УДК 004

Дробот М.В. студент гр. 125-20-1
Науковий керівник: Олішевський І. Г., асистент кафедри БІТ
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

БЕЗПЕКА ІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ

За статистикою Global Digital 2021 року, соціальними мережами користуються 53,6% населення світу, а це близько 4.2 мільярда користувачів. На сьогоднішній день в мережі Інтернет налічується більше 250 соціальних мереж. Користувачами подібних сервісів є люди різного віку, починаючи від підлітків і закінчуючи пенсіонерами. Саме тому сучасникам необхідно знати як правильно користуватися соц. мережами, яку інформацію можна публікувати на своїх сторінках, а яку - ні. Адже серед мільярдів користувачів завжди знайдуться шахраї або ті, які захочуть завдати вам шкоди.

Для безпечного користування соціальними мережами не потрібно робити чогось неможливого. Є невелика кількість пунктів, при виконанні яких можна досягти максимальної захищеності від найбільш розповсюджених загроз.

1. Середа користування. У першу чергу потрібно переконатись у тому, що браузер, або комп'ютер, з якого буде виконано вхід до соціальної мережі, не має ніяких вірусів та фішингових програм. Не варто користуватись невідомим ПЗ для того, щоб увійти до своєї сторінки, адже не можна бути цілком впевненим, що уведені дані не потраплять до рук небажаних осіб. Найбільш розповсюдженою помилкою є завантаження браузеру на свій комп'ютер через сторонні хмарні середовища або файло-обмінники. Дуже часто у програмному коді браузерів, узятих з таких сайтів, є непомітний скрипт, який викачує уведені вами дані на сторінках та надсилає їх хакерам. Саме тому потрібно завантажувати браузери з офіційних сайтів та завжди оновлювати його. Також, не забувайте про антивірус вашого комп'ютеру, який у разі небезпеки зможе попередити про підозрілі частинки програмного коду завантажувальної програми.

2. Справжність сторінки. Іноді ми зовсім не звертаємо увагу на зовнішній вигляд сторінки, до якої переходимо. Потрібно перевіряти справжність адреси сторінки, на яку бажаєте потрапити. Існує багато сайтів з підробленою адресою, що на вигляд мають той самий інтерфейс, як і справжній. Наприклад, використовуючи шрифт Times New Roman майже неможливо відрізнити цифру 1 від маленької латинської літери L. Саме такими прийомами підробки адрес і користуються шахраї. Результатом заходу через подібний сайт може бути як викрадення вашого логіну або паролю, так і розміщених на сторінці даних. Щоб уникнути цього, варто вводити самому адресу сторінки, на яку бажаєте потрапити і, для зручності, додати до закладок браузеру, аби мати швидкий доступ до неї.

3. Паролі. При реєстрації в соціальних мережах потрібно створити надійний пароль, що містить не менше 7 символів, включаючи символи нижнього та верхнього регістру, цифри і, якщо можливо, спеціальні символи (!,*,/,? т.п.). Існує велика кількість програм підбору паролів. Для прикладу візьмемо програму, засновану на методі Bruteforce. Даний метод підбору паролів заснований на тому, що до програми заносяться певні символи, з яких потім машина генерує абсолютно раптові комбінації символів. Від довжини та складності паролю залежить час, який буде потрібен для його підбору. Тож чим унікальніше набір символів, тим складніше буде розгадати ваші реєстраційні дані як програмам, так і людям. Варто пам’ятати, що для кожної сторінки пароль повинен бути унікальним і не повторюватися, щоб при можливому зломі одного облікового запису, не можна було потрапити під тими ж даними до іншого.

4. Інформація на сторінці. Не публікуйте конфіденційну інформацію сторінках соціальних мереж. Наслідками подібних дій може стати розповсюдження ваших даних в інших гілках мережі Інтернет, доступ до банківських рахунків та навіть шантаж. Гадаю, усі пам'ятають ситуацію 4 жовтня 2021 року, коли велика кількість відомих соц. мереж припинила свою роботу на деякий час. Може хтось знає, а може і ні, але за цей період на популярному хакерському форумі з'явилось оголошення про продаж даних 1.5 мільярда користувачів Facebook. Ця інформація офіційно підтверджена інтернет-джерелом дослідження конфіденційності даних та кібербезпеки Privacy Affairs. Тож не слід зберігати важливу інформацію у діалогах, навіть у вкладках “Збережене” та “Обране”, тому що при витоку реєстраційних даних сторінки усе це може потрапити до рук шахраїв.

5. Повідомлення. Дуже розповсюдженим способом шахрайства є розсилка повідомлень з проханням допомогти від обличчя друзів та знайомих. Я сам ставав жертвою розсилки таких повідомлень, як "Привіт. У мене зараз сталася дуже неприємна ситуація і мені терміново потрібно 200 гривень. Чи не можеш ти, будь-ласка, перевести мені їх на карту, а я тобі завтра поверну, навіть більше." Знизу був прикріплений номер банківського рахунку і наприкінці веселий смайлик. На моє щастя я заздалегідь мав номер картки своєї подруги і перевів гроші саме на неї, не звертаючи уваги на той номер. Через хвилину мені передзвонила ця подруга зі словами "Дякую, а що за свято сьогодні?". Отже перед тим, як реагувати на подібні повідомлення, потрібно зв’язатися з цією людиною по телефону, або через іншу мережу, щоб переконатися, що повідомлення надіслано саме від неї, а сторінка не була зламана шахраями.

Також не варто завантажувати невідомі файли та переходити за невідомими посиланнями від незнайомих користувачів. Усім зрозуміло, що є ризик заразити комп’ютер вірусними програмами.

Висновки

Проблеми безпеки та шахрайства у соц. мережах будуть існувати доти, доки існують самі соц. мережі. Кожен з нас має ризик стати жертвою інтернет-злочину та втратити свої конфіденційні дані, тож є лише 2 варіанти

вберегти себе від цих загроз. 1 - видалити свої облікові записи з усіх соціальних мереж і припинити користуватися ними, 2 - дотримуватися усіх заходів для запобігання небажаних подій.

Перелік посилань

- https://socialmedialist.org/social-media-apps-201-250.html - кіль-ть соц мереж.
- https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/ - статистика global digital 2021.
- https://minterese.ru/pravila-bezopasnosti-v-sotsialnyh-setyah/ - основні правила безпеки соц мереж.
- https://www.privacyaffairs.com/facebook-data-sold-on-hacker-forum/ - продаж даних про 1.5 млрд користувачів FB.
- https://www.anti-malware.ru/threats/brute-force - метод підбору паролей Bruteforce.