УДК 004.6

О.С. Пазюк
Ю.В. Бойчук

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

Досліджено загрози персональним даним у соціальних мережах та розглянуто правила захисту даних.

Ключові слова: соціальні мережі, інформація, обробка персональних даних, доступ.

Abstract

Threats to personal data in social networks are investigated and data protection rules are considered.

Keywords: social networks, information, processing of personal data, access.

Вступ

Протягом останнього десятиліття значної популярності набувають соціальні мережі. В них люди можуть обмінюватися інформацією, налагоджувати ділові зв'язки та просто спілкуватися. Начебто все просто і такі справи не потребують детального вивчення. Але сучасна тенденція показує, що користувачі досить недбало ставляться до безпеки особистої інформації. А тому у мережі з'являється більше справ, пов'язаних із використанням даних певної фізичної чи юридичної особи або ж установи, дедалі більше жертв кіберзлочинів звертаються до правових установ. Тенденція інтернет-шахрайства зростає з кожним днем [1].

Основна частина

Зростання популярності соціальних мереж привертає увагу викрадачів особистих даних, хакерів, спамерів, розробників вірусів. Оператор соціальної мережі зобов'язаний провести обробку персональних даних, однак при цьому рівень конфіденційності і захист особистих даних покладено практично повністю на самого користувача, оскільки йому надано право самостійно вирішити, які дані він робить загальнодоступними, а до яких обмежує доступ. Тож захист персональних даних користувача в соціальній мережі – справа самого користувача.

Найчастіше користувач навіть не здогадується, що його акаунт зламаний. Шахраї діють обережно, щоб користувач нічого не запідозрив, а зламані профілі використовують у власних цілях: для вступу в групи, додавання лайків і коментарів тощо. Це безпечний для шахраїв спосіб монетизації чужого акаунта, оскільки більшість людей не пам'ятає, у які групи вони вступали, а перевіркою коментарів і лайків у всіх незліченних спільнотах Facebook, Telegram, Viber, Instagram та інших взагалі ніхто не займається [2].

Закон України "Про захист персональних даних" встановлює вимоги до обробки та захисту персональних даних, в тому числі і в Інтернет-середовищі [3]. Згідно цього закону: персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Що включають у себе персональні дані? У законодавстві України так називають будь-яку інформацію, яка допомагає визначити особистість користувача. Тобто персональними даними може бути: ім'я та прізвище, дата та місце народження, сімейний стан, паспортні дані, професія тощо. Разом із тим, паролі та аккаунти не являються персональними даними, адже не несуть ніякої конкретної інформації про особу. Але можуть бути використані у скоєнні віртуальних злочинів. Такі дані можуть ставати загальнодоступними тільки зі згоди користувача та видалені при першому їх проханні.

Що ж саме загрожує нашим даним в персональних мережах?

Електронна пошта більше ніж просто поштова скринька. Ви використовуєте її для реєстрації на більшості сайтів і сервісів, а значить, отримавши доступ до пошти, зловмисники зможуть зламати і інші ваші акаунти. Ніхто не відміняв і загрозу таємниці листування, що зберігається в діалогах документам. Якщо це робочий ящик, то до хакерів може потрапити закрита корпоративна інформація. І тоді зламана електронна пошта буде не тільки вашою проблемою - під загрозою опиниться безпеку всього листування в компанії.

Месенджери - кращі об'єкти для шахраїв, якщо вони хочуть поживитися інтимними подробицями вашого життя. У всіх є скелети в шафі, але це не означає, що вони повинні стати надбанням громадськості. Якщо ви грамотно не захистили свій аккаунт, то біда може трапитися коли завгодно. Для багатьох листування в соціальних мережах і месенджерах замінює електронну пошту - вони обмінюються фотографіями, документами, інший конфіденційною інформацією.

У всіх сучасних смартфонів є основний обліковий запис: для iOS це Apple ID, для Android - облікового запису Google. Якщо зловмисники отримають до них доступ, цінна інформація про вас і вашому смартфоні виявиться в їх руках. У минулому році стала відома історія про шахрая, який обманним шляхом отримував доступ до Apple ID, блокував телефон жертви і вимагав грошей за розблокування. Таке часто трапляється і при покупці смартфонів, коли недобросовісний продавець продає вам, по суті, цегла, яким можна користуватися, не ввівши пароль до зламаної облікового запису. Програми, що встановлюються з App Store, Google Play або Windows Marketplace, запитують доступ до даних: вашим контактам, геолокації, календарем, платіжним даними. Кожен раз уважно читайте, до якої інформації запитує доступ додаток або гра. Наприклад, навіщо грі-головоломці знати ваше місце розташування і для чого конвертера величин потрібен ваш календар?

Тому ми маємо бути обережними з нашими персональними даними і дотримуватися таких правил:

1. В першу чергу слід вигадати складний пароль мінімум з 8 символів, з урахуванням регістру (користуватись великими і малими літерами), також слід увімкнути двофазну авторизацію через телефон (до акаунту в особистих налаштуваннях додається телефон, і при вводі логіну та паролю сайт відправляє код через смс, який додатково потрібно ввести).

2.Якщо полюбляєте соціальні мережі, такі як «Facebook», обов’язково публікуйте свої записи з увімкненою функцією «тільки для друзів».

3. Не залишайте номер свого мобільного на жодному з сайтів, блогів, коли розміщуєте інформацію про себе. Його легко відслідкувати просто використавши пошук по фото.

4. В соціальних мережах не використовуйте геолокації.

5. Активуйте функцію заборони індексації сторінок гулом.

6. Користуйтеся прогамами-щитами/файєрволами, вони сповістять вас про загрозу та не допустять її проникнення у комп’ютер.

7. Здійснюйте перевірку гіперпосилань, у яких ви не впевненні, за допомогою антивірусних програм.

8. В будь-якій із соціальних мереж обмежуйте доступ до свого особистого контенту.

9.Не соромтесь повідомляти про спам або неприйнятний зміст.

10. Найголовніше! Інформацію про себе потрібно розміщувати обдумано, аби не потрапити в зону ризику [4].

Висновки

Отже, видаляйте все, чим не захотіли би ділитися з незнайомцем. Наступного разу, коли буде бажання запостити щось у себе на сторінці, поміркуйте, чи не зможе дана інформація бути використана проти вас. Пам’ятайте, що інформація, яку ви власноруч оприлюднили у себе на сторінці, автоматично стає загальнодоступною. Безперечно, не слід впадати в паніку та видалятися з усіх соцмереж, але потрібно завжди пам’ятати про безпеку своїх даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захист інформації в мережі інтернет. Як захистити особисті дані. [Електронний ресурс] // TIMES.ZT.UA. – 2017. – Режим доступу до ресурсу: https://times.zt.ua/lajfxak-khytroshhi-yaki-zaxystyat-vid-shakhraiv/.

2. Захист персональних даних в соціальних мережах [Електронний ресурс] // Вінницький апеляційний адміністративний суд. – 2016. – Режим доступу до ресурсу: http://www.vaas.gov.ua/news/zaxist-personalnix-danix-v-socialnix-merezhax/.

3. Закон України "Про захист персональних даних" [Електронний ресурс] // Верховна Рада України. – 2010. – Режим доступу до ресурсу: http://zakon.rada.gov.ua/laws/show/2297-17.

4. Галич М. Як захистити персональні дані у мережі — поради спеціалістів [Електронний ресурс] / Марина Галич // UNIVERSE. – 2015. – Режим доступу до ресурсу: http://universe.zp.ua/?p=4505.

Бойчук Юлія Володимирівна – студентка групи УБ-15б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: yulia060798@gmail.com

Пазюк Олександр Сергійович – студент групи УБ-15б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: sashapazyuk1@gmail.com

Науковий керівник: ***Катаєв Віталій Сергійович*** – асистент кафедри менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: kataev@vntu.net.

Boichuk Yulia V. – student UB-15b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: yulia060798@gmail.com

Paziuk Oleksandr S. – student UB-15b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: sashapazyuk1@gmail.com

Supervisor: ***Kataev Vitaliy S.*** – assistant of the Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kataev@vntu.net.