ЗАПОБІГАННЯ РОЗГОЛОШЕННЮ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

***Цибуляк Б.З.**, канд. фіз.-мат. наук, доцент кафедри управління інформаційною безпекою;*
***Шиптицька І.І.**, студент; **Любовецька Я.О.**, студент*
Львівський державний університет безпеки життєдіяльності

Використання передових інформаційних технологій та досягнень науково-технічного прогресу дало людям неабиякі можливості для спілкування. Соціальна мережа – це структура, що базується на людських зв'язках або ж взаємних інтересах. В якості інтернет-сервісу соцмережа може розглядатися як платформа, за допомогою люди можуть здійснювати зв'язок між собою та групування за специфічними інтересами. Завдання такого сайту полягає у тому, щоб забезпечити користувачів всіма можливим шляхами для взаємодії один з одним – відео, чати, зображення, музика, блоги та інше [1]. Сьогодні користувачами соціальних мереж є десятки мільйонів людей. На сторінках цих сервісів користувачі проводять багато годин на день бо соціальні мережі у значній мірі задовольняють потреби у спілкуванні. Але оскільки такі місця згуртовують багатьох людей, тут також полюють кіберзлочинці.

Проте за привабливістю соціальних мереж приховаються деякі небезпеки, про які потрібно знати. Найбільший недолік соціальних мереж – публікація у вільному доступі конфіденційної інформації про людину. Більшість мереж збирають значно більше особистих даних, ніж фактично вимагається для реєстрації. Так, якщо постаратися, через соціальні мережі можна дізнатися про людину практично усе. За допомогою програм, що розпізнають особу по фотографії і дозволяють знайти в Глобальній мережі усі матеріали, з нею пов'язані, ми можемо дізнатися про людину значно більше, ніж вона хоче про себе розповідати. Для прикладу, в США соціальні мережі регулярно використовуються поліцією для пошуку інформації. Абсолютно усе, що ми викладаємо в соціальні мережі, залишається там назавжди. Пошукові машини також зберігають усю інформацію в кеші при індексації, так що бути упевненим в тому, що усі небажані матеріали видалені, не можна. Також існує можливість обману користувача такої мережі. Адже існують шахраї, що усілякими способами намагаються одурити нас та заробити на цьому. Саме тому не слід видавати свою особисту інформацію незнайомцям.

Сьогодні злам аккаунта в "Вконтакті", спустошення вашого електронного гаманця або викрадення пошти стали настільки буденними речами, що на них вже ніхто не звертає уваги. Головною причиною, по якій користувачі стають жертвами шахраїв, дотепер залишається їхня зайва довірливість. Багато людей не розуміють, що інформація, розміщена ними в соціальних мережах, може бути знайдена і використана ким завгодно, у тому числі не обов'язково з добрими намірами. Інформацію про учасників соціальних мереж можуть знайти їхні роботодавці, батьки, діти, колишні або

теперішні дружини чи чоловіки, збирачі боргів, злочинці, правоохоронні органи тощо.

Наприклад, наприкінці зими 2012 року десятки користувачів "Однокласників" зіткнулися з "новим" для себе видом шахрайства. Зловмисники створювали підроблені профілі родичів або знайомих потенційної жертви, втиралися в довіру і надсилали особисті повідомлення з проханням відправити їм код, що прийшов на телефон жертви. Ці коди використовувалися соціальною мережею для придбання віртуальної валюти. В результаті зловмисники одержували прибуток, а довірливі користувачі розлучалися з реальними грошима зі своїх телефонних рахунків.

Першопричиною такого шахрайства є безпечність самих користувачів соціальних мереж, що залишають про себе дуже багато конфіденційної інформації (контактні дані, адреси, номери телефонів тощо) у відкритому доступі. Зловмисники в будь-який момент можуть використовувати цю інформацію в незаконних цілях.

Інформація про ваше фінансове становище є, мабуть, однією з найбільш секретних. У жодному разі не можна повідомляти про розмір вашої заробітної плати та про те, де ви її отримуєте і зберігайте. Під грифом секретності повинна залишитися й інформація про вашу організацію. Не публікуйте повідомлень особистого характеру на так званій "стіні". Не треба забувати про те, що шедеври на "стіні" бачить не лише одержувач, але й інші користувачі. Тому перед тим, як відправити чергове повідомлення провокаційного змісту, задумайтеся, чи не зашкодить воно адресату.

Для дітей наслідки безконтрольного спілкування з Інтернетом можуть бути найбільш непередбачуваними. У соціальних мережах, як і колись у реальному дворі, можна зустріти і друзів, і ворогів, і хуліганів, і відвертих негідників. Інститут соціології НАН України у 2009 році провів Всеукраїнське соціологічне дослідження, яке виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фото незнайомцям в Інтернеті; 17% – без вагань діляться інформацією про себе і свою родину (адреса, професія, графік роботи батьків, наявність цінних речей у домі тощо). Близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і лише дехто звертає увагу на вартість послуги. Лише у 11% батьків знають про такі онлайн-загрози, як "дорослий" контент, азартні ігри, онлайн-насилля, кіберзлочинність. Спілкуючись у соціальних мережах, дитина може легко стати жертвою шахраїв та педофілів. Діти, на відміну від дорослих, зовсім інакше реагують на симпатію, проявлену до них незнайомими людьми. І, не відчуваючи небезпеки, можуть відверто розповісти їм про свої захоплення, проблеми, сумніви і тривоги. А досвідчений маніпулятор може легко скористатися цією інформацією зі своєю мерзенною метою.

Ще одною небезпекою є те, що спілкуючись у соціальних мережах тривалий час, діти втрачають здатність до реального спілкування. Як правило, діти спілкуються у мережі зі своїми ж однокласниками або однолітками, тому говорити про абсолютну заміну реального спілкування

віртуальним не варто. Найчастіше у мережевому "павутинні" губляться замкнуті, сором'язливі підлітки, яким у реальності складно налагодити будь-які соціальні відносини. Потрапивши у соціальну мережу, дитина відмежовується від батьків, перестає підтримувати з ними відносини. Віддалення від сім'ї – нормальний етап дорослішання. Без цього підліток не зможе збагнути свою унікальність, знайти власне місце під сонцем. Ця стадія розвитку дитини збігається з періодом активної соціалізації, який, як уже зрозуміло, протікає не лише у реальному, а й у віртуальному світі [2].

Тому для підвищення рівня безпеки при роботі в соціальних мережах пропонуємо користувачам дотримуватись ряду нескладних правил.

- Розміщення в Інтернеті особистої інформації наражає користувачів на ризик втратити роботу або стати жертвою шахрайства чи знущань.
- Вибовкувати все, що лишень прийде в голову – не найкраща ідея, проте мільйони людей саме це щодня й роблять. Більшість з них досі не розуміють, до яких наслідків може призвести також їхня онлайн-поведінка в соціальних мережах на кшталт Facebook, LinkedIn тощо.
- Щиро оповідаючи про свої емоції та почуття, ми полегшуємо завдання шахраям, які забажають втертися до нас у довіру та викликати співчуття, а також стаємо зручною мішенню для кібер-знущань та принижень.
- Розміщене необережне фото чи коментар здатні зруйнувати репутацію, кар'єру чи навіть привести до суду. Наприклад, професору з Північної Дакоти вдалося одержати компенсацію в 3 мільйони доларів від свого колишнього студента, який написав, що викладач є педофілом [3].
- Думай перед тим, як писати щось у Twitter чи іншу соціальну мережу, адже це може побачити будь-хто.
- Не пишіть, де знаходитесь саме зараз. Одна справа зателефонувати вашим друзям і повідомити, що ви спізнюєтесь на зустріч. І зовсім інша - повідомити 47 вашим "друзям", половину з яких ви ніколи не бачили, що повертатиметесь додому пізно й самі.
- Не викладайте в мережу інформацію про ваше життя. Викладання подробиць про те, до якої школи ви ходили або ваше дівоче прізвище, може призвести до того, що з часом злодії знатимуть про вас не менше, ніж ваша сім'я.
- Бережіть інформацію про інших людей.
- Поменше пишіть про дорогі покупки. Злодії вишукують людей, з яких можна поживитися. Коли ви розповідаєте про дорогі подарунки, які накупили до свят, то даєте іншим сигнал, що не завадило б понишпорити у вашому домі чи авто.
- Не дайте злодіям дізнатися, що вас немає вдома. Крадіжка – ризикована справа, а тому завжди безпечніше лізти у пустий будинок: можна винести все, що забажаєш, і більш того – піти чистим. Не пишіть про те, що їдете з дому або й взагалі де живете.
- Бережіть інформацію про своїх дітей. Чим менше інші люди знають про ваших і чужих дітей, тим краще. Не пишіть про їхнє місцеперебування,

звички, уподобання, друзів, гуртки після школи. Безпека дітей – це найважливіша річ.

- Ризик стати жертвою переслідування цілком реальний. Зустрічатися особисто зі своїми новими друзями з Twitter варто лише у публічних місцях.
- Не розповідайте подробиці, які хулігани можуть використати, щоб підколювати вас у мережі. Дражняться не тільки злі діти.
- Не діліться інформацією, що може зашкодити вашій репутації. Невлучними жартам, політичними тирадами, дурними витівками завдяки сучасним технологіям та соціальним мережам ви можете миттєво знищити свою репутацію.
- Не ображайте і не брешіть про ваших рідних, друзів чи колег. Плітки про друзів можуть стати для вас справжньою халепою. Пам'ятайте, за руйнування чужої репутації доведеться відповідати.

Отже, кожен користувач повинен сам дбати про конфіденційність своєї інформації, оскільки від наявності чи відсутності особистих даних соціальна мережа нічого не втрачає, а зловмисникам це лише на руку.

1. Пішковцій С. Що таке соціальні мережі? [Електронний ресурс]. – Доступний з http://blogoreader.org.ua/2008/04/09/about-social-networks/
2. Діти і соціальні мережі. [Електронний ресурс]. – Доступний з http://skola36.ucoz.ru/4_batk.doc
3. Forbes: правила безпеки в соціальних мережах. [Електронний ресурс]. – Доступний з http://life.pravda.com.ua/technology/2010/11/19/65605/