УДК 351.865

Скрута Г.В., Шкарупа І.В., Нікуліщев Г.І.
Запорізький національний технічний університет

Забезпечення інформаційної безпеки у соціальних мережах

Життя сучасних людей в еру інформаційного суспільства не можна уявити без Інтернету. Зараз – це частина нашого повсякденного життя. Інтернет є досить багатогранним. Це одночасно середовище для спілкування, розваг та навчання. За допомогою Інтернету стало можливим робити покупки та оплачувати послуги. Для багатьох людей – це спосіб заробітку. Проте найбільшою цінністю в мережі є сама інформація. Великою перевагою Інтернету можна назвати його всеохопність, тобто об’єднання людей і ресурсів. На сьогодні Інтернет є доступним майже кожному.

Інтернет - глобальна комп'ютерна мережа, що охоплює увесь світ. Сьогодні Інтернет має близько 15 мільйонів абонентів у більш ніж 150 країнах світу. Щомісяця розмір мережі збільшується на 7-10%.

Досить тісним є зв'язок Інтернету з освітнім процесом. Інформація, яка необхідна людині, що навчається, може міститись не тільки у підручниках, збірниках, журналах, а й у електронному вигляді в мережі. Сьогодні різноманітність навчальних джерел є надзвичайно великою. Також необхідно зазначити можливість дистанційного навчання, що тепер є поширеним явищем. Цей процес заощаджує велику кількість часу.

Інтернет робить наше життя легшим і зручним.

Часто Інтернет використовують для спілкування в соціальних мережах. Соціальні мережі все глибше проникають у життя користувачів. У них можна знайти однодумців, вони допомагають завжди бути в курсі останніх подій та нагадують про дні народження друзів і знайомих. Але поряд з перевагами віртуального спілкування є небезпека заволодіння приватною інформацією зловмисниками для використання її в неправомірних цілях.

Мета роботи - розглянути можливі небезпеки у соціальних мережах та шляхи їх подолання. Як відомо, захист починається з усвідомлення того, чого потрібно остерігатися. Спеціалісти у галузі кібербезпеки виділяють найбільш типові загрози, серед яких: маніпуляція, ЗПЗ (зловмисне програмне забезпечення), мережеві та комп’ютерні атаки, дезінформування, фармінг, фішинг тощо.

Зловмисники використовують всі види обману для отримання доступу до особистої інформації користувача мережі та її використання. Однією з яких є фішинг.

Фішинг — це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію. Цей вид шахрайства заснований на довірі та заволодінні злочинцем аккаунтом іншого користувача. Він зазвичай передбачає надсилання користувачу соціальної мережі повідомлення, яке ніби походить із довіреного джерела, наприклад від знайомого з проханням позичити електронних грошей, скачати контент або перейти за посиланням. Людина не може точно знати, хто відправив їй повідомлення – друг чи шахрай, який заволодів його сторінкою, і, як правило, вона, не замислюючись про це, виконує прохання.

Фішингова атака може розвиватись наступним чином – користувачеві приходить повідомлення від знайомої з проханням перерахувати гроші на картку або мобільний телефон в борг. Користувач довіряє людині та перераховує їй чималу суму грошей, але насправді аккаунтом знайомої заволоділа інша людина, яка розсилає такі повідомлення та краде чужі гроші. Відгородити себе від цього шахрайства дуже просто: треба лише зв’язатися з тим, хто відправив повідомлення з проханням по іншому

каналу зв’язку (наприклад, зателефонувавши йому) і запитати підтвердження прохання.

Досить поширеним явищем у мережі є випадки, коли у повідомленні може бути посилання на віруси, черв'яки, троянські програми Ці небезпечні програми створені для зараження комп'ютера з метою його пошкодження, викрадення особистої інформації, шпигунства чи показу реклами.

Підключений до Інтернету комп`ютер не тільки отримує доступ до інформації, розташованої на серверах глобальної мережі, але й стає вразливим для зовнішніх мережевих атак, підготовлених зловмисниками. Веб-сайти й соцмережі вразливі до атак. Такий вид загрози найважче попередити. Але користувач може встановити декілька бар'єрів між собою та атакуючим. Найбільш простий спосіб захистити свій комп’ютер від мережевих атак - встановити на нього та належним чином налаштувати антивірусне програмне забезпечення та міжмережевий екран.

Нерідко у соцмережах можна зустріти явище дезінформування – спосіб психологічного впливу, що полягає в навмисному поданні користувачеві такої інформації, яка вводить його в оману відносно справжнього стану справ. Перекручені, неповні або неправдиві відомості поширюються для досягнення пропагандистських, військових, комерційних або інших протизаконних дій. Людина, яка була дезінформована, в свою чергу продовжує подальше розповсюдження неправдивої інформації серед користувачів (через друзів, групи та сторінки в соцмережі), адже вірить обману.

Фармінг — це перенаправлення жертви за помилковою адресою, наприклад це імітація сторінки авторизації в соціальну мережу з метою заволодіння логіном та паролем від облікового запису. Аби не потрапити у цю пастку необхідно уважно дивитися, за якими посиланнями та сторінками здійснюється перехід та використовувати механізм двофакторної аутентифікації в соцмережі.

Отже, для захисту від загроз необхідно мати на увазі наступне:

1. Слід реєструватися не у всіх підряд соцмережах, а лише у тих, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача.
2. Авторизацію в соцмережі слід виконувати, вводячи її URL у адресний рядок браузера вручну або використовуючи заздалегідь збережені вкладки чи посилання.
3. Якщо є сумніви щодо знайомства з користувачем, який подав заявку у друзі, треба дочекатися підтвердження його особистості через інші джерела.
4. Обов’язково час від часу слід змінювати паролі на всіх своїх сторінках. Бажано використовувати окремі паролі для кожного аккаунту – тоді, в разі зламу однієї сторінки, інші залишаться в безпеці.
5. . Слід пам’ятати, що будь-яка інформація, розміщена в Інтернеті, з великою імовірністю залишається там назавжди, навіть в разі її видалення автором, адже може бути збережена або поширена іншими користувачами.
6. Особливу увагу слід приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

В роботі проведений аналіз найбільш поширених загроз для користувачів соціальних мереж. Автори пропонують загальні рекомендації для уникнення цих загроз. Якщо дотримуватися рекомендацій щодо поведінки у мережі Інтернет, можна зменшити ймовірність потрапити до пастки зловмисників та втратити конфіденційну інформацію.

Список використаних джерел

1. *Офіційний сайт газети «Львівська пошта»: Небезпека соціальних мереж [Електронний ресурс]. – Режим доступу: http://www.lvivpost.net/suspilstvo/n/24110* .