УДК 004.056:316.472.4

Н.Б. Макух, Т.О. Чоп
Тернопільський національний університет ім. І.Пулюя, Україна

КОНФІДЕНЦІЙНІСТЬ У СОЦІАЛЬНИХ МЕРЕЖАХ

N. Makukh, T. Chop

CONFIDENTIALITY IN SOCIAL NETWORKS

Сьогодні важко уявити своє життя без соціальних мереж. Найбільшу популярність вони набули серед юнацтва, адже саме там молоді люди мають можливість спілкуватися, отримувати різноманітну інформацію, працювати чи ділитися власною творчістю. З іншого боку, ми надзвичайно рідко задумуємось про те, скільки інформації про нас є в інтернеті. У сучасних реаліях надзвичайно важливо дбати про власну конфіденційність, адже люди навіть не здогадуються скільки даних про них можна отримати та як зловмисники можуть використати цю інформацію.

Соціальні мережі – один з найбільш популярних ресурсів в Інтернеті і варто знати, чим ми платимо за свою присутність у них. Реєструючись у соцмережі ми вказуємо свої контактні дані (телефон, email, ім'я та прізвище, місце проживання, дату народження, фотографію), у профілі зазначаємо місце навчання, роботи, хобі, іншу приватну інформацію, зокрема таку, яка стосується нашого оточення. Окремий блок інформації про користувачів становить їхня активність: контент, якому вони надають перевагу, місця, в яких перебували, відгуки, коментарі, фото – всі ці речі дозволяють без особливих зусиль скласти профайл будь-якого підписника.

Керівництво Facebook в 2018 році надало відповіді, яку саме інформацію збирає соціальна платформа: час, частоту та тривалість активності в вікні з вкладкою соцмережі; покупки, здійснені на сторонніх сайтах; плагіни в браузері користувача; рухи курсору на пристрої; використання камери; метадані фотографій (включно із часом і місцем зйомки); встановлені додатки; назви та типи файлів на пристрої; ідентифікатори додатків; кількість вільного місця на пристрої; контакти з довідника користувача; журнал дзвінків та історію SMS з Android-пристроїв; найближчі точки доступу Wi-Fi і стільникового зв'язку; інформацію мобільних і стаціонарних провайдерів через комп'ютери, телефони, зв'язані телевізори та інші пристрої в мережі; рівень заряду пристрою; параметри та дозволи на пристрої; інформацію та фотографії інших користувачів, а також частоту взаємодії та спілкування з ними [1].

Об'єм даних, які збираються соціальними мережами використовується ними з різною метою: умовно легальна (цільовий показ реклами, унікального контенту, оточення), незаконна (маніпуляція, спам, шантаж, переслідування та ін.). Небезпека полягає у тому, що доступ до даних має досить велика кількість осіб: не враховуючи співробітників соціальних платформ, це також і правоохоронні органи. Особливість платформ в тому, що персональні дані користувачі без жодних обмежень можуть використовувати і сторонні програми (аутентифікація/реєстрація через Facebook), сервіси Google. При цьому платформа не бере на себе відповідальності за порушення правил конфіденційності цими програмами. Це створює умови, за яких зловмисники отримують можливість для протиправних дій [2].

Зважаючи на те, наскільки публічними є сучасні профілі у соціальних мережах, проблема конфіденційності особистої інформації є особливо актуальною. Відповідно до Закону «Про доступ до публічної інформації» конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [4]. Важливо розуміти, що визначати, яка інформація є конфіденційною може сама людина, проте є така інформація, яка автоматично визначається законом «Про інформацію» як конфіденційна: дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [4].

Конфіденційною вважається інформація про юридичну особу. «Відповідно до статті 505 Цивільного кодексу України, це можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру і щодо яких ця юридична особа вжила заходи щодо збереження секретності. До конфіденційної юридичною особою може бути віднесена також і інша інформація»[4].

Таким чином, необережне поводження із особистою інформацією, незахищеність даних та легковажне відношення до того, яким контентом людина оперує у соціальній мережі може мати небажані та, навіть, невиправні наслідки. До таки відносяться: розсилка «вірусних» повідомлень, які насправді можуть виявитись спамом, або фейком, або ж містити неперевірені посилання, перехід за якими може привести на сторонні, небезпечні платформи, стати причиною завантаження зловмисним ПО; долучення до друзів невідомих осіб, оскільки особисті та корпоративні акаунти можуть бути підставними, дезінформаційними; викрадання персональної інформації внаслідок її слабкого захисту (простих, однакових паролів до акаунтів, електронної пошти, онлайн-банкінгу), останнє призводить до низки негативних наслідків (витік даних, персональної інформації: фотографій, переписки, що, в свою чергу, може призвести до таких кіберзлочинів як секстинг, булінг, фішинг). Порушення конфіденційності становить загрозу не лише для окремої людини, але й для місця її роботи, оскільки такі акаунти є джерелом виходу на корпоративні дані; більшість працівників вважають за нормальну практику перегляду персональної сторінки із робочих пристроїв.

У зв'язку з постійним вдосконаленням інструментів кіберзлочину спеціалісти ESET рекомендують користувачам: Не переходити за підозрілими посиланнями. Якщо легітимність ресурсу викликає у вас сумнів, краще знайти потрібну інформацію за допомогою пошукової системи Google. Ділитися лише перевіреною інформацією. В іншому випадку ви можете тільки допомогти зловмисникам в поширенні небажаного контенту. Налаштувати параметри конфіденційності. Незалежно від того, якою сторінкою ви управляєте, особистою чи корпоративною, важливо правильно налаштувати її конфіденційність. Таким чином повна інформація зі сторінки буде доступною тільки певним особам, інші зможуть бачити лише частину даних[5].

Отже, підсумовуючи сказане, можна зробити висновок, що часто люди нехтують власною конфіденційністю, реєструючись чи дописуючи в соціальних мережах. Необхідно розповідати людям про всі ризики, які можуть чекати на них в інтернеті, а самим користувачам ставати більш відповідальними та уважно читати, на що вони дають згоду, коли реєструються на тій чи інші платформі.

Література:

1. Facebook зізнався, які дані збирає про користувачів. URL https://www.epravda.com.ua/news/2018/06/13/637741/
2. Правила поведінки у Facebook, або як убезпечити свої персональні дані в соціальних мережах. URL https://bit.ly/3oKYcfJ
3. Конфіденційна інформація. URL https://bit.ly/3DDjp1l
4. Конфіденційна інформація, інформація про особу та персональні дані. URL https://bit.ly/3cwZkhs
5. Загрози безпеці в соціальних мережах — як уникнути інфікування. URL https://bit.ly/3nvK3nh