Кравчук Тетяна Андріївна
студентка
Академія Адвокатури України
м. Київ, Україна

МЕСЕНДЖЕРИ, СОЦІАЛЬНІ МЕРЕЖІ ТА СОЦІАЛЬНА ІНЖЕНЕРІЯ. ЯК ВТРАТИТИ АНОНІМНІСТЬ ТА БЕЗПЕКУ

У сучасних реаліях дуже важливо, щоб власний телефон або комп'ютер не став найсильнішою «зброєю» проти його ж власника та тих з ким він спілкується.

Метою роботи є розкриття поняття «соціальна інженерія», набуття слухачами навичок її користування. Також метою роботи є показ небезпеки популярних месенджерів й соціальних мереж, та основи власної кіберобізнанності

Прикладом простої соціальної інженерії є так званий «фішинг». Зазвичай це певні посилання, які приходять до користувача електронною поштою, або у соц. мережах. Переходячи за посиланням користувач отримує перед собою абсолютно реалістичну сторінку, на якій йому пропонується ввести свої дані. Саме через схожість сторінки на офіційну, в більшості випадків юзер вводить усю свою ідентифікаційну інформацію.

Щодо безпеки найпопулярніших соц. мереж. Згідно з даними Facebook, станом на 4 квітня 2019 року, дані більш ніж 540 млн. юзерів були абсолютно незахищені.

Ще одним популярним месенджером сьогодення є WhatsApp. Світова громадськість шокована новиною про те, що WhatsApp перетворював будь-який телефон в шпигунський пристрій. Хакери могли отримати доступ до всіх ваших даних, включаючи фотографії, електронну пошту та СМС просто через те, що на вашому телефоні було встановлено WhatsApp [1].

Новина не є дивовижною. Минулої осені WhatsApp вже визнавав наявність схожою проблеми – один відеодзвінок через WhatsApp давав зловмисникові доступ до всіх даних на вашому телефоні [2].

Погана захищеність соц. мереж викликає величезний попит на ринку чогось «більш захищеного». Але, нажаль, абсолютної конфіденційності ще не зміг домогтися ні один розробник. Так, наприклад, французька влада створила власний захищений месенджер Tchap, але він одразу ж був зламаний [3].

Як висновок можна зазначити наступне: 1) на сьогоднішній день треба приділяти величезну увагу власній кібербезпеці й кіберобізнан-

ності, заради того, щоб не потрапити на гачок до соціальних інженерів; 2) увагу, користуючись соц. мережами, треба приділяти навіть найменшим дрібницям, оскільки на сьогоднішній день не існує абсолютно захищеної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Business Insider WhatsApp was hacked and attackers installed spyware on people's phones – 15 травня 2019
2. Security Today WhatsApp Bug Allowed Hackers to Hijack Accounts – 12 жовтня 2018
3. URL https://xakep.ru/2019/04/22/tchap/