Москаленко М.В.
Національна академія Служби безпеки України

Захист інформації в соціальних мережах

На сьогодні, соціальні мережі — один з найбільш відвідуваних ресурсів в глобальній мережі інтернет. З їх допомогою аудиторія отримує новини від традиційних до альтернативних джерел, коментує їх, тлумачить та займається поширенням з них інформації, стаючи співучасником своєрідного інформаційного процесу. Сотні мільйонів користувачів щодня витрачають чимало часу для ознайомлення із загально-тематичними новинами в мережах на зразок Facebook. Люди добровільно позбавляють себе бодай частини звичної приватності (заповнюють профіль правдивими даними, завантажують свої фото), заради того, щоб дізнатись більше про інших, їх інтереси та погляди на життя. Поширення інтернету, а також оптимізація робочого та вільного часу людини стимулює до відмови від класичних форм спілкування на користь форм новітніх [2].

Дуже важко уявити сучасні комунікації між людьми, які мешкають в різних містах та країнах без активного використання соціальних мереж. Безумовно, - це дуже зручно, оперативно, пізнавально й нерідко – приємно. Але, на початковому етапі, щоб майбутньому користувачеві зареєструватись в певній соціальній мережі, їх власники (правовласники) тим чи іншим шляхом змушують надати їм добровільну і найчастіше досить широку інформацію про користувачів (тобто – про більшість з нас). А ми, в силу певних причин, не знаємо і (або) не розуміємо цього, внаслідок чого досить часто беззастережно, швидко, і що найцікавіше - абсолютно добровільно надаємо їм таку розширену інформацію не тільки про себе, а й навіть про своїх родичів, друзів, товаришів по службі тощо. Іноді така інформація може суперечити основним положенням закону України «Про захист персональних даних» [3].

Розглянемо на прикладі Facebook, яким чином захистити свою інформацію та убезпечити себе від її витоку, користуючись соціальними мережами.

Станом на початок 2016 року, база даних Facebook містить понад 1,55 мільярда акаунтів користувачів. Кожного дня вони завантажують понад 200 мільйонів фотографій і залишають понад 2 мільйони коментарів до різноманітних об'єктів мережі. На перебування в Facebook і Instagram припадає 20 відсотків усього часу, який витрачається на життя, стверджують адміністрації соцмережі. За даними сайту Alexa.com, серед 500 веб-сайтів, Facebook по відвідуванню займає 2 місце в світі. Facebook зареєстрував 8 мільярдів переглядів відео на день з аудиторією близько 500 мільйонів осіб [2].

Правила безпеки при використанні соціальної мережі Facebook.

Facebook – один з найпопулярніших сайтів соціальних мереж. У багатьох людей є облікові записи Facebook. Більшість з них використовує рекомендовані налаштування конфіденційності Facebook і діляться інформацією, яка не повинна бути опублікована взагалі. Тому зосередимося на налаштуваннях конфіденційності Facebook. Деякі основні правила і рекомендації:

Створення стійкого пароля. Створіть стійкий пароль, щоб захистити ваш профіль від зловмисників. Основне правило - не використовуйте загальновідомі слова або імена в якості пароля, а якщо вже використовуєте, зробіть їх складними, щоб декодувати. Це означає не тільки додавати цифри в кінці, адже фактично це неефективний шлях. Хороший пароль можна отримати змішуванням великих і малих літер, символів та чисел.

Наприклад, слово «слони» може бути змінено наступним чином: eLEp25haNTs. Крім того, ваш пароль повинен бути не менше восьми символів. Не забувайте додавати такі спеціальні символи як, #, $,%, &, »щоб зробити ваш пароль ще стійкіше. Наприклад: eLEp25h @ NT $.

Інформація про ваші дні народження. Ймовірно, ви ніколи не могли навіть подумати, що така проста інформація може використовуватися проти вас. Однак це може послужити ключем для викрадачів ідентифікаційних даних і тому не рекомендується показувати повну дату народження у вашому профілі. Натомість покажіть тільки місяць і день або взагалі не вказуйте цю інформацію. Ви можете змінити цю інформацію у Вашому профілі.

Вибір налаштувань конфіденційності. Facebook дозволяє вибирати інформацію, якою ви хочете поділитися і хто може її бачити. Це означає, що ви можете обмежити доступ до своєї біографії, фотографій, відео, повідомлень для певних людей або групи, ваших друзів, друзів друзів. Наприклад, зробіть свою інформацію про профіль доступною тільки для ваших друзів, таким чином невідомі люди не будуть перевіряти, де ви живете і що робите. Між іншим, вашу контактну інформацію, таку як адреса і номер телефону, не варто публікувати взагалі, так як ви, мабуть, не любите непроханих гостей або телефонних дзвінків від незнайомих людей серед ночі.

Інформація про ваші плани. Відправляючи повідомлення про те що ви їдете на канікули або на вихідні, ви даєте підказку зловмисникам про те, що в зазначений час ваш будинок буде порожній.

Запобігайте використанню пошукових систем для знаходження інформації про вас. Загальний профіль може бути знайдений Google, або іншою пошуковою системою - досить ввести ім'я людини і прізвище. Саме так, наприклад, роботодавці отримують більше інформації про людину, яку вони хочуть найняти на роботу. Зловмисник може зробити те ж саме. Так що, якщо ви хочете захистити свою конфіденційність, переконайтеся, що загальнодоступний пошук відключений. Для цього в розділі Пошуку засобів управління конфіденційністю Facebook оберіть "Результати пошуку Facebook» доступні тільки для друзів. Публікація імені вашої дитини. Не використовуйте ім'я дитини в заголовках або фото тегах. Якщо хтось це зробить, попросіть видалити ім'я та тег [1].

Отже, наявність загроз інформаційній безпеці людини в соціальних мережах зовсім не означає, що треба боятися ними користуватися або видалятися одразу. Для безпечного користування слід, по-перше, думати яку інформацію про себе розміщати в соціальних мережах, не вказувати ні в якому разі свої персональні дані, інформацію, що стосується близьких людей, родичів, по-друге, використовувати антивірусне програмне забезпечення на ПК, по-третє, не заповняти всі поля, які пропонує заповнити соціальна мережа(адреси навчання, роботи, проживання і т.д.). Просто не говоріть зайвого в Інтернеті, зазвичай найслабшою ланкою в мережі є людина, а не програмний код.

Список використаних джерел

1. *Голубенко О. Л. Соціальні мережі як загроза безпеки [Електронний ресурс] / О. Л. Голубенко, А. С. Петров, А. О. Петров. – 2011. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/VSUNU/2011_7/title/1.pdf.*
2. *Деркаченко А. Я. Соціальні мережі, як середовище для технологій маніпулятивного впливу [Електронний ресурс] / А. Я. Деркаченко. – 2016. – Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493.*
3. *Карманний Є. В. Підходи до захисту інформації при користуванні соціальними мережами [Електронний ресурс] / Є. В. Карманний, С. О. Ковжога. – 2015. – Режим доступу до ресурсу: http://dspace.nlu.edu.ua/bitstream/123456789/8420/1/Karmannuy_Kovgoa.pdf.*