлення пароля в соціальних мережах працює через електронну пошту. Якщо хакеру вдасться захопити пошту він зможе захопити і аккаунт соціальної мережі зареєстрований на цю пошту. А відновлення пароля пошті працює через секретне питання. Зазвичай до пошти запитання? Правильно - дівоче прізвище матері. Але це не дуже-то і секретна інформація. Її цілком можна дізнатися. Ось і все - пошта і все, що на неї зареєстровано зламано. Як від цього захиститися? Придумуємо ще один безпечний пароль і вводимо його у відповідь на секретне питання до вашої пошти.

Спосіб 3: Перехоплення пароля. Якщо Ви користуєтеся інтернетом в громадському місці через безкоштовну точку доступу - Ваш пароль не може бути перехоплено. Так само якщо Ви заходите в соціальна мережа з чужого комп'ютера, або з комп'ютера в інтернет - кафе- Ваш пароль не може бути перехоплено програмами-keyloger-ами, які запам'ятовують все, що було набрано з клавіатури. Так само Ваш пароль можуть дізнатися люди знаходяться поруч, коли ви набираєте.

Спосіб 4: Різні методи соціальної інженерії.(що це таке можна прочитати за посиланням в Wikipedia) Використовуючи які зловмисник може змусити користувача розповісти йому дані для доступу. Наприклад хакер надсилає користувачу лист нібито від техпідтримки mail.ru з схожого адреси в якому моторошно вибачається за незручності і просить у зв'язку з технічними роботами вислати йому свої логін і пароль. Запам'ятайте: ніколи ніяка служба техпідтримки не попросить у Вас ваш пароль. І ніколи ні за яких обставин не потрібно розповідати ваш пароль стороннім.

Спосіб 5: Фішинг. (перекладається як рибалка) Це один з методів соціальної інженерії, який зараз дуже поширено, тому зупинимося на ньому детальніше. Суть методу в тому, що користувача різними способами перенаправляють на сайт, в точності схожий на сайт соціальній мережі (наприклад копія сайту однокласники) і просять авторизуватись. Користувач вводить свої облікові дані, після чого його перенаправляє на цей сайт (однокласників) а пароль залишається у хакера. Наприклад Вам приходить лист на пошту нібито від сайту однокласники що у Вас нове повідомлення і посилання, щоб його відкрити. Якщо клацнути по посиланню - потрапляєш на сайт точнісінько скопійований з однокласників з проханням ввести свій логін і пароль. У цей момент потрібно уважно придивитися що за адресу сайту в рядку браузера і чи

справді він відповідає потрібному або відрізняється, як наприклад цей http://www.ondoklassnlki.ru. Такі посилання можуть приходити і від друзів в соціальних мережах чиї сторінки були зламані. Так само різні ігри та програми на сторінках соціальних мереж можуть перенаправляти користувача на такі сайти. Потрібно бути гранично уважним коли вводиш пароль.

Спосіб 6: Файли cookie. Це файли, які сайті передає на комп'ютер користувача при вході. Ці файли зберігаються на комп'ютері користувача. За допомогою файлів cookie сайт дізнається користувача при повторному вході. Коли Ви встановлюєте галочку "запам'ятати мене" на формі введення пароля, сайт запам'ятовує Вас (можливо на місяць) і при наступному вході ідентифікує файл cookie і пускає без пароля. Якщо галочка "запам'ятати мене" не встановлена сайт запам'ятовує Вас поки Ви не закриєте браузер. Щоб припинити такий вхід без пароля потрібно натиснути посилання "Вихід" на Вашій сторінці в соціальній мережі. Якщо хакер отримає ваш cookie-файл поміняти пароль він не зможе, але почитати особисту переписку і розіслати повідомлення від Вашого імені зможе. До тих пір поки відкрита Ваша сесія. Як можуть вкрасти Ваш cookie-файл? Якщо змусять Вас перейти за певною посиланням. Навіть можна і не красти нічого. Якщо Ви в цей момент вже зайшли на сайт соціальній мережі від Вашого імені можна розіслати повідомлення або злити Вашу переписку. Захист від цього - лише бути уважним і не переходити за підозрілими посиланнями. Взагалі підозрілі посилання краще не відкривати - можна і підчепити вірус. Я іноді дивуюся людям, які з давно застарілим антивірусом або взагалі без нього працюють роками на комп'ютері та в інтернеті, і у них немає жодного вірусу. Вся справа в тому, що вони ходять в інтернеті тільки на відомі їм сайти і обережно, і не встановлюють нових програм. А в інших за місяць зі свіжим антивірусом ціла колекція троянів... Є над чим замислитися.

Спосіб 7: Вірус. Програми які працюють на комп'ютері користувача можуть отримати доступ до різних даних, в тому числі і до паролів, файлів cookie. Шкідливі програми можуть збирати таку інформацію та відправляти її через інтернет злодіям. Захист у даному випадку звичайно свіжий антивірус. Але, як показує практика, жоден антивірус не захищає на 100%. І звичайно ж перша захист це обережність користувача. Якщо ви встановлюєте програми з інтернету, качайте їх з авторитетних перевірених сайтів. Краще всього брати програми на сайті виробника (тобто з перших рук). Так само віруси можуть розсилати поштою у вигляді вкладень. Можна заразити свій комп'ютер перейшовши по посиланню в інтернеті. Деякі якісні віруси залишаються непоміченими антивірусами протягом багатьох місяців. Так що головний захист - обережність користувача.

Спосіб 8: Діри в безпеці сайту соціальної мережі. Сучасні соціальні мережі та поштові портали це складні програмні комплекси та хакери в їх роботі знаходять помилки і примудряються отримувати доступ до закритих даних на сторінках користувачів, або навіть зламувати сторінки. Звичайно адміністрація ресурсу і програмісти то ж не дрімають і закривають виявлені вади. Захиститися тут ми ніяк не можемо, можемо лише повідомити про відомі факти злому в адміністрацію ресурсу.

Отже, для безпечного користування соціальними мережами і поштою слід використовувати безпечний пароль як мінімум 8 знаків, використовувати безпечний пароль у відповіді на секретне питання в пошті, не користуватися соц мережами і поштою через безкоштовні точки доступу Wi-Fi в інтернет клубах і на чужих комп'ютерах, не розповідати і не висилати свій пароль нікому ні під яким приводом. При введенні пароля на вхід в соцмережу або пошту звернути увагу на адресу сайту в рядку браузера і перевірити той чи це сайт. Якщо сумніваєтеся, краще наберіть вручну або заходьте через збережені закладки. Необхідно з обережністю переходити по запропонованих посиланнях, переходити тільки якщо повністю довіряєте. Треба утримувати антивірусний захист в актуальному стані, не встановлювати сумнівні програми на ПК, не відкривати сумнівні поштові вкладення.

Список використаних джерел

1. *Зайченко Ю.П. Комп'ютерні мережі: Навчальний посібник. – К.: Слово, 2003. – 286 с. – 20.00.*
2. *Лозікова Г.М. Комп'ютерні мережі. – К.: Центр навчальної літератури, 2004. – 128 с.*
3. *Валецька Тетяна Михайлівна Комп'ютерні мережі. Апаратні засоби. – К.: Центр навчальної літератури, 2004. – 208 с.*